International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 86 - 91, 2015, ISSN:- 2319–8656

Improved Learning Management System (i-LMS): A Flat Form for Content Creation and Sharing for Kenyan Secondary Schools

Anthony Mutua Nzioki
Jomo Kenyatta University of Agriculture and Technology
School of Computing and Information Technology
P.O. Box 62000 - 00200, City Square, Nairobi, Kenya

Abstract: Use of ICTs integration for enhanced learning has been studied for some time now with focus mainly on content delivery. It has however been noted that ICTs usage for learning has not picked well and in a uniform way. Further, little has been done to ensure delivery from a common pool so as to promote standardization of curriculum delivery especially on content creation and sharing. This has left a gap in ICT usage and improvement of delivery. The main objective in this paper is to look at the usability of learning management system software (LMS) and recommend the development of an improved interactive learning management system (i-LMS) to facilitate data collection from users to support teaching and learning functions in secondary schools. The model shall enable content creation and sharing among students, teachers, content developers and administrators. Captured data will be kept in a common repository in a database for access by all schools for learning. This will help improve delivery through Learning Management Systems software by making it possible to avail resources to a bigger audience from a common pool.

Keywords: ICT Integration, i-LMS**,** Improved Interactive Learning Management System, Enhanced Learning

1. INTRODUCTION

Information and Communications Technologies (ICTs) have been integrated in education in many developing and developed countries alike however the use of ICTs in Kenyan secondary schools lags behind. [13] argue that the use of ICTs in curriculum delivery or eLearning is inevitable and the skills are very necessary to participate in the knowledge societies and economies of the world.

One way of looking at e-learning gives the following approaches

- Enhanced approach which enhances face to face learning using web-based technology e.g. Learning Management Systems (LMSs)
- Blended approach which focuses on both face to face and online learning and
- Online approach which uses online learning only.

Supported by two modes of e-learning

- Asynchronous where learning content is served from a web server and is available any time so learners access it at their own pace.
- Synchronous where all learners and facilitator are logged in at the same time and communicate directly and virtually with each other.

Much of the world seems to have adopted enhanced eLearning using the asynchronous mode. On the other hand only a few Kenyan schools boast of a pool of useful resources that can help them deliver in their teaching and learning effectively regardless of which mode is used for delivery and are found mainly in urban

areas. Many Kenyan secondary schools lack useful resources like libraries or are poorly equipped where available. Yet schools keep on increasing in numbers every other day against the dwindling number of teachers as well. This means an acute shortage of learning resources in the school settings alongside uneven distribution of resources. Hence there cannot be uniformity in curriculum delivery.

1.1 General Overview

Use of ICTs is supported by [8] by saying ICTs have brought a new dawn in curriculum delivery which is no longer optional but a necessity in schools at various levels of learning. [12] gives one example of this revolution as the development of learning management systems (LMS), course management systems (CMS), and virtual learning environments (VLE) that facilitate teaching and learning outside the physical classroom. She further says often, these terms are used interchangeably in designating the same tools or software. The government has shown an effort in the provision of ICTs infrastructure as well as few schools going out to purchase their own computers for use. Although most of them are used primarily for office work or computer literacy classes, this can be overturned by converting them to teaching and learning tools that can be used both online and offline.

[11] in a study to investigate the use of web tools in UK, content that learners are clearly motivated to use Web 2.0 tools for learning and teachers have an important role to play in assisting learners in using these technologies. This therefore implies that the same learners can give reliable feedback that can be used to help improve what is delivered through the Learning Management Systems as well as sharing which has not been the case. Open source software has enabled the integration of learning modules through the development of Learning Management Systems (LMS) and Content Management Systems which have capacity for forums, instant messaging, and online submission of work and the marking of such work. These systems however are however keen on providing a module for feedback on assignments yet they can be improved to upload user content from schools with resources so as to be accessed by schools without resources for use.

Technology acceptance and usage being an active area of research, has seen several models and theories proposed so as to understand the driving force behind technology adoption [2]. However there has not been a good way to help collect and process data on ICTs usage in the classrooms for purposes of improving delivery with ICTs since available LMSs collect data mainly on user interaction with stored content with no interface for direct user input of created content. Nevertheless LMSs can have a built-in tool that allows create content and store in the learning management system database for later use. By looking at the expected improvement on curriculum delivery by the use of LMSs in secondary schools especially in the rural areas, e-learning for secondary schools is given a high priority in this paper.

1.2 Background

Most secondary schools are located in rural areas hence are isolated geographically and socially hence face a number of problems in ensuring quality curriculum delivery. Such schools face problems like lack of teachers, inadequate teaching and learning resources as well as poor quality teaching among others. Schools located in remote areas are therefore disadvantaged as far as learning resources are concerned compared to urban areas. The government is working very hard to raise the quality of education and also to expand access yet the scarce resources are limiting this good move. Hence the need to look for an equalizer as far as provision of resources and quality curriculum delivery is concerned. It is visualized that once network connectivity is established in secondary schools, sharing of the said learning resources will make teaching and learning enjoyable as well as help realize set goals in curriculum delivery.

It is against this background that content creation and reuse through a shared LMS to enhance learning is recommended. Focus should therefore be on the development of improved Learning Management System (i-LMS) software that can allow content creation,

storing at a central place, sharing and reuse amongst schools to enhance learning and create uniformity in the content access and delivery.

2. ICT IN THE CLASSROOM

The contemporary perspective of ICTs today in the classroom is teaching with, through or incorporating ICTs as it permits enhanced teaching and learning. It is further denoted as a change in pedagogical practice that uses ICT as a resource, [9]. However [7] argues that the huge educational investment has not produced satisfying evidence of ICT adoption and use in teaching and learning. Further on the same, [10] argue that evidence available suggests that the education sector is investing heavily on ICT but its adoption in the education sector lagged behind the business sector which has picked on technology acceptance and use very well. [6] asserts that the experience of projects failing once project funding is over is common and gives rise to some cynicism. [5] further say one of the shortcomings of using only outcomes-based indicators for quality assurance is that they are often not very useful for improving the (often complex) processes that lead to desirable outcomes. It is however possible to improve delivery through updating and sharing of learning resources available through users of the provided technology which has not been the case today. Such learning resources may be delivered through LMSs.

2.1 Learning Management System (LMS)

According to [17] an LMS is an integrated software that automates administration tracking and reporting of courses or programmes through the following functions; centralized and automated administration; use of self-service and self-guided services; assembling and delivering learning content rapidly; consolidating training initiatives on a scalable web based platform; supporting portability and standards; and personalizing content and enabling knowledge reuse. [1] [5] assert that a brief search of leading journals on research in higher education and national websites responsible for teaching and learning, such as the Higher Education Academy in Great Britain and Educause in America, offers evidence of the frequency of this type of learning situation. The Open University of the UK for example currently uses an LMS, Moodle, for its users in its distance learning programmes and is rated as the second-largest Moodle deployment by user-base. Despite this widespread use, the aspect of content creation and sharing from the learners for improving the delivery of the LMSs in enhancing learning has not come out well.

The concept of Learning Management Systems (LMSs) in the classrooms has been embraced of late as a sure way of introducing technology in the classrooms. They can be server-based or cloud based software programs that mainly contain information about users, courses and content [16]. According to [15] a Learning Management System (LMS) is a software application for the administration, documentation, tracking, reporting and delivery of e-learning education courses or training programs. Further [3] sees an LMS as a software application or web-based technology used to plan, implement and assess a specific learning process. Several surveys are carried out to investigate the factors that are related to the use of computer technology in teaching and learning processes by teachers [4]. However not much has been done focusing on content creation by the learners.

Nonetheless existing LMSs do not seem to have factored in a module for input of data from the user for improvement of the LMS but instead depend on automated captures of user interaction with the systems. Hence data collection and sharing has not fully realized its intended objective of supporting improvement of delivery through the LMS software.

This leaves out a gap that would otherwise have been filled if there was a dependable feedback from the users of the LMSs tailored to collect data that would help assess the usability of the software in question in realizing the intended goals of curriculum delivery as well as add details to stored content for reuse.

This paper therefore focuses on use of LMSs software in the classrooms to create content and upload with an aim to improve delivery through sharing of the same data by schools.

3. PROPOSED METHODOLOGY

3.1 Web 2.0 Tools and Learning

In a research done by [14] there is a host of student and tutor support tools included in the LMS systems. Web 2.0 tools are highly useful in enhanced eLearning for they provide new ways of creating, collaborating, editing and sharing user-generated content online and with ease of use while learning. Tools like blogging, wikis, Googledocs, podcasts, and online photo galleries can be developed and used for the teaching and learning of certain topics in a variety of subject areas. However, the availability and quality of specific tools vary. It was felt there was need for better support and more tools for teamwork and collaboration.

3.2 The Cloud Concept

As an evolving paradigm in data management, cloud computing can be an effective tool if used to store learning content in a centralized database for access. It entails the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. The following framework thus puts into use of the concept of cloud computing in ensuring that teachers and learners from different schools can create, upload and share content in a common platform. This will promote the creation of a resource database for use by all secondary schools as well as uniformity in delivery regardless of distance.

3.3 The i – LMS Model Application

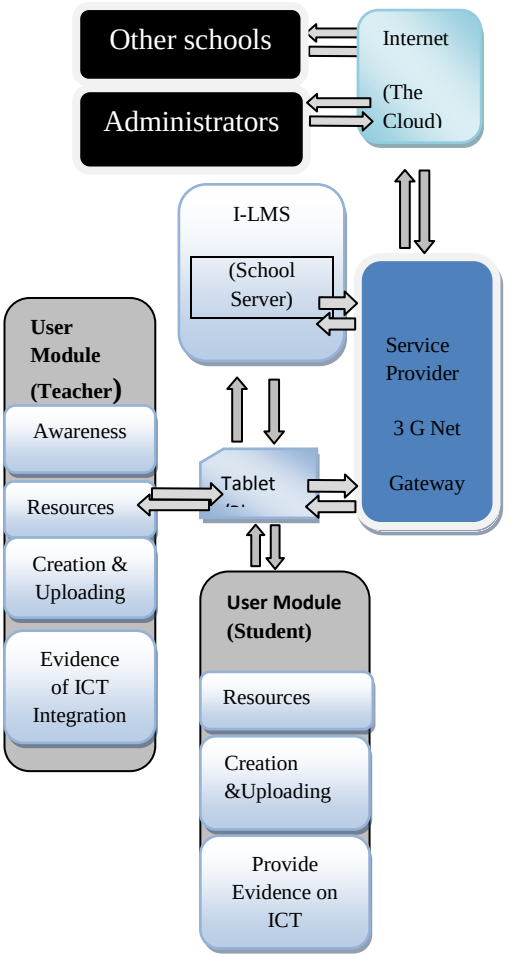


Figure 1: The i - LMS

Table 1: The I-LMS Application

Resources	Communication programs to the users in support of ICT integration in classrooms
Data Access	Application will be designed to use tablets, mobile phones or computers to access data
Content Creation and Uploading	A two way communication to help create and upload content and evidence of ICT integration in the classrooms
Analysis and Summaries	Developed application will provide support for data analysis and generate required summaries from databases in the internet (cloud) using uploaded data.

3.4 Design and Development

3.4.1 Tools

Tools that may be used include, Unified Modeling Language, VB2010, Macromedia studio (Dreamweaver) ASP.NET, PHP, HTML and Xampp server. The proposed tool will be designed using Unified Modeling Language and will allow use of activity diagrams, use case, diagrams and a flowchart. A database will be developed using Xampp and web based application services by PHP and HTML

3.4.2 Components of the Model

The tool will be modeled with three different units. The first unit will be the personal computer (PC) side which will be formed of user interface components, the database and the web server components internet gateway will be setup to run on the server and have access to back-end database server for interactive usage of the tool, user interface and internet front end will also be connected to a back-end. The programs expected in the PC are Web server, a gate way server, internet webpage, database and its platform and user interfacing between the PC and the appliance. To ensure security connection to the webpage will be secured through the server certificate and secure socket layer (SSL) algorithm. In addition a login/password based access will be setup to prevent unauthorized access.

4. CONCLUSION

The Kenyan government is currently doing a project to equip primary schools with laptops for learning. A similar project to equip secondary schools with ICT equipment has been in place for sometime now though not as aggressive as the new one. One major chalenge however remains in the stardadization of content and delivery using the supplied equipment.

This gap can be effectively addressed the discussed cloud computing model which proposes a module to capture and store data that can be used for reuse by students and teachers at their own convenience from various points. This can become a reality especially with the intended supply of electricity to all areas in the country. As well gadgets that can access internet can be purchased at affordable prices by all interested parties. Thus with a common storage in the discussed cloud concept, learning content can be accessed as from anywhere. Developed content as well will be uploaded for sharing in a common repository. This will thus ensure uniformity in content delivered and ease of accessibility by all regardless of the area on is located.

It is therefore recommended that the Kenyan Government should embrace the use of cloud computing to centralise curriculum delivery from a common pool. This will see the implementation of ICT integration in teaching and learning in schools succeed in delivering and sharing same standard content become a reality.

5. ACKNOWLEDGEMENT

Publishing is a requirement in my on-going studies for a masters degree. I would like to acknowledge the good work of moulding me that is being done by Dr W. Cheruiyot of Jomo Kenyatta University of Agriculture and Technology.

6. REFERENCES

[1] Abbas Abdoli Sejzi, B. A. (2013, July 1). Learning Management System (LMS) and Learning Content Management System (LCMS) at Virtual University. *2nd International Seminar on Quality and Affordable Education (ISQAE 2013)*, pp. 216-220. Retrieved from http://educ.utm.my/tl/wp-content/uploads/2013/11/301.pdf

[2] Akbar, F. (2013, October 21). *What affects students acceptance and use of technology?* Retrieved from Dietrich College Honors Theses.: http://repository.cmd.edu/hsshonors/179

[3] Aziah, N., & Marzuki, W. (2005). Innovation for Better Teaching and Learning: Adopting the Learning Management System. *Malaysian Online Journal of Instructional Technology*, 2(2), pp. 27-40.

[4] Baek, Y., Jong, J., & Kim, B. (2008). What makes teachers use of technology in theclassroom? Exploring the factors affecting facilitation of technology with a Korean sample. *Computers and Education*, Vvol.50, no. 8, pp. 224-234.

[5] Ellis, R. A., & Calvo, R. A. (2007). Minimum Indicators to Assure Quality of LMS-supported Blended Learning. *Educational Technology & Society*, , Vol 10 (2), 60-70.

[6] Farrell, G. (2013, October 15). *ICT in Education in Kenya - infoDev*. Retrieved from infoDev:www.infodev.org/en/Document.409.pdf

[7] Gülbahar, Y. (2007). Technology planning: A roadmap to successful technology integration inschools. *Computers & Education*, Vvol. 49, no. 4, pp. 943-956.

[8] Kaur, R., & Sidhu, G. K. (2010). Learner autonomy via Asynchronous Online Interactions: A Malaysian Perspective. *International Journal of Education and Development using Information and Communication Technology*, Vol. 6, Issue 3, pp. 88-100.

[9] Law, N., Pelgrum, W. J., & Plomp, T. ((eds) 2008). *Pedagogy and ICT Use in Schools around the World - Findings from the IEA SITES 2006 Study*. Hong Kong: Springer.

[10] Leidner, D., & Jarvenpaa, S. L. (1995). The use of Information Technology to enhancemanagement school education. A theoretical view. *MIS Quarterly*, pp. 265-291.

[11] Luckin, R., Wilma, C., Graber, R., Kit, L., Mee, A., & Oliver, M. (2009). Do Web 2.0 really open the door to learning? Practices, perceptions and profiles of 11-16 year olds. *Learning, Media and Technology*, Vol (34) 2 87-104.

[12] Martin, F. (2008). Blackboard as the Learning Management System of a Computer Literacy Course. *MERLOT Journal of Online Learning and Teaching*, Vol. 4, No. 2.

[13] Oye, N. D., A.Iahad, N., & Ab.Rahim, N. (2012). Using Mixed method Approachto Understand Acceptance and Usage of ICT in Nigerian Public University. *International Journal of Computers & Technology*, Volume 2 No. 3.

[14] Paulsen, M. F. (2003). Experiences with Learning Management Systems in 113 European Institutions. *Educational Technology & Society*, 6 (4) 134-148.

[15] Ryann, E. K. (2009, 20-06-2013 20). Field Guide to Learning Management Systems. *ASTD Learning Circuits*.

[16] Sharma, A., & Vatta, S. (2013). Role of Learning Management Systems in Education. *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol 3, 6 pg 997-1002.

[17] Suman, N., Chawan, P., & Meshram, B. B. (2011). CMS, LMS and LCMS for e-learning. *International Journal of Computer Science Issues*, Vol 8, Issue 2 , 644.

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 92 - 96, 2015, ISSN:- 2319–8656

Fuzzy Goal Programming Techniques for Production Planning in Industry

A.K. Bhargava
Department of Mathematics,
M.M.H College, Ghaziabad (UP),
Affiliated: C.C.S. University,
Meerut (U.P.) India

S.R. Singh
Department of Mathematics,
D.N. College, Meerut (UP),
Affiliated: C.C.S. University,
Meerut (U.P.) India

Divya Bansal
Institute of Management Studies, Ghaziabad (UP)
(Research Scholar, Banasthali University, Rajasthan, India)

ABSTRACT

This paper presents the production planning problem in industry with different operational constraints, including strategic aim of the company, profit goal, limit on finishing and furnace hours needed, cups manufactured with target values being imprecise in nature. The fuzzy goal programming techniques is applied to maximize the production capacity, maximize the profit, minimize the extra finishing labor and furnace hours, and ensure the manufacturing capacity. The objective of this paper is to elaborate a plan which takes manager's preferences into account. The results illustrate the flexibility of the proposed model by adjusting goal priorities with respect to importance of each objective and the aspiration level with respect to desired target values. LINDO 14.0 optimizer solver is used to draw results of the problem.

Keywords: Goal Programming, Production Planning, Fuzzy Goal Programming, Satisficing.

1. INTRODUCTION

The production planning problems involves objectives as to either maximize profit or minimize cost and is formulated to a single-objective function in linear programming. But in real life there are multiple objectives involved with imprecise target values. In order to design an efficient production planning system, a good understanding of the environment in terms of customers, products and manufacturing processes is a must [16]. Production planning is a complicated task that requires cooperation among multiple functional units in any organization. Therefore, new tools for production planning are required that consider these issues. To achieve this, in this paper, a fuzzy goal programming technique is used to determine optimal production plans.

With fast computational growth [8], both linear and non-linear goal programming can be solved using well-developed software such as Linear Interactive and Discrete Optimization (LINDO, 2011) or meta-heuristics such as simulated annealing, genetic algorithms, tabu search and so on [10].

Goal programming (GP), was developed by Charnes and Cooper [1]. Lee [11] applied the goal programming approach to production planning and then to aggregate production planning. Ghosh et al. [4] presents a goal programming technique for nutrient management by determining the optimum fertilizer combination for rice production. Tamiz et al. [18] have studies the modeling approach of goal programming does not attempt to maximize or minimize the objective function directly as in the case of conventional linear programming. Instead of that the goal programming (GP) model seeks to minimize the deviations between the desired goals and the actual results to be obtained according to the assigned priorities. Dantzig [2, 3] developed linear programming under uncertainty and also provided solution of two-stage linear programs with uncertainty called as the stochastic programming. In stochastic programming, the parameters are random variables with known distribution. The use of fuzzy set theory in GP was first considered by Narasimhan [13, 14, 15], Hannan [5, 6, 7], Ignizio [9]. Rubin and Narsimhan [17] and Tiwari et al. [19, 20] have investigated various aspects of decision problem using FGP. An extensive review of these papers is given by Tiwari et al. in 1985.

2. FUZZY GOAL PROGRAMMING

The simple additive model in conventional GP for m goals $G_i(x)$ with deviational variables d_i^+ , d_i^- is defined as

$$\text{Minimize}\sum_{i=1}^{m}\left(d_i^+ + d_i^-\right)$$

$$d_i^+ \cdot d_i^- = 0,$$

$$d_i^+, d_i^-, x \geq 0, \; i = 1, 2, ..., m,$$

where g_i represents the aspiration level of the i-th goal.

2.1 Fuzzy Goal Programming Model

Now, further consider the FGP problem formulated as:

Find X

To satisfy $G_i(X) \gtrsim g_i, i = 1, 2, ..., m$, (2)

Subject to

$$AX \leq b$$

$$X \geq 0,$$

where X is an n-vector with components $x_1, x_2, ..., x_n$ and $AX \leq b$ are system constraints in vector notation. The symbol '$\gtrsim$'refers to the fuzzification of the aspiration level (i.e., approximately greater than or equal to). The i-th fuzzy goal $G_i(X) \gtrsim g_i$ in (2) signifies that the DM is satisfied even if less than the g_i upto certain tolerance limit is attained. A linear membership function μ_i for the i-th fuzzy goal $G_i(X) \gtrsim g_i$ can be expressed according to Zimmermann [21, 22] as

$$\mu_i = \begin{cases} 1 & if\ G_i(X) \geq g_i \\ \dfrac{G_i(X) - L_i}{g_i - L_i} & if\ L_i \leq G_i(X) \leq g_i \\ 0 & if\ G_i(X) \leq L_i \end{cases} \quad (3)$$

where L_i is the lower tolerance limit for the fuzzy goal $G_i(X)$. In case of the goal $G_i(X)$ ˆ g_i, the membership function is defined as

Subject to $G_i(x) + d_i^- - d_i^+ = g$

$$\mu_i = \begin{cases} 1 & if\ G_i(X) \leq g_i \\ \dfrac{U_i - G_i(X)}{U_i - g_i} & if\ g_i \leq G_i(X) \leq U_i \\ 0 & if\ G_i(X) \geq U_i \end{cases} \quad (4)$$

where U_i is the upper tolerance limit.

The additive model of the FGP problem (2) is formulated by adding the membership functions together as

$$\text{Maximize } V(\mu) = \sum_{i=1}^{m_1} \mu_i + \sum_{j=m_2}^{m} \mu_j$$

Subject to

$$\mu_i = \frac{G_i(X) - L_i}{g_i - L_i}$$

$$\mu_j = \frac{U_j - G_j(X)}{U_j - g_j}$$

$$AX \leq b,$$

$$\mu_i, \mu_j \leq 1; i = 1, 2, ..., m_1, \; j = m_1, ..., \text{m},$$

$$X, \mu_i, \mu_j \geq 0, i = 1, 2, ..., m_1, \; j = m_1, ..., \text{m},$$

(5)

where $V(\mu)$ is called the fuzzy achievement function or fuzzy decision function.

The weighted additive model is widely used in GP and multiobjective optimization techniques to reflect the relative importance of the goals/objectives. In this approach the DM assigns differential weights as coefficients of the individual terms in the simple additive fuzzy achievement function to reflect their relative importance, i.e., the objective function is formulated by multiplying each together. This leads to the following formulation, corresponding to (4):

$$\text{Maximize } V(\mu) = \sum_{i=1}^{m_1} w_i \mu_i + \sum_{j=m_2}^{m} w_j \mu_j$$

Subject to

$$\mu_i = \frac{G_i(X) - L_i}{g_i - L_i},$$

$$\mu_j = \frac{U_j - G_j(X)}{U_j - g_j}$$

$$AX \le b,$$

$$\mu_i, \mu_j \le 1; i = 1, 2, ..., m_1, j = m_1, ..., m,$$

$$X, \mu_i, \mu_j \ge 0, i = 1, 2, ..., m_1, j = m_1, ..., m, \quad (6)$$

where w_i is the relative weight of the i-th fuzzy goal, w_j is the relative weight of the j-th fuzzy goal.

3. PRODUCTION PLANNING PROBLEM

Let us consider a problem proposed by Jones and Tamiz (2010) where a company produces three types of cups, termed grade A, grade B and grade C. Each grade A cup requires 2 hr of furnace time and 3 hr of finishing labor. Each grade B cup requires 3 hr of furnace time and 5 hr of finishing labor. Each grade C cup requires 4 hr of furnace time and 10 hr of finishing labor. A grade A cups yields a profit of £1.00, a grade B cup a profit of £1.50, and a grade C cup a profit of £2.20. The company currently has 1000 hr of furnace time and 2000 hr of finishing labor per day. They have a high level of demand and therefore they have a strategic aim of increasing production to 1000 cups per day by increasing the level of furnace and finishing hours available. The company wants to achieve the following goals:

Goal 1: Achieve the strategic aim of 1000 cups per day.

Goal 2: Achieve a profit of at least £1250.

Goal 3: Minimize the extra finishing and furnace hours needed.

Goal 4: Ensure that at least 300 of each type of cup is manufactured.

with the relative preference weights attached to all the goals as given below in Table 1:

Table 1: Preference weight

S. No.	Goal	Preference weight
1.	Achieve the strategic aim of 1000 cups per day	5.0
2.	Achieve a profit of at least £1250	3.0
3.	Minimize the extra finishing and furnace hours needed	2.0
4.	Ensure that at least 300 of each type of cup is manufactured	1.0

Assuming these goals to be fuzzy in nature, let the tolerance limit of four goals be (800, 1100, 2550, 5200, 280, 265, 260).

4. FORMULATION OF THE PROBLEM

Let

x_1 = Number of cups of grade A produced per day

x_2 = Number of cups of grade B produced per day

x_3 = Number of cups of grade C produced per day

Goals:

(i) Strategic aim of the company:

The company has the strategic aim of achieving 1000 cups per day which is assumed fuzzy in nature with the tolerance limit of 800 cups per day.

$$x_1 + x_2 + x_3 \gtrsim 1000 \quad (7)$$

(ii) Profit goal:

The company desires to achieve a profit of at least £1250 with the tolerance limit of £1100.

$$x_1 + 1.5x_2 + 2.2x_3 \gtrsim 1250 \quad (8)$$

(iii) Limit on finishing and furnace hours needed:

The company wants to limit the finishing and furnace hours to 1000 hours of furnace time and 2000 hours of finishing labor per day with the tolerance limit of 2550 and 5200, respectively.

$$2x_1 + 3x_2 + 4x_3 \lesssim 1000 \quad (9)$$

$$3x_1 + 5x_2 + 10x_3 \lesssim 2000 \quad (10)$$

(iv) Cups manufactured:

Company desires to manufacture at least 300 of each type of cup, again, assumed to be fuzzy in nature with the tolerance limit of (280, 265, 260).

$$x_1 \gtrsim 300 \quad (11)$$

$$x_2 \gtrsim 300 \quad (12)$$

$$x_3 \gtrsim 300 \quad (13)$$

4.1. Fuzzy Goal Programming Problem is formulated as:

$$Maximize \ \frac{5}{11}\mu_1 + \frac{3}{11}\mu_2 + \frac{2}{11}(\mu_3 + \mu_4) + \frac{1}{11}(\mu_5 + \mu_6 + \mu_7)$$

Subject to

$$\mu_1 = \frac{(x_1 + x_2 + x_3) - 800}{1000 - 800}$$
$$\mu_2 = \frac{(x_1 + 1.5x_2 + 2.2x_3) - 1100}{1250 - 1100}$$
$$\mu_3 = \frac{2550 - (2x_1 + 3x_2 + 4x_3)}{2550 - 1000}$$
$$\mu_4 = \frac{5200 - (3x_1 + 5x_2 + 10x_3)}{5200 - 2000}$$
$$\mu_5 = \frac{x_1 - 280}{300 - 280}$$
$$\mu_6 = \frac{x_2 - 265}{300 - 265}$$
$$\mu_7 = \frac{x_3 - 260}{300 - 260}$$

$x_i, \mu_j \geq 0$ (i = 1, 2, 3 ; j = 1, 2,...,7)

$0 \leq \mu_j \leq 1$ (14)

4.2. Computational Results

Using the data presented, the proposed weighted fuzzy goal programming model is tested using LINDO [12] software package and the results are shown in Table 2:

$x_1 = 280.5, x_2 = 265, x_3 = 260$

$\mu_1 = 0.0275, \mu_2 = 1, \mu_3 = 0.099,$

$\mu_4 = 0.135, \mu_5 = 0.025, \mu_6 = 0, \mu_7 = 0.$

Table 2: Interpretation of the Results

Goal	Description	Fuzzy Target Level	Satisfied	Achieved Value
1	Strategic aim	Tolerance limit of 800	Partial	805.5 ($x_1 + x_2 + x_3$)
2	Profit	Tolerance limit of 1100	Yes	1250
3	Minimize extra finishing and furnace hours	Tolerance limit of 2550 Tolerance limit of 5200	Partial Partial	2396 4766.5
4	No. of cups manufactured	A – Tolerance limit of 280 B – Tolerance limit of 265 C – Tolerance limit of 260	Partial Partial Partial	280.5 265 260

5. CONCLUSION

In this paper, we have solved the production planning problem through the weighted fuzzy goal programming (WFGP) technique representing the relative importance of each goal. Two major objectives with imprecise target values are optimized through fuzzy goal programming. The goals are relatively balanced by different goal programming variants. The similar technique could be used for short-term and intermediate production planning in other continuous process industries. The number of fuzzy goals can be increased based on the decision maker's desirability.

REFERENCES

[1] Charnes, A. and Cooper, W. W. 1961. Management Models and Industrial Application of Linear Programming. Vol. I, John Wiley & Sons, Inc., New York.

[2] Dantzig, G. B. 1955. Linear programming under uncertainty, Management Science, 1, 197-206.

[3] Dantzig, G. B. and Mandansky, A. 1961. On the solution of two-stage linear programs under uncertainty, In I. J. Neyman, Editor, Proc. 4th Berkeley Symp. Math. Stat. Prob., 165-176.

[4] Ghosh, D., Sharma, D. K. and Mattison, D. M. 2005. Goal programming formulation in nutrient management for rice production in West Bengal. International Journal of Production Economics, 95, 1–17.

[5] Hannan, E. L. 1981. Linear programming with multiple fuzzy goals. Fuzzy sets and Systems, 6, 235–248.

[6] Hannan, E. L. 1981. On fuzzy goal programming, Decision Sci., 12, 522–531.

[7] Hannan, E. L. 1982. Contrasting fuzzy goal programming and fuzzy multicriteria programming. Decision Sci., 13, 337–339.

[8] Ignizio, J. P. 1983. A note on computational methods in lexicographic linear goal programming. Journal of the Operational Research Society, 34 (6), 539–542.

[9] Ignizio, J. P. 1982. On the (re)discovery of fuzzy goal programming. Decision Sci., 13, 331–336.

[10] Jones, D. and Tamiz., M. 2010. Practical Goal Programming. Springer.

[11] Lee, S. M. 1972. Goal Programming for Decision Analysis. 1st ed. Auerbach Publishers Inc., Philadelphia.

[12] LINDO System, Inc. 2011. LINGO Optimization Modeling Language (User Manual), Chicago, IL.

[13] Narasimhan, R. 1980. Goal programming in a fuzzy environment. Decision Sci., 11, 325–336.

[14] Narasimhan, R. 1981. On fuzzy goal programming–Some comments. Decision Sci., 12, 532–538.

[15] Narasimhan, R. 1982. A geometric averaging procedure for constructing supertransitive approximation to binary comparison matrices. Fuzzy Sets and Systems, 8, 53–61.

[16] Olhager, J. and Wikner, J. 2000. Production planning and control tools. Production Planning and Control, 11(3), 210–222.

[17] Rubin, P. A. and Narasimhan, R. 1984. Fuzzy goal programming with nested priorities. Fuzzy Sets and Systems, 14, 115–129.

[18] Tamiz, M., Jones, D. and Romero, C. 1998. Goal programming for decision making: An overview of the current state-of-the-art. European Journal of Operational Research, 111, 569–581.

[19] Tiwari, R. N., Dharmar, S. and Rao, J. R. 1986. Priority structure in fuzzy goal programming. Fuzzy Sets and Systems, 19, 251–259.

[20] Tiwari, R. N., Rao, J. R. and Dharmar, S. 1985. Some aspects of fuzzy goal programming. International Symposium on Mathematical Modelling of Ecological Environmental and Biological Systems, Kanpur, India.

[21] Zimmermann, H.-J. 1976. Description and optimization of fuzzy systems, International. J. General Systems, 2, 209–215.

[22] Zimmermann, H.-J. 1978. Fuzzy programming and linear programming with several objective functions, Fuzzy Sets and Systems, 1, 45–55.

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 92 - 97, 2015, ISSN:- 2319–8656

The Critical Technological Factors OF E-Government in Kenya

Godfrey Kyalo Makau,
Department of Business and Social Sciences,
Jomo Kenyatta University of Agriculture & Technology (JKUAT)
Nairobi, Kenya

Elijah, I. Omwenga
Department of computer Science, School of Computing and Informatics,
University of Nairobi,
Nairobi, Kenya

Njihia James Muranga
Department of Management Science, School of Business
University of Nairobi,
Nairobi, Kenya

Abstract: EGovernment and innovation can provide significant opportunities to transform public administration into an instrument of sustainable development. However, the rate of failure of eGovernment projects in the developing world, and specifically Africa, has raised questions on the critical factors contributing to their success or failure. The general lack of comprehensive information concerning eGovernment project performance status and the critical technological factors influencing it in Kenya also necessitated this study. To answer this question, this study aimed at assessing the critical technological factors of eGovernment projects performance in Kenya. The study targeted all the 18 eGovernment projects in place implemented through the Communications Authority (CA) of Kenya. The results are based on response from 217 respondents who consisted of 52 eGovernment project implementers and 165 eGovernment service consumers. The study found that of the technological predictors of eGovernment, only system integration, processes and usage of eGovernment system emerged to have positive significant relationships with project performance in Kenya. Other factors including information technology standards, security issue, privacy issue, cooperation or collaboration, eGovernment portal availability, eGovernment portal access, and various computer usages also had positive but insignificant relationships with eGovernment project performance and hence not critical in influencing to eGovernment project performance in Kenya.

Keywords: eGovernment, Projects, Critical, Technological, Factors, Performance

1. INTRODUCTION

1.1 Background of the Study

We According to the UN (2014), eGovernment is basically defined as the use of ICT and its application by the government for the provision of information and public services to the people. More broadly, it can be referred to as the use and application of information technologies in public administration to streamline and integrate workflows and processes, to effectively manage data and information, enhance public service delivery, as well as expand communication channels for engagement and empowerment of people. The opportunities offered by the digital development of recent years, whether through online services, big data, social media, mobile apps, or cloud computing, are expanding the way we look at eGovernment. While eGovernment still includes electronic interactions of three types—i.e. government-to-government (G2G); government-to-business (G2B); and government-to-consumer (G2C)—a more holistic and multi-stakeholder approach is taking shape.

Governments have paid more attention to eGovernment in the last two decades, with central focus on its adoption. While the current UN (2014) survey indicates that eGovernment has been adopted by all the 193 UN global member states examined for online service provision, majority remain at the low or intermediate levels of eGovernment development, termed emerging and enhanced stages in the United Nations four stage online service model (UN, 2014). In addition, the regional representation mirrors those of past surveys, with a majority of 64 per cent (16 countries) from Europe, 20 per cent (5 countries) from Asia, 8 per cent (2 countries) from Americas and 8 per cent (2 countries) from Oceania. None of the African countries belongs to the top 25 ranks. Progress in Africa remains relatively slow and uneven with limitations in ICT infrastructure and human capacity posing the greatest challenge (UN, 2014).Therefore, hidden behind the massive adoption is the shocking fact that most eGovernment projects, especially in the African and developing countries have ended up failing (Heeks and Bailur, 2007). EGovernment is a multifaceted concept presented in three perspectives: technological, organisational and environmental perspectives (Oliveira and Martins, 2011).

Empirical studies have concluded that eGovernments in the developing African countries face numerous technological difficulties and hence the need for more home-grown studies to bridge the existing knowledge gaps (Ahmad, et al, 2012). Therefore, from a technological perspective, eGovernment refers to the use of information and communication technologies (ICT) -such as Wide Area Networks, the Internet, and mobile computing -by government agencies in provision of services (Cordella & Bonina, 2012). Based on this conceptualisation, eGovernment project's success or failure mainly depends on its ICT characteristics.

Technology is a prerequisite for e-government roll out and yet its adoption remains a major challenge for developed as well as developing countries. When developing an eGovernment system, ICT infrastructure in form of computers and other telecommunication hardware and software plays a bedrock role (Barker, 2011). Benefits such as efficiency, electronic service delivery and cost-effective services in the public sector due to adoption of eGovernment, cannot be fully achieved if there is a technical barrier.

Therefore, addressing technical barrier need to incorporate several elements, from hardware to software; in addition to other components, such as the Internet, web-technologies, telecommunication, networks connectivity and capacity,

databases, hardware equipment, software applications, design and interoperability (Basu,2004). ICT that shapes e-government also requires a properly aligned ICT strategy, satisfying system attributes, information/data management, and regulatory framework (Baker, 2011). It is in line with this background that this study sought to assess the technological determinants of eGovernment.

1.2 Statement of the Problem

In Kenya, just like in other developing nations, a myriad of technological challenges have been identified as influencing the successful implementation, adoption and use of eGovernment. Kenya is currently ranked number 119 globally, retaining same reanking since 2012 survey. However, in African countries ranking, it declined from number 7 (UN, 2012) to number 9 (UN, 2014). This saw Kenya ranked second in the East African Community after Rwanda in terms of their E-Government Development Index (UN, 2014). Despite their dismal in eGovernance, African governments support eGovernment and appreciate its contribution to the government agenda (Mutula, 2008).

The realization that for eGovernment projects in developing and transitional countries, 35% were total failures, 50% were partial failures and only 15% were successful (Heeks, 2003;Schedler and Schmidt, 2004), has drawn focus to unravelling the factors affecting success of eGovernment projects in the developing world. This study sought to answer this question by assessing the technological critical factors influencing performance of eGovernment projects in Kenya.

1.3 Objectives of the Study

1. To determine the technological factors influencing performance of eGovernment in Kenya.

2. To assess the nature of relationships between the technological factors and eGovernment performance.

2. LITERATURE REVIEW

Generally, many researchers have confirmed a positive relationship between the quantity and quality of ICT infrastructure and eGovernment Adoption, use, and hence successful eGovernment performance (Klischewski and Scholl, 2008). The perceived ICT availability, usefulness, compatibility, relative advantage, image, and complexity among other attributes can enhance or impede eGovernment project success (Ahmad, 2012). Specifically, there are many components and elements involved from hardware to software; in addition to other components, such as technology standards, eGovernment Portal and Access, security and privacy, ICT Strategy, infrastructure, Information/Data Management, and ICT Regulatory framework, design and interoperability (Al-Sobhi et al, 2010).

Ahmad et al. (2012), found that Technology standards can either impede or promote collaborative efforts between government agencies. They also found that the more complex and transformational eGovernment developments, the more integration is required among internal and external applications for success. The success of online services in eGovernment also depends on eGovernment Portal and Access that is in place for services rendered by the government (Schware and Deane, 2003). Heeks (2003), found that the more secure and privacy guaranteeing the systems are, the higher the confidentiality assurance and consequently the more the usage and successful eGovernment implementation outcome. The success of e-government is also directly related to the quality of ICT infrastructure, the telecommunication network infrastructure and their capacity, reliability and affordability (Basu, 2004). Lack of or poor ICT strategy, layout design and technical interoperability has been also found to influence eGovernment projects performance (Ahmad, 2012). Lack of technical skills, complexity, and difficulties in using eGovernment systems have been found to directly influence eGovernment performance (Gil-García and Pardo, 2005). Effort expectancy, which is defined as the degree of ease associated with the use of the system (Venkatesh et al., 2003) is the construct coined to accommodate all user difficulties. Three constructs make up the concept: perceived complexity, and ease of use. Schaper and Pervan (2007), found that effort expectancy has a significant influence on intention to use behavior and eGovernment success.

3. METHODOLOGY

3.1 Research Design

A cross-sectional descriptive research design was employed in this study. This is because descriptive research describes data and characteristics about the population or phenomenon being studied (Rohillo, 2010). It was therefore most appropriate for this study since the study aimed at analysing and describing the critical technological factors affecting eGovernment in Kenya. The study was however cross-sectional since data was collected at one particular time across all the existing eGovernment projects and both internal project environment (project implementers) and external environment (e-service consumers) respondents (Schurink, 2009).

3.2 Target Population

The study targeted all the 18 eGovernment projects that had been in place since 2005 and which were implemented through the Directorate of eGovernment (but now renamed CA) in Kenya government. The respondents therefore included all the eGovernment project implementers and eGovernment service consumers of the eGovernment services in Kenya.

3.3 Data Collection

The study collected both primary and secondary data. Primary data were collected using survey questionnaires supplemented with interviews and observations where necessary and possible. Secondary data sources included journals, books and articles addressing the objectives of this study.

3.4 Operationalization of Variables

This study employed quantitative measures using a 4-point likert scale and also qualitative measures as advocated by Agresti (2002). The operationalization and measurements of the variables in this study is as shown in Table 1 below.

Table 1. Operationalization and measurements of the variables

THE TECHNOLOGICAL FACTORS INFLUENCING EGOVERNMENT PROJECT IMPLEMENTATION, ADOPTION, & E-SERVICE USE IN KENYA		
Construct	**Construct Domains**	**Measures**
Technological Factors	ICT strategy	4-point likert
	ICT standards	
	National ICT infrastructure	
	ICT architecture interoperability	
	ICT security	
	ICT quality	
	ICT compatibility and interoperability	
	Linkages and communication among stakeholders	
	eGovernment system security and privacy	
	eGovernment system integration	
	eGovernment portal and access	
	eGovernment Project attributes.	

3.5 Data Analysis

Data analysis was performed at both descriptive and inferential statistical analysis levels using a mixture of tools available in SPSS. They include content analysis for the open ended questions; correlations and factors analysis through use of contingency tables; and logistic regression analysis. Descriptive statistics involved use of frequency tables, percentages and charts and other measures of variable associations (De Vaus, 2001). Inferential statistics included the Wald statistic, Odds Ratio, Pvalues, -2Log Likelihood size, and Nagelkerke R^2 values (Field, 2009; Saunders et al., 2003).

4. RESULTS AND DISCUSSIONS

The results are based on responses from the 217 respondents out of the 300 who participated (72% response rate). Of the 217 respondents, 52 were eGovernment project implementers while 165 were eGovernment service consumers.

4.1 The Technological Factors Influencing eGovernment Projects Implementation, Adoption and E-service Use (Success and Failure) in Kenya

Eight statements on four point likert scale were used to assess the technological factors affecting egovernment project implementation. The parameters that were measured include: Information Technology standards; Security issue; Privacy issue; System Integration; Cooperation or Collaboration; EGovernment portal availability; EGovernment portal access; and, Processes.The results are as shown in table 2 below.

Table 2.Technological Factors Descriptive Analysis Results

		Strongly disagree	Disagree	Agree	Strongly agree
Information Technology standards	All ICT assets are standard in terms of quality, compatibility and interoperability thereby enabling smooth linkages and communication among all eGovernment stakeholders	13%	40%	37%	10%
Security issue	There are enough computer security measures to secure personal data on the eGovernment systems.	6%	55%	29%	10%
Privacy issue	There is enough assurance of privacy and confidentiality on the eGovernment systems.	18%	40%	30%	12%
System integration	The eGovernment system is well integrated across different platforms to provide a full and real 'one stop shop' for dealing with the Kenya Government.	12%	43%	31%	14%
Cooperation or Collaboration	All stakeholders and government agencies are positively contributing to successful e-projects implementation	10%	27%	43%	20%
EGovernment portal availability	The Kenya government Portal is available and accessible all the time.	12%	43%	35%	10%
EGovernment portal access	Any Kenyan can use the government Portal to for payments any time.	23%	33%	37%	8%
Processes	EGovernment has caused positive changes to the entire process thereby significantly accelerating process execution (from a few minutes to a couple of seconds)	8%	18%	61%	14%

4.2 Test of Associations and Factor Analysis

The study sought to establish the specific factors predicting eGovernment projects performance from the collected data through tests of associations. This was achieved through correlations and factor analysis. The composite variables emerging from factors analysis were then used in regression analysis, presentation, interpretation and discussions of the outcomes.

The goal of factor analysis was to reduce "the dimensionality of the original space and to give an interpretation to the new space, spanned by a reduced number of factors (Darlington, 2004). Guttman-Kaiser rule was applied in retaining only the factors whose eigenvalues were larger than 1 and in total accounted for over 0.5 of the variance (Field 2000). Therefore, items with variance loadings of over 0.6 were retained for further analysis as recommended by Rietveld & Van Hout (1993).

Correlation Results

The results from correlations showed that most of the eight items including security issue, privacy issue, cooperation or collaboration, eGovernment portal availability,

eGovernment portal access,and processes correlated well with most of other items. However, information technology standards did not and hence was therefore eliminated and the rest used in running factor analysis.

Factor Analysis Results

The table 3 below shows the eigenvalues associated with each linear component (factor) before extraction and after extraction. In the end, the system retained all the items within one significant factor considered to significantly affect eGovernment implementation, adoption and use in the research. With only one factor extracted, there was no rotation conducted. The extracted components had Eigenvalue accounting for 57.480% of the variance explained. This figure being above the threshold of 50%, it indicates that the one-component factor model derived from the analysis fitted the data appropriately.

Table 3. Technological Factors Total Variance Explained Results

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.024	57.480	57.480	4.024	57.480	57.480
2	.997	14.238	71.718			
3	.625	8.928	80.646			
4	.463	6.621	87.267			
5	.411	5.871	93.138			
6	.261	3.731	96.869			
7	.219	3.131	100.000			

Extraction Method: Principal Component Analysis.

Items loading of over 0.6 for the component combined to form the one principal component with the variables clustering as shown in table 4 below. The cronbach alpha analysis for the new component reliability (0.875) also confirms internal consistency among all the derived technological factors therein. Therefore, the seven items are declared to belong to the technological dimension variable.

Table 4. Technological Factors Component Matrix Results

	Component
	1
Security issue	.818
Privacy issue	.810
System integration	.738
Cooperation or Collaboration	.760
EGovernment portal availability	.793
EGovernment portal access	.763
Processes	.605
Cronbach's Alpha	**.875**

Extraction Method: Principal Component Analysis.
a. 1 components extracted.

4.3 Correlation Between Technological Factors and Project Performance

This was performed to determine the critical technological factors predicting eGovernment project performance in Kenya from the many proposed in the model. The table 5 below displays the correlations output. From the results, only system integration, processes and usage of eGovernemnt system emerged to have positive significant relationships with project performance hence declared critical at this stage and reserved for entry into the logistic regression model. However, Information Technology standards, Security issue, Privacy issue, Cooperation or Collaboration, eGovernment portal availability and eGovernment portal access, emerged to have also positive but insignificant relationships with project performance and hence dropped at this stage.These findings concur with those of Ahmad et al. (2012),who found that the more complex and transformational eGovernment develops, the more integration is required among internal and external applications for success. They also support Gil-García and Pardo, (2005) findings that lack of technical skills, complexity, and difficulties in using eGovernment systems (processes) directly influence eGovernment performance. They support the fact that transformation and re-engineering of government processes and activities must be embraced for successful eGovernment (Basu, 2004). However, the findings contradict that of Ahmad et al. (2012), who found that technology standards can either impede or promote collaborative efforts between government agencies and that lack of or poor ICT strategy, layout design and technical interoperability influence eGovernment projects performance. They also contradict Heeks (2003) finding that the more secure and privacy guaranteeing the systems are, the higher the confidentiality assurance and consequently the more the usage and successful eGovernment implementation outcome. These results are as shown in tables 5 and 6 below.

Table 5 Correlation BetweenTechnical Factors and Project Performance

		Information Technology standards	Security issue	Privacy issue	System integration	Cooperation or Collaboration	EGovernment portal availability	EGovernment portal access	Processes
Project performance	Pearson Correlation	.029	.230	.237	.398**	.245	.129	.284	.356*
	Sig. (2-tailed)	.847	.124	.118	.006	.101	.393	.053	.015
	N	47	46	45	46	46	46	47	46

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 6 Correlation Between ICT Usage and Project Performance

		Computer usage in performing business tasks	Computer usage in browsing, emailing, downloading and uploading information	Computer usage in buying things online, e-commerce and e-business	Computer usage in interacting with the government, downloading and uploading information government information	Usage of Kenya's eGovernment system
Project performance	Pearson Correlation	-.027	-.022	.047	.138	.189**
	Sig. (2-tailed)	.716	.760	.523	.058	.009
	N	188	194	185	188	191

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

4.4 Regression Analysis

In this study, regression analysis was necessary to assess the model Goodness of fit, R and R^2. Logistic regression was used and therefore interpretation of the results was based on the

Wald statistics, Odds Ratios, Pvalues, -2Log Likelihood sizes, and Nagelkerke R^2 values, which is generated in SPSS output (Field (2009). While the correlations outputs showed that there existed seven technological factors influencing eGovernment projects performance, regression analysis was necessary to go further in determining the critical ones among them that may need keen attention on the minimum to ensure success. Univariate logistic regression procedure was therefore performed to predict the probability that a participant would give his/her eGovernment project a success performance judgment (rating) given mere presence of or other behaviour attributes of the factor(s) considered.

Given the base rates of the two e-government project performance options (success=1 and failure=0), the system correctly grouped 62.2% of the respondents cases as having reported success of e-government project with only 37.8% of the cases reporting failure of e-government project based on the project performance characteristics alone. This finding contradicts the Heeks (2003) and Schedler and Schmidt (2004) study findings that eGovernment projects in developing and transitional countries are 35% total failures, 50% partial failures and only 15% were successful.

By testing the effect of each technological factor entered in the model, the results show that the 2 Log Likelihood function would drop by 6.589 if a single unit of the model technological factor (X_1) was added to the model (which already has the intercept) and the drop was highly significant (Pvalue = 0.010). Table 7 below shows the block1 outputs where the SPSS added Technological Factors (X_1) as the predictor. Omnibus Tests of Model Coefficients gave a Chi-Square of 7.076 on 1 df which was significant as the P-value (.008) was less than 5% (.05). This is a test of the null hypothesis that adding the independent variable to the model did not significantly increase the likelihood of the respondents to give an eGovernment project a success outcome judgment when it is correctly so. A positive and significant Chi-Square statistic indicates that there was a positive relationship between X_1 and the eGovernment project success performance.

Table 7 Omnibus Tests of the Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	7.076	1	.008
	Block	7.076	1	.008
	Model	7.076	1	.008

Under Model Summary printed in table 8 below, the -2 Log Likelihood statistics of 52.591, measures how poorly or well the model predicts the judgment decisions. The figure is small and smaller the statistic the better the model. The Cox & Snell R^2 can be interpreted like R^2 in a multiple regression although it does not reach a maximum value of 1. A value of .146 therefore implies that only 14.6% variation in the dependent variable is explained by the model. The study used the alternative, the Nagelkerke R^2 whose output of 0.198 indicates that a larger figure of 19.8% in the dependent variable is explained by the model.

Table 8 Model Goodness of Fit Tests Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	52.591[a]	.146	.198

a. Estimation terminated at iteration number 4 because parameter estimates changed by less than .001.

Table 9 below shows the Hosmer-Lemeshow statistic, which tests the null hypothesis that there is a linear relationship between the predictor variable and the log odds of the outcome variable. A chi-square statistic was then computed comparing the observed frequencies with those expected under the linear model. A non-significant chi-square indicates that there exists a linear relationship and therefore the data fits the model well (Pvalue = 0.808).

Table 9 Hosmer and LemeshowLinearity Test

Step	Chi-square	df	Sig.
1	3.003	6	.808

From Table 10 results, it is noted that overall success rate in classification has improves from 62.2%to 73.3% (11.1% contribution/prediction power) after adding the independent variable.

Table 10 Classification for the Final model

			Predicted		
			Project judgment		Percentage Correct
	Observed		Yes	No	
Step 1	Project judgment	Yes	22	6	78.6
		No	6	11	64.7
	Overall Percentage				73.3

a. The cut value is .500

Table 11 below shows the Regression Coefficients and Odds Ratio. The Wald Chi-Square statistic, which tests the unique contribution of each predictor, holding other predictors constant is also given. The output indicates that the predictor X_1 relationship with the outcome meets the conventional .05 standard for statistical significance. It's 2.565 odds ratio statistic indicates that the chances of eGovernment project success judgment are increased by more than double for each one point increase in respondent's exposure to or interaction with eGovernment project Technological Factors and the increase is highly significant (Pvalue =.016).

Table 11 Variables in the Model Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	X1	.942	.390	5.835	1	.016	2.565
	Constant	-3.458	1.305	7.024	1	.008	.032

a. Variable(s) entered on step 1: X1.

5. CONCLUSIONS

For the eight technological factors included in the models, seven of them (security issue, privacy issue, cooperation or collaboration, eGovernment portal availability, eGovernment portal access, and processes) emerged to fit well within the technological factors domain with Cronbach's Alpha above the 0.06 cut off. Only information technology standards stood on its own contradicting previous grouping of the factors within the technological factors domain.

In this study, only system integration, processes and usage of eGovernemnt system emerged to have positive significant relationships with project performance. Therefore, the three are the only critical technological factors predicting eGovernment projects performance in Kenya. The rest

including information technology standards,security issue,privacy issue, cooperation or collaboration, eGovernment portal availability, eGovernment portal access, and various computer usages emerged to have also positive but insignificant relationships with project performance and deemed less important in predicting eGovernment projects performance in Kenya.

6. RECOMMENDATIONS

Based on good practices from around the world, and the literatures reviewed in the study, effective e-government development depends on not only organizational and other environmental dimension factors, but also a robust ICT backbone. The UN(2014) survey also emphasise the need for proper national ICT policy and e-government strategy, backed by robust ICT infrastructure, adequate human capital and online service delivery, as of critical importance to the development of effective e-government for a sustainable and desirable future in the developing world.

Project implementers and e-service users in Kenya should therefore concentrate in managing the above highlighted critical technological factors because they determine eGovernment project implementation, adoption and use and hence eventual performance outcomes in Kenya. Researchers should conduct further studies in other settings and involving larger samples of eGovernment project stakeholders in order to explore all critical factors within the developing world contexts. This is very necessary because the current study only focussed on technological factors only. The critical environmental and organisational factors need to be highlighted too. These three dimensions have been noted to contain the factors behind the high failure rates of eGovernment projects in developing nations.

7. REFERENCES

[1] Agresti, A. (2002). *Categorical Data Analysis* (2nd Edition ed.). RW: Mee.

[2] Ahmad, M. O. Markkula, J. and Oivo, M. (2012). *Factors Influencing the Adoption of eGovernment Services in Pakistan.* Paper presented at the Proceedings of the 9th European, Mediterranean and Middle Eastern Conference on Information Systems, Munich, Germany.

[3] Barker, J. (2011). The technology–organization–environment framework. In Information Systems Theory: Explaining and Predicting our Digital Society (Dwivedi, Y., Wade, M. and Schneberger, S. Eds.), pp. 231-246, Springer, New York.

[4] Basu, S. (2004). E-government and developing countries: an overview. *International Review of Law, Computers & Technology, 18*, 109-132.

[5] De Vaus, D. A. (2001). *Research design in social research* London: SAGE.

[6] Gil-Garcìa, J. R., & Pardo, T. A. (2005). E-government success factors: Mapping practical tools to theoretical foundations. *Government Information Quarterly, 22*, 187-216.

[7] Heeks, & Bailur, S. (2007). Analyzing e-government research: Perspectives, philosophies, theories, methods, and practice. *Government Information Quarterly, 24*, 243-265.

[8] Heeks. (2003). Most egovernment-for-development projects fail: how can risks be reduced? : Institute for Development Policy and Management.

[9] Klischewski, R., & Scholl, H. J. (2008). Information quality as capstone in negotiating e-overnment integration, interoperation and information sharing. *Government, an International Journal, 5*, 203-225.

[10] Mutula, S. M. (2008). Africa's e-government status with developed and transitional nations. *Information Management & Computer Security 16* (3), 235-250.

[11] Oliveira, T., & Martins, M., F. . (2011). Literature Review of Information Technology Adoption Models at Firm Level. *The Electronic Journal Information Systems Evaluation 14*(1), pp110- 121.

[12] Rohillo Pradeep (2010). *Research Methodology*. APH Publishing Corporation. New Delhi.

[13] Saunders, M., Lewis, P., & Thornhill, A. (2003). *Research methods for business students* (3rd edition ed.). Harlow: Prentice Hall.

[14] Schaper, L. K., & Pervan, G. P. (2007). ICT and OTs: A model of information and communication technology acceptance and utilisation by occupational therapists. *International Journal of Medical Informatics, 76*, 212-221.

[15] Schedler, K., & Schmidt, B. (2004). Managing the e-government organization. *International Public Management Review* 1-20

[16] Schurink, E. (2009). Qualitative Research Design as Tool for Trustworthy Research. *The Journal of Public Administration*, 44 (4.2) 803-823.

[17] Schware, R., & Deane, A. (2003). Deploying e-government programs: The strategic importance of I before e. *Info, 5*(4), 10-19.

[18] UN. (2012). United Nations E-government Survey 2012. Retrieved Accessed: 03 May, 2012 http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf

[19] UN. (2014). United Nations E-government Survey 2014. Retrieved Accessed: 10 January, 2014 http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf

[20] Venkatesh, Morris, M., Davis, G., & Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly, 27*, 425-478.

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 103 - 107, 2015, ISSN:- 2319–8656

Malware Hunter: Building an Intrusion Detection System (IDS) to Neutralize Botnet Attacks

R. Kannan
Department of Computer Science
Sri Ramakrishna Mission Vidyalaya
College of Arts and Science
Coimbatore ,Tamilnadu,India.

A.V.Ramani
Department of Computer Science
Sri Ramakrishna Mission Vidyalaya
College of Arts and Science
Coimbatore ,Tamilnadu,India

Abstract: Among the various forms of malware attacks such as Denial of service, Sniffer, Buffer overflows are the most dreaded threats to computer networks. These attacks are known as botnet attacks and self-propagating in nature and act as an agent or user interface to control the computers which they attack. In the process of controlling a malware, Bot header(s) use a program to control remote systems through internet with the help of zombie systems. Botnets are collection of compromised computers (Bots) which are remotely controlled by its originator (Bot-Master) under a common Command-and-Control (C&C) structure. A server commands to the bot and botnet and receives the reports from the bot. The bots use Trojan horses and subsequently communicate with a central server using IRC. Botnet employs different techniques like Honeypot, communication protocols (e.g. HTTP and DNS) to intrude in new systems in different stages of their lifecycle. Therefore, identifying the botnets has become very challenging; because the botnets are upgrading their methods periodically for affecting the networks. Here, the focus on addressing the botnet detection problem in an Enterprise Network

This research introduces novel Solution to mitigate the malicious activities of Botnet attacks through the Principle of component analysis of each traffic data, measurement and countermeasure selection mechanism called Malware Hunter. This system is built on attack graph-based analytical models based on classification process and reconfigurable through update solutions to virtual network-based countermeasures.

Key words: IRC, IDS, Anomaly, Countermeasure, Denial of Service.

1. INTRODUCTION

Network security consists of the requirements and policies adopted by a network administrator to prevent and monitor various forms of intrusion and attacks on services obtained via Net[2]. To access the data over network, an efficient authentication is needed which is provided and verified by the administrators. The user gets user identification and password to get access to the targeted network. The network security encompasses all types of networks including private ones[9]. All types of transactions whether public or private such as government services, business activities etc need security for their data and other resources of a computer network. The Network security system secures and protects the net based resources. The proposed framework leverages hierarchical models to build a monitoring and control process to classify the network traffic data to the virtual machine to significantly improve attack detection and mitigate attack consequences[8].

1.1 Problem Definition:

Data and Network security is one of most important area that has attracted a lot of research and development effort in recent times, particularly, in the area of cloud data protection. The vital information of all types have to be secured against attackers to prevent from exploring the vulnerabilities of a cloud system and prevent them from compromising the virtual machines by deploying a large-scale Distributed Denial-of-Service (DDoS) system. DDoS attacks usually involve early stage actions such as multistep exploitation, scanning, and convert the virtual machines and do attacks through the compromised machine (zombies) which have been taken over by botmasters to hide from detection. In the cloud also, i.e IaaS cloud[2], the detection is difficult in case of attack with novel characteristics. This is because cloud users may have installed vulnerable applications on their virtual machines.

1.2 Botnet

A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be of any type such as taking control of an Internet Relay Chat (IRC) channel or sending of spam mail or participation in DDoS attacks. Botnet is a name constructed by joining the terms robot and network[3][4].

There are many types of attacks and detection systems with the malware help. The classification of attacks are as given below

- In DDoS attacks, various sources submit multiple requests to a single Internet based accessible point and overload it with fake request and prevent the point from accessing needed data For instance if a phone number which tries to connect to internet[1][9]
- Adware intrusion hides the original advertisements with fake ones on web pages
- Spyware is software which sends information to its creators about the activities of the users. Compromised systems exist in an establishment network can be useful since they possess information useful for the

organization. The valuable data are stolen by these spywares and misused by the intruders

- E-mail spam contain advertisements and malicious contents.
- When a false web traffic is generated for some gain it is called Click fraud [9].
- Fast flux is a DoS attack the botnet uses to hide the phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies.
- Brute is way of making remote machine services such as FTP,
- Worms. The botnet focuses on recruiting other hosts.
- Scare ware is software that is marketed by exploiting the fear of users. This kind of scare ware make the attacked computer as a bot and induce the user to buy a rogue anti-virus to regain access to their computer.[9]

An intrusion detection system (IDS) is an application program that monitors network and system functioning for malicious activities or policy violations and produces reports to a server which supervises it. Various methods are adopted to detect traffic which are suspicious in nature. Generally the IDS are classified in to two, namely Network based detection system (NIDS) and host based detection systems (HIDS). The Intrusion detection and prevention systems (IDPS) concentrate on identifying possible incidents of logging information about them and inform the attack attempts.

Types of Intrusion Detection system

1) Network Intrusion Detection Systems:

Network Intrusion Detection Systems (NIDS) are placed at a strategic point or points i.e in between the server to which the system connected and to the Internet. It analyses the traffic and matches the traffic that is passed on the subnets to the library of earlier attacks. On finding the attack it alerts the administrator[2][3].

2) Host Intrusion Detection Systems

Host Intrusion Detection Systems (HIDS) run on individual hosts or devices connected to network. A Host Intrusion Detection Systems scans the data and will alert the user or administrator of suspicious activity is detected. It compares the existing system files with the earlier files. If any mismatch is found it alerts the administrator. The example of the Host Intrusion Detection Systems are useful in the mission critical machines that are not expected to change their configuration. The HIDS (*Host Intrusion Detection Systems*) can be customised to the specific needs of systems.

Statistical Detection Techniques used in Intrusion Detection System

A. Statistical anomaly-based IDS

An Intrusion Detection System (IDS) which is structured on anomaly will monitor network traffic and compare it with standards. The Intrusion Detection System will find the deviations from the standards for the network and other parameters such as protocol, bandwidth and allied devices and alert the administrator or user when traffic is detected which is anomalous or different to significant level than the preset standard. However there is a possibility for False alerts even for a legitimate use of bandwidth if the baselines are not intelligently configured.[2]

B. Signature-based IDS

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from identified threats. This kind of antivirus program detects malwares in this way only. The real problem is identifying the fresh threats and the signature for detecting that threat being applied to Intrusion Detection System.
Hence identifying new threats will be a problem [4] in this method of detection.

Problem Objective:

However, all the above threats fall in to the category of Botnet. This study proposes a new solution to mitigate the malicious activities of botnet attacks through a detection mechanism and gives a strategy for counter. To prevent attack on virtual machines which exist in the cloud, a multistage distributed attack detection system through the Principle of component analysis of each traffic data, measurement and countermeasure selection mechanism called Malware Hunter. This system is built on attack graph-based analytical models based on classification process and reconfigurable through update solutions to virtual network-based countermeasures. The proposed framework leverages hierarchical models to build a monitoring system and control process to classify the network traffic data to the virtual machine to significantly improve attack detection and to eliminate risk.

2. SURVEY OF LITERATURE

2.1. Detection of Spam Zombies

This study focuses on compromising of the machines which is one of the key security threats on the Internet. This technique is used in preventing various forms of security attack. The attack of spamming provides an economic incentive for attackers to recruit the large number of compromised machines, here the aim is to focus on the detection of the compromised machines in a network that send spam, which are called as spam zombies. The development of a good spam zombie detection procedure named SPOT by monitoring outgoing messages from network. SPOT is system designed and named based on a powerful statistical tool Sequential Probability Ratio Test. Additionally, the performance evaluation of SPOT using a two-month e-mail trace.

The evaluation studies show that SPOT is an effective and efficient system in automatically detecting compromised machines. For instance, among the given IP addresses which were observed in tracing e-mails, SPOT identified more than one quarter were connected to bots. Of these bots except very few could be confirmed independently and these few were with possibility for attack. Further the SPOT failed to detect only seven machines in the process of tracing. In fact SPOT out performed, other two detection

algorithms which used the method of comparing number and percentage of spam messages enter, efficiently.

2.2. Detecting Malware Infection through IDS-driven Dialog Correlation

In this study, a new kind of "Network perimeter monitoring strategy", was used to check the correspondence during the period of an infected system. Monitoring system is process developed to track the two-way communication flows between internal assets and external systems that match a state-based modeled on sequence of infection. It consists of a correlation engine that is driven by three malware-focused "network packet sensors", to find malware infection in various forms and activities and to prevent attacks on external systems

The Monitoring system finds such internal external system links and indicates that there is an infection in the local computer(s). The Monitoring system matches infection dialog model with actual infection, generates a report and lists out the relevant events and event sources that played a role in the infection process. The method of analytical strategy matches the flow of correspondence between the intra and the Internet. This contrasts the strategy to other intrusion detection and alert methods. Here the results are given using Monitoring system in both virtual and live testing environments and discuss our Internet release of the Monitoring system prototype. The monitoring system is made available for operational use and to help stimulate research in understanding the life cycle of malware infections.

2.3. Scalable, graph-based network vulnerability analysis

Well secured networks are also vulnerable frequently due to constant innovation by attackers. New combinations of exploits are innovative ways through which attackers do attacks. The researchers forth a multiple graph-based algorithms in the form of trees/graph attacks. The proposed trees/graphs consider all possible types of attacks to penetrate in to a system or network, using previous exploits also.

The latest approach uses a modified version of the model checker NuSMV as a powerful inference engine for chaining together network exploits, already happened. In this study the researchers argued that the method gave more data than actual need for analysis and its ability to handle bigger size of networks and they proposed a representation compact size and scalable.

They claimed that it was possible to produce attack trees from their representation with even more information for bigger networks, even when they if they do not go through attack tree. The claim of them stated that attacker can bypass backtracking. This assumption eliminated the need for analysis at higher level unnecessarily and made larger network within the reach of analysis.

2.4. MulVAL(Multivalue): A Logic- Based Network Security Analyzer

This study determines the security impact software vulnerabilities on a particular network, and considers interactions among multiple network elements. For a useful vulnerability analysis tool there are two factors to be taken in to consideration namely, the ability to integrate the given vulnerability specifications automatically from bug-reporters and the scalability with larger networks. They proposed to develop MulVAL, a overall framework to conduct the analysis of vulnerability on multiple hosts and multiple stages on networks. The MulVAL adopts Data log as the modeling language for the elements in the analysis in specification of bugs, describes the configuration defines rules for reasoning to find malware, getting permission of OS and provide model for privileges etc. They leveraged the vulnerability-database existed and scanned tools by expressing their output in Data log and feeding it to their MulVAL reasoning engine. The collection of information helps to analyze in a shorter span of time even for larger networks.

2.5. Scalable Optimal Countermeasure Selection Using Implicit Enumeration on Attack Countermeasure Trees

The constraints, on the basis of investment cost on security preclude a security decision maker from implementing all possible measures to counter. Present security optimization strategies based on analytical model do not prevail for the following reasons:

(i) No method provides an optimal security solution in the absence of probability assignments to the model.

(ii) When size of network grows, the efficiency of the tool decreases

(iii) The methods which follow attack trees (AT) normally do not allow for the inclusion of countermeasures On the other hand the non-state-space model (e.g., attack response tree) responses are modified in to state-space model and cause state-space explosion.

This researcher proposes a new AT paradigm and named it attack countermeasure tree (ACT) whose structure takes into account attacks as well as countermeasures (in the form of detection and mitigating attack events). They used techniques of branch and bound, greedy method etc to study multiple objective functions with goals such as minimizing the number of countermeasures, the cost of security of ACT and maximizing the benefit from implementing a certain countermeasure set in the ACT under various constraints. They formed every problem of optimization as an integer programming problem which also allowed them to find optimal solution even in the absence of probability assignments to the model. Their method of scales suited for larger ACTs and they compared its efficiency with other approaches.

3. METHODOLOGY

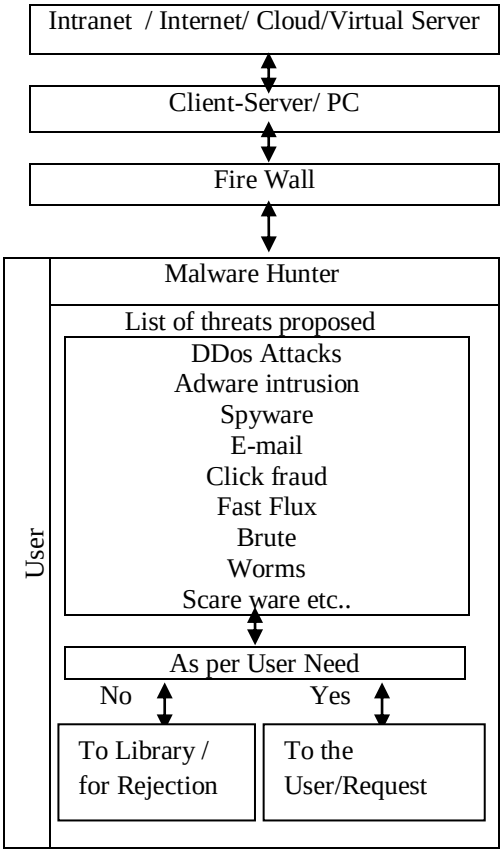


Fig 1: Architecture Diagram of the Malware Hunter Establishment of a Host and Network layer to monitor the Network

Host based intrusion detection [3] system is modeled to capture the attack to the host through monitoring and prediction process. In fig 2, the architecture for the proposed security model has been shown.

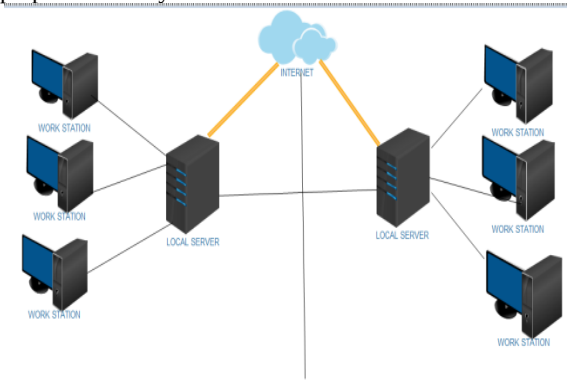


Fig: 2 Architecture of Network Based Intrusion Detection System (IDS)

Threats faced by the applications can be categorized based on the goals and purposes of the attacks. A through exposure to the forms and purposes of threats put a person in an advantageous position in detecting the threats and neutralize them.

The properties of attack and Identification of various forms of attack.

- Network performance is abnormally slow (when files are opened or access to web sites)[9]
- Non availability of access to a given web site
- Inability to access any web site
- Increase in count of the number of spam emails received—(this type of DoS attack is considered an e-mail bomb)
- Frequent Disconnection to Internet
- Denial of Internet access to the Net[10].

Denial-of-service attacks can also lead to problems in the network 'branches' around the target computer. For instance, if a router of a LAN and Internet is attacked, it may compromise all the computers connected to the Network. In case of larger scale attacks, Networks at regional level may be infected, irrespective of the intention of the attackers.

Procedure 1: Reading the File through Buffer Reader

Step 1: Start
Step 2: Create a File
Step 3: Copying the File & then it will compare with each node & Reading the List.
Step 4: Condition is checked, it's true it will attach the file in to buffer reader.
Step 5: If it's False then copy the file into Buffer.
Step 6: File will be monitored.

Procedure 2: Reading and Writing a file in Buffer

Step 1: Start
Step 2: Create a File
Step 3: Copying the File, Then it will compare with each node & reading the list
Step 4: Condition is checked, it is true it will attach the file into buffer writer
Step 5: If it's false, then malware type will be stored in buffer writer

Formatting the threat forms

Novel threats in the network and host system is difficult to identify due to the changing strategy of attackers. An efficient novel attack detection system has the characteristics of each event (i.e., the pockets of IP / the TCP connection) such as payload strings and induction of conditional rules which have a very low probability of being violated shall be framed[3][4].

Learning Rules for anomaly detection

1. We extend the network traffic model to include needed quantum of attributes and payload application.
2. We introduce a non-stationary model, in which the event probability (an attribute having some value) depends on the time of its most recent happening.
3. We introduce an efficient algorithm for selecting good rules for anomaly detection from a rule space that is exponentially large in the number of attributes.

4. RESULT AND ANALYSIS

The system against botnet and DOS attacks which are shown below. Most of the attacks shown with some evidence, so here the results are simplified and report the detections.

It illustrates how to dynamically add malware behaviors. In each system call concerned, we set up needed checkpoints and each of these check points is responsible for checking the behaviors belonging to the same operation with the support of a modifiable behavior list in memory.

The performance results provide us a benchmark for the given hardware setup and shows how much traffic can be handled by using a single detection area. Construction of a distributed model to scale up to a data center-level IDS is needed.

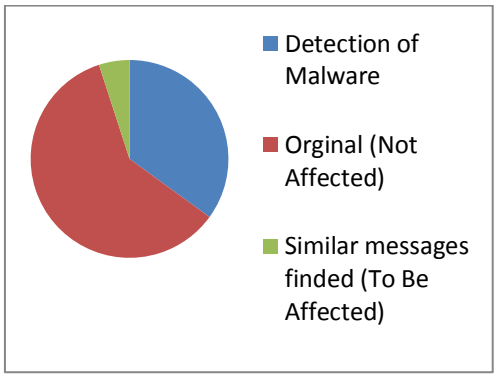


Fig 3: Detection Accuracy of the Malware Hunter Data Recovery process

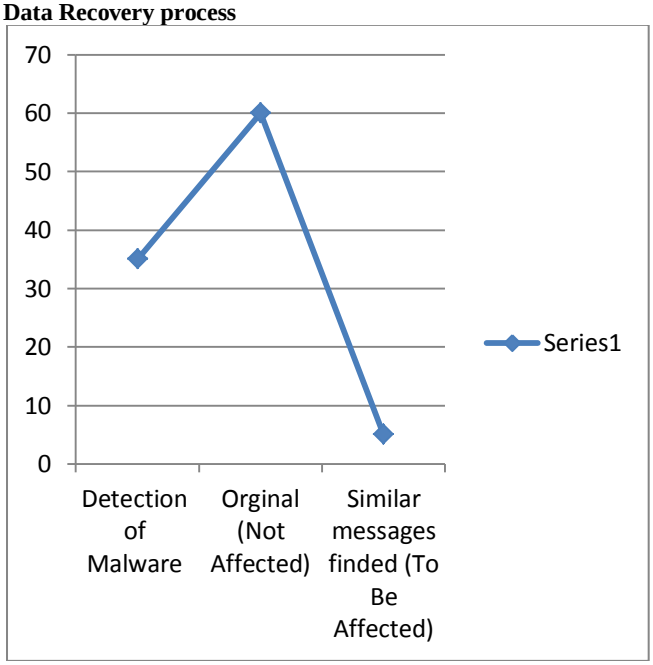


Fig 4: Rate of data recovery

5. CONCLUSION

The results show that the Detection of Accuracy of the Malware hunter in multiphase distributed vulnerability detection through the Principle of component analysis. Each traffic data is under the dynamic attack evolution capacity and countermeasure selection mechanism called Malware Hunter which uses graph-based analytical model for its formation, uses the classification and reconfigurable process against update solutions to virtual network-based counter measures. The classification is done using the principle component analysis to establish the efficient detection mechanism against various types of attacks. The modeling parameters have been constructed for attack detection solutions of botnet attacks. The framework proposed provides hierarchical models to build a monitor and control process to classify the network traffic data to the virtual machine to significantly improve attack detection and mitigate attack consequences. Hence malware hunter achieves the good detection performance against all types of network and host based intrusion evolving.

6. ACKNOWLEDGMENT

I would like to express my deep thankful to Dr.A.V.RAMANI, M.Sc.M.PhIl.Ph.D Head & Guide, Department of Computer Science, Sri Ramakrishna Mission Vidyalaya college of Arts and Science, Coimbatore for his valuable guidance and encouragement throughout the paper and providing necessary facilities to this work.

7. REFERENCES

[1] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, “Detecting Spam Zombies by Monitoring Outgoing Messages,” IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198-210, Apr. 2012.

[2] NICE: Network Intrusion Detection and Countermeasure selection in Virtual Network Systems, Ritika Saroha and Sunita, International Journal of Computer Science Engineering and Technology(IJCSET) | May 2014 | Vol 4, Issue 5,158-160, ISSN : 2231- 0711

[3] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, “BotHunter: Detecting Malware Infection through IDS-driven Dialog Correlation,” Proc. 16th USENIX Security Symp. (SS ’07), pp. 12:1-12:16, Aug. 2007.

[4] G. Gu, J. Zhang, and W. Lee, “BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic,” Proc. 15th Ann. Network and Distributed Sytem Security Symp. (NDSS ’08), Feb. 2008.

[5] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, “Automated Generation and Analysis of Attack Graphs,” Proc. IEEE Symp. Security and Privacy, pp. 273-284, 2002,

[6] “NuSMV: A New Symbolic Model Checker,” http://afrodite.itc. it:1024/nusmv. Aug. 2012. R. Sadoddin and A. Ghorbani, “Alert Correlation Survey: Framework and Techniques,” Proc. ACM Int’l Conf. Privacy, Security and Trust: Bridge the Gap between PST Technologies and Business Services (PST ’06), pp. 37:1-37:10, 2006.

[7] L. Wang, A. Liu, and S. Jajodia, “Using Attack Graphs for Correlating, Hypothesizing, and Predicting Intrusion Alerts,” Computer Comm., vol. 29, no. 15, pp. 2917-2933, Sept. 2006.

[8] S. Roschke, F. Cheng, and C. Meinel, “A New Alert Correlation Algorithm Based on Attack Graph,” Proc. Fourth Int’l Conf. Computational Intelligence in Security for Information Systems, pp. 58-67, 2011.

[9] M. Frigault and L. Wang, “Measuring Network Security UsingBayesian Network-Based Attack Graphs,” Proc. IEEE 32nd Ann.Int’l Conf. Computer Software and Applications (COMPSAC ’08),pp. 698-703, Aug. 2008.

[10] K. Kwon, S. Ahn, and J. Chung, “Network Security ManagementUsing ARP Spoofing,” Proc. Int’l Conf. Computational Science and ItsApplications (ICCSA ’04), pp. 142-149, 2004.

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 108 - 119, 2015, ISSN:- 2319–8656

A Study of Approaches and Measures aimed at Securing Biometric Fingerprint Templates in Verification and Identification Systems

Joseph Mwema
SCIT
Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

Stephen Kimani
SCIT
Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

Michael Kimwele
SCIT
Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

Abstract: The need for fool proof authentication procedures away from traditional authentication mechanisms like passwords, security PINS has led to the advent of biometric authentication in information systems. Biometric data extracted from physiological features of a person including but not limited to fingerprints, palm prints, face or retina for purpose of verification & identification is saved as biometric templates. The inception of biometrics in access control systems has not been without its own hitches & like other systems it has its fair share of challenges. Biometric fingerprints being the most mature of all biometric spheres are the most widely adopted biometric authentication systems. Biometric systems effectiveness lies on how secure they are at preventing inadvertent disclosure of biometric templates in an information system's archive. This however has not been the case as biometric templates have been fraudulently accessed to gain unauthorized access in identification and verification systems. In order to achieve strong and secure biometric systems, biometric systems developers need to build biometric systems that properly secure biometric templates. Several biometric template protection schemes and approaches have been proposed and used to safeguard stored biometric templates. Despite there being various biometric template protection schemes and approaches in existence, none of them has provided the most authentic, reliable, efficient and deterrent means to totally secure biometric fingerprint templates. This research sought to establish status of the current biometric template protection techniques and methods by conducting a survey and analyzing data gathered from a sample of seventy-eight (78) respondents. We will report these results and give our conclusion based on findings of the survey in this paper.

Keywords: Biometrics; Fingerprints; Templates; Security; Encryption; Unimodal Biometric Systems

1. INTRODUCTION

The advent of increased security threats in information systems and need to guarantee unbeatable systems security has enticed system designers & developers to incorporate use of passwords, PINs and access codes for system users' authorization. Unfortunately these have not provided the most needed security and have been hacked or obtained illegally as emphasized by [1].System designers & developers went further and considered use of biometrics in design of systems' verification and identification procedures. Tan in [2] showed that use of biometric authentication schemes is more efficient over traditional password based access control methods. Statistics however show that biometric systems have not been known to be impervious to hacks and there are several known possible attacks on biometric systems which have rendered them insufficient in providing water tight security as is evidenced by [3].

Biometrics is the automatic identification of a person's physiological or behavioral patterns or traits. Biometric patterns captured from a person are saved as biometric templates. Ahmad et al [4] caution that 'security of biometric templates in a biometric system' as one of the technical issues and challenges regarding use of biometric systems.

This research will study schemes and approaches aimed at securing biometric fingerprint templates in biometric authentication systems, report data results and findings from respondents who were surveyed from a selected sample of seventy-eight (78) respondents picked from a study population of biometric system developers.

The objectives of this research work are:

- To review existing biometric fingerprint template protection schemes and approaches.
- To determine strengths and drawbacks of existing biometric fingerprint template protection methods.
- To identify what are the best practices for securing fingerprint templates in unimodal biometric systems.
- To establish what features would an ideal unimodal biometric fingerprint template protection scheme have.

2. EXISTING BIOMETRIC TEMPLATE PROTECTION SCHEMES & APPROACHES

Jain et al in [15] categorized biometric template protection schemes into *Feature Transformation* and *Biometric Encryption.* The existing biometric template protection schemes and approaches currently in use usually fall into these two categories. We discuss Bio-hashing, Cancellable biometrics, Fuzzy vault, Fuzzy commitment and Watermarking.

2.1 Bio-Hashing

Bio-hashing is a biometric template protection approach in which features from a biometric template are transformed using a transformation function defined by a password or a key known only to the user [5]. This key or password needs to

be securely stored and remembered by the user for subsequent authentication. The key or password used by user in bio-hashing increases entropy of biometric template which further deters adversary attacks. Direct mixing of pseudo-random number (which is kept secret) and biometric data is used to compute a binarized key of 80-bits key with a 0.93% false rejection rate of the system [6]. This generated physical token can be used in smartcard or USB tokens as shown by [5] thus fostering more security than passwords or PINs where controlled levels of access are required.

2.2 Cancellable biometrics

Unlike passwords, PINs and access codes, biometric templates can never be replaced with newer ones if compromised. To circumvent this challenge cancellable biometrics was introduced where biometric templates can be cancelled and replaced [7]. Cancellable biometrics scheme is an intentional and systematic repeatable distortion of biometric template data with the purpose of protecting it under transformational-based biometric template protection. In the concept of cancellable transformation, a transformed template can be cancelled and re-issued by changing transformation parameters if misplaced [8].

2.3 Fuzzy vault

Fuzzy vault is a cryptographic construct that was first proposed by Jules and Sudan in [9] where secret information is encrypted and decrypted securely using a fuzzy unordered set of genuine points and haff points. Geetika & Kaur described a biometric fuzzy vault as a biometric cryptosystem used for protecting private keys and releasing them only when the legitimate users enter their biometric data [10] while Deshpande & Joshi defined a fuzzy vault as a scheme utilized for secure binding of randomly generated key with extracted biometric features [11].

2.4 Fuzzy commitment

Fuzzy Commitment is a biometric cryptosystem which is used to secure biometrics traits represented in binary vector [12]. Jeny & Jangid further described a fuzzy commitment scheme as one where a uniformly random key of length 1 bits is generated and used to exclusively index an n-bit codeword of suitable error correcting code where the sketch extracted from the biometric template is stored in a database.

2.5 Watermarking

The aim of watermarking is to use biometric fingerprint templates as a 'message' to be embedded in a robust watermarking application like copyright protection in order to enable biometric recognition after the extraction of the watermark. In a biometric watermarking scheme, if an attacker tries to replace or forge the biometric template then he must have the knowledge of pixel values where watermark information is hidden as evidenced in [13].

3. RESEARCH METHODOLOGY

3.1 Research Design

This research adopted survey research design because it is extensive thus ensuring we could get an accurate sample from the target population in which to gather targeted results and be able to draw conclusions and findings. Survey research is flexible for online surveys as well as for collecting data for later analysis. The study largely employed Quantitative research approach to compute results and Qualitative research approach where descriptive and broad understanding was required in questions asked to respondents.

3.2 Study Population

The target population in this research constituted of all biometric software developers who currently are in the roles of developing biometric software systems or integrating biometrics into information systems and persons who work or have worked as biometric systems developers in biometric projects in Kenya. We used LinkedIn the social networking site for professionals to draw our target study population.

3.3 Sampling Technique and Sample Size

This research employed simple random sampling. We chose to use this method over other random sampling methods because it provisioned for an equal likelihood of a biometric software developer from the study population being included. Individuals have the same probability of being chosen at any stage in a simple random sampling process as evidenced by [14]. We chose a sample size of seventy-eight (78) biometric systems developers as respondents from the target population.

3.4 Research Instrument and Data Analysis Tools

Online Questionnaires were selected because they enabled us to collect standardized data from biometric systems developers in LinkedIn. Questionnaires gather data that is ready for later statistical analysis of responses. Questionnaires were tailored to capture data pertinent to the research's objective and research questions. This study used Statistical Package for Social Sciences (SPSS) software for data analysis and interpretation.

4. DATA ANALYSIS AND DISCUSSION

Questions in the Questionnaires were open ended and closed ended. Closed ended questions were comprehensive and equally exclusive to avoid ambiguity of collected data in scenarios of non-conforming select options of the questions presented to respondents. Questionnaire used in the study comprised of these (4) sections: Biometric System Developer's Background, Biometric Templates Security, Efficiency of Encryption Methods and Biometric Templates Security Challenges.

4.1 Biometric System Developers' Background

Biometric system developers' particulars and relevant data based on their experience with biometrics systems were captured in this section. These details included age, years of experience as biometric systems developers, type of biometric systems developed, if they had undertaken studies in biometric systems development, knowledge in data encryption and what their thoughts were on impediments preventing wide scale adoption of biometrics.

4.1.1 Respondents' Age

Data collected had the following statistics for ages of the respondents. The age 20 years and below had 0(0%) entries, 3(3.8%) of the respondents were between *21-25* years, The age 26-30 years had 27(34.6%) respondents. 21 (26.9%) respondents were in the age bracket 31-35 years and 27 (34.6%) were of age 35 years and above. This data is shown in Table 1 below.

Table 1. Statistics of Respondents Age

Age of respondents in years	No. of Respondents	No. of Respondents in percentage (%)
21 - 25	3	3.8%
26 - 30	27	34.6%
31 - 35	21	26.9%
35 and above	27	34.6%
Total	**78**	**100.0%**

4.1.2 Respondents' Experience as Biometric Systems Developers

From the data collected, 52 (66.7%) of the respondents had 1-5 years of experience as biometric systems developers, 19 (24.4%) had experience of 6-10 years. While only 5 (6.4%) respondents had 11-15 years of experience, only 2 (2.6%) had an experience of 16 years and above. This data is shown in details in Table 2.

Table 2. Statistics of Respondents Experience as Biometric Systems Developers

Experience in years as a Biometric Systems Developer	No. of Respondents	No of respondents in percentage (%)
1 - 5 years	52	66.7%
6 - 10 years	19	24.4%
11 - 15 years	5	6.4%
16 years and above	2	2.6%
Total	**78**	**100.0%**

4.1.3 Type of Biometric Systems Developed

Data collected indicated 64(82.1%) of respondents had experience developing *fingerprint systems*, 43(55.1%) had developed *face recognition systems* while 16 (20.5%) had been developing *iris systems*. A further 14 (17.9%) had experience in developing *voice recognition systems* and 7 (9.0%) had been developing palm *vein recognition systems*. 12 (15.4%) of respondents had experience developing other biometric systems which included *online signature*, *finger vein* and *score level fusion of face and fingerprints*. This data is shown in Table 3 and Table 4.

Data results showing where respondents develop more than one type of biometric system is shown in Table 4. From the data results in Table 4, the most developed biometric systems by the sampled respondents are fingerprints & face biometric systems being developed by 32(41.0%) of the sampled respondents.

Table 4. Statistics of Type of Biometric Systems Developed

Type of Biometric Systems Developed	No. of Respondents	Total No. of Respondents	No of Respondents in percentage (%)
Fingerprint	64	78	82.1%
Face	43	78	55.1%
Iris	16	78	20.5%
Voice	14	78	17.9%
Palm Vein Recognition	7	78	9.0%
Other(s)	12	78	15.4%
Total		**78**	**100.0%**

4.1.4 Respondents who have studied about Biometric Systems Development

Data collected revealed that 46 (59.0%) of respondents had undertaken studies or a course in biometric systems development while 32(41.0%) were active biometric systems developers without having had any particular training in the field. These statistics were tabulated in Table 5.

Table 5. Statistics of Respondents who have studied Biometric Systems Development

Studied Biometric Systems Development	No. of Respondents	No of respondents in percentage (%)
Yes	46	59.0%
No	32	41.0%
Total	**78**	**100.0%**

Table 3. Statistics of Respondents who Develop One or More Biometric Systems

Biometric Systems Developed by Respondents	No. of Respondents	No. of respondents in percentage (%)
Face	3	3.8%
Face, Iris	4	5.1%
Face, Palm Vein Recognition	1	1.3%
Face, Score level fusion of face and fingerprint	1	1.3%
Face, Voice	1	1.3%
Fingerprints	4	5.1%
Fingerprints, Face	32	41.0%
Fingerprints, Face, Iris, Palm Vein Recognition	1	1.3%
Fingerprints, Finger vein	1	1.3%
Fingerprints, Iris	10	12.8%
Fingerprints, Palm Vein Recognition	6	7.7%
Fingerprints, Voice	10	12.8%
Iris	1	1.3%
Iris, Voice	1	1.3%
Voice	1	1.3%
Voice, online signature	1	1.3%
Total	**78**	**100.0%**

4.1.5 Respondents' Experience in Data Encryption

Respondents' knowledge in data encryption was captured during data collection to determine their level of expertise in securing data with encryption & prevent adversary attacks on archived data.

Table 6. Statistics of Respondents Knowledge in Data Encryption

Respondents Knowledge in Data Encryption	Score Level Weights	No. of Respondents	No. of Respondents in Percentage (%)
Excellent	5	14	17.9%
Above Average	4	31	39.7%
Average	3	28	35.9%
Poor	2	5	6.4%
Very Poor	1	0	0.0%
	Mean=3.63	**Total =78**	**Total =100.0%**

Respondents' knowledge in data encryption as shown above in Table 6. illustrated that 14(17.9%) of respondents considered there knowledge in data encryption as *excellent*, 31(39.7%) respondents ranked *above average* while 28(35.9%) respondents data encryption knowledge was ranked as *poor*. None of the respondents in the data collected thought their data encryption skills fared *very poorly*. The overall mean for the rankings of respondents' data encryption knowledge was 3.63 which is slightly more than average tending to above average and a good pointer that biometric developers are keen on security of data.

4.1.6 Impediments towards wide scale adoption of Biometric Systems

From data collected, impediments preventing wide scale adoption of biometric systems, *high costs of biometric hardware & software* was the main reason identified by respondents at 53(67.9%) followed by 41(52.6%) of respondents who cited *lack of expertise to develop, implement & support biometric systems*. 31(39.7%) of respondents were of the opinion that *accuracy of biometric identification systems* was a contributing factor while *big data size of biometric templates* and *known security flaws* were singled out by 15(19.2%) and 10(12.8%) of respondents respectively. Other impeding factors identified by the remainder of 18 (23.1%) of respondents were *verification & identification time, low bandwidth because of the big size of biometric data, users' unwillingness to give out their biometric data alluding security concerns and trust*. This data is presented in Table 7.

Table 7. Statistics of Impediments that delay wide scale adoption of Biometric Systems

Impediments Towards Wide Scale Adoption of Biometric Systems	No. of Respondents	Total No. of Respondents	No. of Respondents in Percentage (%)
High Costs of Biometric Hardware & Software	53	78	67.9%
Known Security Flaws	10	78	12.8%
Lack of Expertise to Develop, Implement & Support Biometrics Systems	41	78	52.6%
Accuracy (False Acceptance Rate and False Rejection Rate)	31	78	39.7%
Big data size of Biometric Templates in storage space	15	78	19.2%
Other(s)	18	78	23.1%
Total		**78**	**100.0%**

4.2 Biometric Templates Security

This section sought to discover preferred area of storage for biometric templates, determine whether there are measures to protect biometric templates, ascertain if there are policies in place that emphasize on securing of biometric templates in storage, then identify which biometric template protection techniques & methods are used and finally find out from respondents which biometric encryption schemes they used.

4.2.1 Biometric Templates Storage Space

Identifying the preferred storage space for biometric templates among the respondents was of importance to us so that we could identify which parts of biometric template storage space are likely to be attacked by hackers and this study sought to determine the storage space used by respondents to save biometric templates in biometric systems. Table 8 below shows results from study as follows; 55(70.5%) of respondents saved their biometric templates in *databases* while only 1(1.3%) of respondents saved biometric templates in *USB modules*. 7(9.0%) of respondents chose *folders* and 10(12.8%) of respondents preferred *smart cards*. The remainder 5(6.4%) of respondents who identified *other* places listed the following storage places; *encrypted databases* and *a combination of both databases and smartcards*.

Table 8. Statistics of where Respondents save Biometric Templates

Biometric Templates Storage Space	No. of Respondents	No. of Respondents Percentage (%)
Folders	7	9.0%
Databases	55	70.5%
Smart cards	10	12.8%
USB Modules	1	1.3%
Other(s)	5	6.4%
Total	**78**	**100.0%**

4.2.2 Respondents who have measures in place aimed at Protecting Biometric Templates

We sought to determine if there were any measures aimed at protecting biometric templates from the sampled respondents and this study showed that 66(84.6%) of respondents had measures in place while 12(15.4%) of respondents did not. These results are shown in Table 9.

Table 9. Statistics to show if Respondents have any Measures in place to Protect Biometric Templates

Are there Measures in place to Protect Biometric Templates	No. of Respondents	No. of Respondents Percentage (%)
Yes	66	84.6%
No	12	15.4%
Total	**78**	**100.0%**

4.2.3 Policies aimed at Protecting Biometric Templates in Storage

To further investigate the magnitude with which security of biometric templates is put into consideration we inquired from the respondents whether there were any policies in their organizations governing security of biometric templates. The results presented in Table 10 showed that 61(78.2%) of respondents had policies in place while 17(21.8%) of respondents admitted that they did not have any governing policies in place.

Table 10. Statistics showing if there are Biometric Templates Security Policies

Are there Biometric Templates Security Policies	Respondents	No. of Respondents Percentage (%)
Yes	61	78.2%
No	17	21.8%
Total	**78**	**100.0%**

Observing that 17(21.8%) of respondents in Table 3.2.3. did not have policies to mitigate biometric templates attacks, asked what measures they had in place to mitigate Biometric template attacks in storage. We established that the following practices were used; *matching live finger again, file access permissions were established in Linux, cryptologic tools, servers without external access were used, databases were password protected and database access permissions were regulated or denied*.

4.2.4 Biometric Templates Protection Techniques

We narrowed further down from determining whether there were measures and policies in place targeted at protecting biometric templates to ascertaining which template protection techniques respondents used. It was established that 39(50%) of respondents used *Biometric Encryption Technique* to secure biometric templates while 16(20.5%) of respondents made use of *Feature Transformation Technique*. 23(29.5%) of respondents did not use any biometric template protection techniques leaving them exposed to experiencing biometric template attacks in their biometric systems. These statistics were presented in Table 11.

Table 11. Statistics for Biometric Templates Protection Techniques Used

Biometric Template Protection Technique	No. of Respondents	No. of Respondents Percentage (%)
Feature Transformation	16	20.5%
Biometric Encryption	39	50.0%
None	23	29.5%
Total	**78**	**100.0%**

4.2.5 Biometric Encryption Technique & Biometric Encryption Schemes

From Table 12, it was established that the majority of respondents 39(50.0%) had indicated that they used *Biometric Encryption* technique. we determined from the study that of the two methods *Key Binding* and *Key Generation* found in *Biometric Encryption* Technique that 16(20.5%) of respondents used Key Binding while 23(29.5%) used Key Generation. From these results also presented in Table 12 it is evident that *Key Generation* method is the most preferred *Biometric Encryption* method than *Key Binding* because there is more security with generating encryption keys than binding encryption keys while securing data.

Table 12. Statistics for Biometric Encryption Methods Used

Biometric Encryption Methods	No. of Respondents	No. of Respondents Percentage (%)
Key Binding	16	20.5%
Key Generation	23	29.5%
None	39	50.0%
Total	**78**	**100.0%**

The current biometric encryption schemes used to protect biometric templates were explored. It was required for respondents to identify the schemes they used to protect biometric templates. From the data collected and tabulated in Table 13 it was shown that 10(12.8%) of respondents had used *Fuzzy Vault*, 6(7.7%) of respondents had used *Water Marking*, 40(51.3%) had used *RSA & ECC* and 9(11.5%) indicated they had used *Fuzzy Commitment* and 12(15.4%) specified they had used *Cancellable Biometrics*. 22(28.2%) of respondents indicated that they did not use any *biometric encryption schemes* while 4(5.1%) of respondents indicated that they used other biometric encryption schemes. The *other* schemes specified by respondents included *private encryptions*, *AES 128b*. The results of the *Biometric Encryption Schemes* used by respondents are shown in Table 13.

Table 13. Statistics of Biometric Encryption Schemes used Under Key Generation Method

Biometric Encryption Schemes	No. of Respondents	Total No. of Respondents	No of respondents in percentage (%)
Fuzzy Vault	10	78	12.8%
Water Marking	6	78	7.7%
RSA and ECC	40	78	51.3%
Fuzzy Commitment	9	78	11.5%
Cancellable Biometrics	12	78	15.4%
None	22	78	28.2%
Other(s)	4	78	5.1%
Total		**78**	**100.0%**

4.3 Efficiency of Encryption Methods

This section was significant in reviewing efficiency of biometric encryption methods used to protect biometric fingerprint templates. It consisted of the following subsections; Views of respondents on efficiency of encryption methods they used, Encryption keys and biometric templates storage space, Practices improving biometric encryption, Encrypting data with biometric encryption keys derived from fingerprint templates, Biometric encryption keys' entropy strength, Biometric encryption keys future use in data encryption.

4.3.1 Respondents' views on Efficiency of Encryption Methods They Use

The scales were equated with values shown in brackets next to them as follows for easier analysis and interpretation of data;

Strongly Disagree(1), Disagree(2), Neutral(3), Agree(4) and Strongly Agree(5).

This section was a basis for determining from respondents if there were risks of hacking biometric encryption methods used to secure biometric templates. We established that 10(12.8%) of respondents *Strongly Disagreed*, 31(39.7%) of respondents *Disagreed*, 22(28.2%) of respondents *Agreed* while 5(6.4%) *Strongly Agreed* and 10(12.8%) neither agreed nor disagreed to any extent and were categorized as *Neutral*. These results were presented in Table 14 below.

Table 14. Statistics showing if there is Risk of Hacking Biometric Encryption Method Used

There is Risk of Hacking Biometric Systems in the Encryption Method Used	No. of Respondents	No of respondents in percentage (%)
Strongly Disagree	10	12.8%
Disagree	31	39.7%
Neutral	10	12.8%
Agree	22	28.2%
Strongly Agree	5	6.4%
Total	**78**	**100.0%**

This section was a basis for determining from respondents if encryption methods used to secure biometric templates were considered fool proof. We established that 7(9.0%) of respondents *Strongly Disagreed*, 19(24.4%) of respondents *Disagreed*, 19(24.4%) of respondents *Agreed* while 9(11.5%) *Strongly Agreed* and 24(30.8%) neither agreed nor disagreed to any extent and were categorized as Neutral. These results were presented in Table 15.

Table 15. Statistics showing if Encryption Methods used by Respondent are Fool Proof

The Encryption Methods Used by Respondent are Fool Proof	No. of Respondents	No of respondents in percentage (%)
Strongly Disagree	7	9.0%
Disagree	19	24.4%
Neutral	24	30.8%
Agree	19	24.4%
Strongly Agree	9	11.5%
Total	**78**	**100.0%**

This section was a basis for determining from respondents if encryption methods used were satisfactory in securing biometric data. We established that 5(6.4%) of respondents *Strongly Disagreed*, 15(19.2%) of respondents *Disagreed*, 31(39.7%) of respondents *Agreed* while 12(15.4%) *Strongly Agreed* and 15(19.2%) neither agreed nor disagreed to any extent and were categorized as Neutral. These results were presented in Table 16.

Table 16. Statistics of Respondents whose Biometric Encryption Method is satisfactory

Biometric Template Encryption Method used is Satisfactory	No. of Respondents	No of respondents in percentage (%)
Strongly Disagree	5	6.4%
Disagree	15	19.2%
Neutral	15	19.2%
Agree	31	39.7%
Strongly Agree	12	15.4%
Total	**78**	**100.0%**

The mode for *if there is risk of hacking biometric systems in Encryption Method used* is **2** whose equivalent is *Disagree*. The greater percentage of respondents Disagreed *that there is risk of hacking biometric systems based on the Encryption Method they used* implying that they believed their biometric encryption method was not so exposed to the risk of hacking.

The mode for *if biometric encryption methods are fool proof* is **3** whose equivalent is *Neutral*. The greater percentage of respondents were not sure whether *biometric encryption methods they used are fool proof* implying that they do not really doubt or consider them to be insecure.

The mode for *if biometric template security is satisfactory in Encryption Method used is* **4** whose equivalent is *Agree*. The greater percentage of respondents agreed that biometric template security is satisfactory based on the Encryption Method they used implying that they believed the biometric encryption method they used provided satisfactory security on biometric templates of the biometric systems they developed. *Spearman's rho* was used to find *correlations* between *encryption methods efficiencies*.

Table 17. Correlations of Encryption Methods based on their Efficiencies

			If there is risk of hacking biometric systems in Encryption Method Used	If biometric encryption methods are fool proof	If biometric template security is satisfactory in Encryption Method Used
Spearman's rho	If there is risk of hacking biometric systems in Encryption Method Used	Correlation Coefficient	1.000	-.223	-.376**
		Sig. (2-tailed)	.	.050	.001
		N	78	78	78
	If biometric encryption methods are fool proof	Correlation Coefficient	-.223	1.000	.322**
		Sig. (2-tailed)	.050	.	.004
		N	78	78	78
	If biometric template security is satisfactory in Encryption Method Used	Correlation Coefficient	-.376**	.322**	1.000
		Sig. (2-tailed)	.001	.004	.
		N	78	78	78

**. Correlation is significant at the 0.01 level (2-tailed).

The correlations presented in Table 17, are described as follows;

There is a moderate **negative** Correlation of **-0.376** with a **p** value of **0.001** between *if there is risk of hacking biometric systems in Encryption Method used* and *if biometric template security is satisfactory in Encryption Method used* implying that if the risk of hacking biometric systems based on biometric encryption method used *increases* then the encryption method's efficiency *reduces* and is not satisfactory.

There is a moderate **positive** Correlation of **0.322** with a **p** value of **0.001** between *if biometric encryption methods are fool proof* and *if biometric template security is satisfactory in Encryption Method used* implying that if biometric encryption method *excels* in being fool proof then the encryption method's efficiency *increases* and is considered satisfactory.

Table 18 gives results for Mean, Median and Mode of *Efficiency of Encryption Methods used*.

Table 18. Mean, Median and Mode of Efficiency of Encryption Methods

	If there is risk of hacking biometric systems in Encryption Method Used	If biometric encryption methods are fool proof	If biometric template security is satisfactory systems in Encryption Method Used
N	78	78	78
Mean	2.76	3.05	3.38
Median	2.00	3.00	4.00
Mode	2 (Disagree)	3 (Neutral)	4 (Agree)

4.3.2 Encryption Keys & Encrypted Biometric Templates Storage Space

We observed that 65(83.3%) of respondents would not want to keep encryption keys in the same storage space with Encrypted Biometric Templates. 13(16.7%) of respondents would on the contrary keep encryption keys together with encrypted biometric templates in the same storage space. The tabulated results are shown in Table 19. The objective of a biometric system developer would be to make it hard for an adversary to decode biometric data in a biometric system by keeping biometric encryption keys in a different location away from encrypted biometric data.

Table 19. Statistics of Respondents who would keep Encryption Keys in the same storage space with Encrypted Biometric Templates

Would keep Encryption Keys in same storage space with Encrypted Biometric Templates	No. of Respondents	No. of Respondents Percentage (%)
Yes	13	16.7%
No	65	83.3%
Total	**78**	**100.0%**

4.3.3 Practices Improving Biometric Encryption

Respondents identified various practices they deemed would improve biometric encryption as follows; 52(66.7%) of respondents believed *Improving Accuracy and Security of Biometric Encryption Algorithms* would help. *Use of Multimodal Biometrics* came in second having been identified by 38(48.7%) of respondents. 36(46.2%) of respondents would rather *Improve Image Acquisition Process* while 31(39.7%) and 24(30.8%) of respondents would *Make Biometric Encryption Resilient against attacks* and *Develop Biometric Encryption Applications* respectively. The Other 3(3.8%) of respondents listed *speeding of biometric identification & verification* and *performing liveliness detection* as other practices that would improve biometric encryption. These results are tabulated in Table 20 and Table 21 below.

Table 20. Statistics of Practices Biometric Encryption

Practices Improving Biometric Encryption	No. of Respondents	Total No. of Respondents	No of Respondents in percentage (%)
Improving Image Acquisition Process	36	78	46.2%
Making Biometric Encryption Resilient against attacks	31	78	39.7%
Improving Accuracy and Security of Biometric Encryption Algorithms	52	78	66.7%
Use of Multimodal Biometrics	38	78	48.7%
Develop Biometric Encryption Applications	24	78	30.8%
Other(s)	3	78	3.8%
Total		**78**	**100.0%**

Table 21. Statistics of Combination of Practices Improving Biometric Encryption

Combination of Best Practices Improving Biometric Encryption	No. of Respondents	No of Respondents in percentage (%)
Encryption Apps	2	2.6%
Accuracy & Security	5	6.4%
Accuracy & Security, Encryption Apps	3	3.8%
Accuracy & Security, Multimodal	8	10.3%
Image Acquisition	3	3.8%
Image Acquisition, Encryption Apps	1	1.3%
Image Acquisition, Accuracy & Security	8	10.3%
Image Acquisition, Accuracy & Security, Encryption Apps	1	1.3%
Image Acquisition, Accuracy & Security, Multimodal	2	2.6%
Image Acquisition, Accuracy & Security, Multimodal, Encryption Apps	1	1.3%
Image Acquisition, Resilient to Attacks	2	2.6%
Image Acquisition, Resilient to Attacks, Accuracy & Security	2	2.6%
Image Acquisition, Resilient to Attacks, Accuracy & Security, Encryption Apps	1	1.3%
Image Acquisition, Resilient to Attacks, Accuracy & Security, Multimodal	2	2.6%
Image Acquisition, Resilient to Attacks, Accuracy & Security, Multimodal, Encryption Apps	6	7.7%
Image Acquisition, Resilient to Attacks, Multimodal	1	1.3%
Image Acquisition, Multimodal	5	6.4%
Image Acquisition, Multimodal, Encryption Apps	1	1.3%
Resilient to Attacks	2	2.6%
Resilient to Attacks, Encryption Apps	2	2.6%
Resilient to Attacks, Accuracy & Security	5	6.4%
Resilient to Attacks, Accuracy & Security, Encryption Apps	2	2.6%
Resilient to Attacks, Accuracy & Security, Multimodal	4	5.1%
Resilient to Attacks, Accuracy & Security, Multimodal, Encryption Apps	2	2.6%
Multimodal	4	5.1%
Multimodal, Encryption Apps	2	2.6%
Other(s)	3	3.8%
Total	**78**	**100.0%**

Key for Table 21:

Image Acquisition : Improving Image Acquisition Process
Multimodal : Use of Multimodal Biometrics
Resilient to Attacks : Making Biometric Encryption Resilient against attacks
Encryption Apps : Develop Biometric Encryption Applications
Accuracy & Security : Improving Accuracy and Security of Biometric Encryption Algorithms
Other(s) : Other(s)

4.3.4 Encrypt Data with Biometric Encryption Keys Derived From Fingerprint Templates

We also wanted to know whether respondents considered *encryption of data using encryption keys derived from biometric fingerprint templates* a feasible idea. The results shown in Table 22 revealed that 48(61.5%) of respondents believed it would be achievable while 30(38.5%) declined. These results proved that if respondents had a way to derive biometric encryption keys from fingerprints they would use this approach.

Table 22. Statistics of Respondents who believed Encryption Keys Derived from Fingerprint templates could be used to protect data in storage

Encrypted Biometric Templates and Biometric Encryption Keys in same Storage Space	No. of Respondents	No. of Respondents Percentage (%)
Yes	48	61.5%
No	30	38.5%
Total	**78**	**100.0%**

4.3.5 Biometric Encryption Keys Entropy Strength

To understand entropy strengths associated with biometric keys we sought to establish whether respondents believed encryption keys derived from biometric templates would be rich in entropy for encrypting data than a combination of passwords and access codes. The study revealed that 72(92.3%) of respondents thought encryption keys derived from biometrics would provide rich entropy than passwords and access codes. 6(7.7%) of respondents were not convinced and when asked why they explained that *there would be overlaps in combination of keys from biometric templates if there are more people* and *strength of security keys is depended on quality of biometric templates implying poor samples would result in lower strength of encryption keys*. These results were presented in Table 23.

Table 23. Statistics of Respondents who Think Encryption Keys Derived from Biometrics would be Rich and Strong in Entropy

If Encryption Keys Derived from Biometrics would be Rich and Strong in Entropy	No. of Respondents	No. of Respondents Percentage (%)
Yes	72	92.3%
No	6	7.7%
Total	78	100.0%

4.3.6 Biometric Encryption Keys Future Use in Data Encryption

The study revealed that 62(79.5%) of respondents agreed that in the foreseeable future, encryption of data using biometric encryption keys will become a common practice among systems developers. 16(20.5%) of respondents did not think it would be possible. In asking this question we wanted to estimate respondents' expectations of future trends of biometric encryption security in this section. These results were shown in Table 24.

Table 24. Statistics of Respondents who Foresee Use Of Entropy from Biometrics in Data Encryption

Does it seem feasible in the near future for Entropy to be Derived from Biometrics and used in Data Encryption?	No. of Respondents	No. of Respondents Percentage (%)
Yes	62	79.5%
No	16	20.5%
Total	78	100.0%

4.4 Biometric Templates Security Challenges

This section sought to establish if respondents faced security challenges with regards to biometric template security then determine biometric attacks encountered and discover if biometric templates storage areas had been compromised. We also sought respondents' opinions on whether they considered databases as the most ideal preference for biometric templates storage and why they would not choose databases for biometric templates storage. Finally, the section investigates options respondents would use to ensure biometric templates are safely stored in databases.

4.4.1 Challenges Pertaining to Biometric Template Security

From the data collected, 15(19.2%) of respondents agreed to having encountered challenges related to biometric template security while 63(80.8%) did not. The respondents who admitted to having faced biometric template security issues were asked to specify in particular which challenges they experienced and they listed the following; *data theft from customer locations, difficulty in guaranteeing high accuracy levels while ensuring security levels are upheld, biometric templates modifications, leaking of biometric template information to unauthorized users, encryption keys being based on combination of passwords possibly known to adversaries, difficulty in generating random chaff surrounding biometric features in mobile devices due to limited processing resources and non-secure infrastructure*. Table 25 below shows these statistics.

Table 25. Statistics of Challenges Encountered in Biometric Template Security

Are there challenges encountered in Biometric Template Security?	No. of Respondents	No. of Respondents Percentage (%)
Yes	15	19.2%
No	63	80.8%
Total	**78**	**100.0%**

4.4.2 Type of Biometric Templates Attacks Encountered

The major attacks waged on biometrics templates by adversaries in biometric systems were; *spoofing* which is the fooling of biometric system by using fake finger, face or iris templates. *Spoofing* ranked as the most encountered attack reported by 43(55.1%) of respondents followed by *Tampering* at 20(25.6%).*Tampering* is where biometric attackers modify biometric feature sets to obtain high verification scores. *Trojan* attacks which entail the replacing of the biometric matcher programs with ones that always allow access were identified as the third most recurring attacks on biometric templates being identified by 19(24.4%) of respondents. *Replay attacks* where biometric system sensors are circumvented by running pre-saved biometric templates and *Substitution attacks* which involve replacing of users' biometric templates with those of adversaries each had 17(21.8%) of respondents identifying them respectively. A further 12(15.4%) of respondents did not encounter any biometric attacks as they specified *none* by selecting the *other* select option. These results were presented in Table 26 and Table 27.

Table 26. Statistics of Biometric Attacks Encountered

Combination of Biometric Attacks Encountered	No. of Respondents	No of Respondents in percentage (%)
Replay attacks	3	3.8%
Replay attacks, Substitution attacks	1	1.3%
Replay attacks, Tampering	1	1.3%
Replay attacks, Trojan attacks	1	1.3%
Spoofing	24	30.8%
Spoofing, Replay attacks	2	2.6%
Spoofing, Replay attacks, Substitution attacks	2	2.6%
Spoofing, Replay attacks, Substitution attacks, Tampering	2	2.6%
Spoofing, Replay attacks, Substitution attacks, Tampering, Trojan attacks	3	3.8%
Spoofing, Replay attacks, Tampering, Trojan attacks	1	1.3%
Spoofing, Replay attacks, Trojan attacks	1	1.3%
Spoofing, Substitution attacks	1	1.3%
Spoofing, Substitution attacks, Tampering	1	1.3%
Spoofing, Substitution attacks, Trojan attacks	1	1.3%
Spoofing, Tampering	3	3.8%
Spoofing, Trojan attacks	2	2.6%
Substitution attacks	2	2.6%
Substitution attacks, Tampering	2	2.6%
Substitution attacks, Tampering, Trojan attacks	2	2.6%
Tampering	3	3.8%
Tampering, Trojan attacks	2	2.6%
Trojan attacks	6	7.7%
Other(s)	12	15.4%
Total	**78**	**100.0**

Table 27. Statistics of Biometric Attacks Encountered

Biometric Attacks Encountered	No. of Respondents	Total No. of Respondents	No of Respondents in percentage (%)
Spoofing	43	78	55.1%
Replay Attacks	17	78	21.8%
Substitution Attacks	17	78	21.8%
Tampering	20	78	25.6%
Trojan Attacks	19	78	24.4%
Other(s) None	12	78	15.4%
Total		**78**	**100.0%**

4.4.3 Biometric Templates Storage Compromised

Other than investigating types of biometric attacks experienced by respondents, we established that 2(2.6%) of respondents had their biometric template storage space compromised implying that adversaries not only attacked biometric templates but also attacked biometric storage space as well. 76(97.4%) of respondents had not experienced any attacks on their biometric templates storage space. The Table 28 shows these results.

Table 28. Statistics showing if Biometric Template Storage has ever been Compromised

Biometric Template Storage Space ever been Compromised	No. of Respondents	No of Respondents in percentage (%)
Yes	2	2.6%
No	76	97.4%
Total	**78**	**100.0%**

Information systems archive data in databases and since most biometric systems too store biometric templates in databases as well we discovered that 61(78.2%) of respondents considered databases as the most ideal storage space for biometric templates while 17(21.8%) of respondents did not. These results are shown in Table 29. The respondents who would not opt for databases to store biometric templates cited *security concerns, long time taken to find template match* and *risks involved in central storage databases*. They would instead *save biometric templates in dedicated memory sticks, encrypted folders* and *smart cards using MOC technology*. Other results showed suggestion of, '*a secure device where the operating system would be incapable of accessing'.*

Table 29. Statistics of Respondents using Databases as Ideal Template Storage Space

Respondents using Databases as Ideal Template Storage Space	No. of Respondents	No of Respondents in percentage (%)
Yes	61	78.2%
No	17	21.8%
Total	**78**	**100.0%**

4.4.4 Measures used to ensure Safe Storage of Biometric Templates in Database

We observed that 59(75.6%) of respondents indicated that *Encrypting of Biometric Templates Before Saving Them in Database* would ensure safe storage of biometric templates in database, 50(64.1%) of respondents would rather *Reduce Levels of Access to Database* while 38(48.7%) and 36(46.2%) of respondents would *Use strong passwords* and *change database passwords often* respectively. 4(5.1%) of respondents who had selected *others* specified that they would *implement strong access control to database, use finger scans to access database, use data vaults, deploy database firewalls* and *implement audit software*. These data results are shown in Table 30 and Table 31.

Table 30. Statistics of Measures ensuring Safe Biometric Templates in Database

Measures used to ensure Safe Storage of Biometric Templates in Database	No. of Respondents	Total No. of Respondents	No of Respondents in percentage (%)
Change Database Passwords often	36	78	46.2%
Use Strong Passwords	38	78	48.7%
Reduce Levels of Access to Database	50	78	64.1%
Encrypt Biometric Templates Before Saving them in Database	59	78	75.6%
Other(s)	4	78	5.1%
Total		**78**	**100.0%**

Table 31. Statistics of Combination of Measures ensuring Safe Biometric Templates in Database

Combination of Measures used to ensure Safe Storage of Biometric Templates in Database	No. of Respondents	No of Respondents in percentage (%)
Change DB passwd	5	6.4%
Change DB passwd, Encrypt Bio Templates	1	1.3%
Change DB passwd, Reduce DB access	2	2.6%
Change DB passwd, Reduce DB access, Encrypt Bio Templates	3	3.8%
Change DB passwd, Strong passwd, Encrypt Bio Templates	2	2.6%
Change DB passwd, Strong passwd, Reduce DB access	3	3.8%
Change DB passwd, Strong passwd, Reduce DB access, Encrypt Bio Templates	20	25.6%
Encrypt Bio Templates	14	17.9%
Reduce DB access	1	1.3%
Reduce DB access, Encrypt Bio Templates	10	12.8%
Strong passwd	1	1.3%
Strong passwd, Encrypt Bio Templates	1	1.3%
Strong passwd, Reduce DB access	3	3.8%
Strong passwd, Reduce DB access, Encrypt Bio Templates	8	10.3%
Other(s)	4	5.1%
Total	**78**	**100.0%**

Key for Table 31:

Change DB passwd : Change Database passwords often
Reduce DB access : Reduce levels of access to database
Strong passwd : Use strong passwords
Encrypt Bio Templates : Encrypt biometric templates before saving them in database
Other(s) : Other(s)

4.4.5 Valuable Suggestions and Hints for furthering Safety of Biometric Templates

The sampled respondents mentioned that *biometric templates security is key to the advancement of the field of biometrics, passwords for biometric systems' databases should be changed every 90 days and no later than 180 days* and that *clearing i.e. zeroing data of de-allocated memory in biometric systems is of utmost significance as memory is vulnerable if malicious scripts could potentially read it and retrieve biometric image data before being emptied.*

5. CONCLUSION

The existing biometric fingerprint template protection schemes and approaches were reviewed. It was discovered that some biometric encryption schemes were preferred over others. From the data collected, majority of respondents saved biometric templates in databases. Spoofing was the most experienced attack on biometric templates. Results from sampled respondents showed that, a combination of measures and not one form of prevention measure were required to protect biometric templates against adversary attacks. In future work, we will propose a two-step encryption & decryption approach for securing biometric fingerprint templates stored in a database.

6. REFERENCES

[1] Das, Ashok Kumar. "Cryptanalysis And Further Improvement Of A Biometric-Based Remote User Authentication Scheme Using Smart Cards." *International Journal of Network Security & Its Applications*, 2011, 13-28.

[2] Tan, Z. "An efficient biometrics-based authentication scheme for telecare medicine information systems." *Przeglad Elektrotechniczny, ISSN 0033-2097, R. 89 NR 5/2013*, 2013, 200-204.

[3] Rathgeb, C., & Busch, C. (2012). "Multi-Biometric Template Protection: Issues and Challenges." *Intech*, 2012, 173-190.

[4] Ahmad, Sharifah Mumtazah Syed, Borhanuddin Mohd Ali, and Wan Azizun Wan Adnan. "Technical Issues and Challenges Of Biometric Applications as Access Control Tools Of Information Security." *International Journal of Innovative Computing, Information and Control Volume 8, Number 11, November 2012*, 2012: 7983-7999.

[5] D, Kannan, and Thilaka K. "Multibiometric Cryptosystem Based On Fuzzy Vault with Biohashing." *IOSR Journal of Electronics and Communication Engineering(IOSR-JECE)*, 2013: 34-43.

[6] Radha, N, and S Karthikeyan. "A Study On Biometric Template Security." *Ictact Journal on Soft Computing*, no. 01 (July 2010): 31-41.

[7] Radha, N, and S Karthikeyan. "An Evaluation Of Fingerprint Security Using NonInvertible Biohash." *International Journal of Network Security & Its Applications (IJNSA)* 3, no. 4 (July 2011).

[8] Ratha, Nalini, Sharat Chikkerur, Jonathan Connell, and Ruud Bolle. "Generating Cancelable Fingerprint Templates." *IEEE Transactions on Pattern Analysis and Machine Intelligence* 29 (April 2007): 561-572.

[9] Juels, Ari, and Madhu Sudan. "A Fuzzy Vault Scheme." *IEEE International Symposium Information Theory*, 2002.

[10] Geetika, and Manavjeet Kaur. "Fuzzy Vault with Iris and Retina: A Review." *International Journal of Advanced Research in Computer Science and Software Engineering*. Volume 3, Issue 4, April 2013 ISSN:2277 128X, 2013.

[11] Deshpande, Avanti, and R B Joshi. "Information Security using Cryptography and Image Processing." *IJSRD - International Journal for Scientific Research & Development* 1, no. 9 (2013).

[12] Jeny, J.Rethna Virgil, and Chanda J. Jangid. "Multibiometric Cryptosystem with Fuzzy Vault and Fuzzy Commitment by Feature-Level Fusion." *International Journal of Emerging Technology and Advanced Engineering , (Volume 3, Issue 3, March 2013)*, 2013.

[13] D, Kannan, and Thilaka K. "Multibiometric Cryptosystem Based On Fuzzy Vault with Biohashing." *IOSR Journal of Electronics and Communication Engineering(IOSR-JECE)*, 2013: 34-43.

[14] Yates, Daniel S., and David S. Moore. *The practice of statistics*. New York: W.H. Freeman, 2008.

[15] Jain, A. K., Ross, A., & Uludag, U. (2005). "Biometric Template Security: Challenges and Solutions." *European Signal Processing Conference (EUSIPCO), (Antalya, Turkey), September 2005.*

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 115 - 118, 2015, ISSN:- 2319–8656

Haralick Texture Features based Syriac(Assyrian) and English or Arabic documents Classification

Basima Z.Yacob
Department of computer science
Faculty of science
University of Duhok
Duhok, Iraq

Abstract: Script identification is very essential before running an individual OCR system. Automatic language script identification from document images facilitates many important applications such as sorting, transcription of multilingual documents and indexing of large collection of such images, or as a precursor to optical character recognition (OCR), in this paper the characterized are between Syriac and English documents or between Syriac and Arabic documents were the characterized is achieved by extracting Haralick texture Features. it is investigated a texture as a tool for determining the script of document image ,based on the observation that text has a distinct visual texture. Further, K nearest neighbour algorithm is used to classify 300 text blocks into one of the two scripts: Syriac, and English , or Syriac and Arabic based on Haralick texture Features . The script was inserted to the System with different rotation angles between 0º and 135º and the results of recognition were good.

Keywords: Syriac script; Haralick Texture Features; OCR; English script; Arabic script; knn algorithm.

1. INTRODUCTION

Script and language identification are a key part of automatic processing of document images in an international environment. A document's script must be recognized in order to choose an appropriate optical character recognition (OCR) algorithm. For scripts used by more than one language, discriminating the language of a document prior to OCR is also helpful, and language identification is crucial for further processing steps such as routing, indexing, or translation.

One of the important tasks in machine learning is the electronic reading of documents. All documents can be converted to electronic form using a high performance Optical Character Recognizer (OCR). Recognition of bilingual documents can be approached by the recognition via script identification.

This paper considers the discrimination between the Syriac and English scripts and between the Syriac and Arabic scripts according to an analysis of text block.

The Syriac (Assyrian) language is one of the Semitic languages that is being spoken in Iraq, Syria, Turkey and Iran by Assyrians. It's an ancient language, one of the rarest and oldest in the world.

Syriac is an ancient Iraqi language, and it is culturally used by human beings in Iraq. It has many religious scripts as well as scientific and literary books which have been completed and achieved throughout the long history and efficient civilization for this language, and conveying this important thought for communication between the present and past generations.

Over the past decades, many different researches and papers have been concerned to discriminate between the two or more difference languages for example Arabic and English or between Indian and English documents and ect. , but no research has been achieved towards the discriminating between Syriac and other languages.

This paper presents a scheme for identification between Syric and English scripts or between Syriac and Arabic script based on Haralick Texture Features.

Two scripts were classified by the classification algorithm, these scripts are Syriac and Roman (English) or Syriac and Arabic. Classification accuracy depends on the rotation angle of the script.

2. RELATED WORK

Santanu Choudhuri, et al. [1] has proposed a method for identification of Indian languages by combining Gabor filter based technique and direction distance histogram classifier considering Hindi, English, Malayalam, Bengali, Telugu and Urdu. Dhanya et al. [2] have used Linear Support Vector Machine (LSVM), K-Nearest Neighbour (K-NN) and Neural Network (NN) classifiers on Gabor-based and zoning features to classify Tamil and English scripts. Wood et al. [3] have proposed projection profile method to determine Roman, Russian, Arabic, Korean and Chinese characters.

Later, script recognizer[4] has been extended to four scripts/ languages (Kannada, Hindi, English and Urdu) with different font sizes and styles by relaxing their constraints over different font sizes[5].

Horizontal projection was attempted [6] to separate two languages English and Arabic at text line level. Here, the horizontal projection profiles of Arabic text have a single peak corresponding to the baseline of the Arabic writing, where characters are connected together. In contrast, projections of English text have two major peaks corresponding to x-line and baseline. The projections of Arabic text lines are smooth while the projections of English text line have sharp jumps Multichannel Gabor filtering designed with four frequencies and four orientations was also applied over the bilingual document images[7] Arabic-English, Chinese-English, Hindi-English and Korean-English bilingual dictionaries to identify the script at word level.

Using the combination of shape, statistical and Water Reservoirs, an automatic line-wise script identification scheme from printed documents containing five most popular

scripts in the world, namely Roman, Chinese, Arabic, Devnagari and Bangla has been introduced[8].

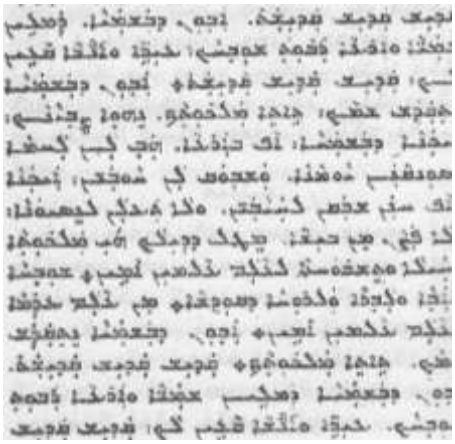
3. PROPOSED APPROACH

The paper primarily aims for block level classification; blocks of text are first extracted from the scanned document. For block of text extracted, Haralick Texture features are computed. These features are integrated to form database of vectors which are then used for Syriac and English or Arabic text separation via k-NN classifier. For better understanding, Figure.1 shows a schematic work-flow of the system

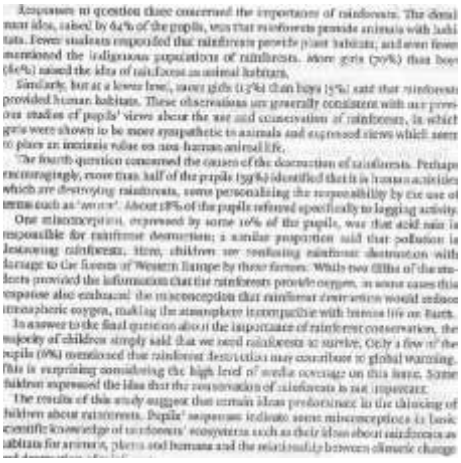
Figure. 1 A screen-shot of an overall work-flow of the system

3.1 Preprocessing

The preliminary task is to do pre-processing. Pre-processing techniques are application dependent. In this paper initially, 600 x600 text blocks are segmented manually from the document images of Syriac, English and Arabic and created 300 text blocks. Out of these 300 images Syriac, English, and Arabic are 100 each. A sample images text blocks of Syriac , English and Arabic are shown in figure 2.



(a)



(b)

(c)

Figure. 2 Examples of document images used for training and testing.

(a) Syriac, (b) English, and (c) Arabic.

3.2 Haralick TEXTURE Features EXTRACTION

From each block of normalized text, the Haralick texture features are evaluated for the purpose of script identification. Haralick Texture features are first reported in [9] for image classification. For better understanding, texture can also be defined as:it is property which contains important information about structural arrangement of surfaces and their relationship with surrounding environment. In this paper, the Haralick Texture of each test image is extracted as attributes to build a database which is used at classification stage. These set of statistical texture features collectively used to generate a feature vector.

Haralick features are used for analyzing the texture of an image on the other hand; Haralick features offer 13 different elements that define the textural structure of a image. Haralick features can be defined as follows [9].

Contrast, Homogeneity, Dissimilarity, Energy and Entropy, as Angular second moment: Energy

$$f_1 = \sum_{i=1}^{Ng}\sum_{j=1}^{Ng}\{p(i.j)\}^2$$

Contrast:

$$f_2 = \sum_{n=0}^{Ng-1} n^2 \left(\sum_{i=1}^{Ng}\sum_{j=1}^{Ng} p(i,j)\right) \quad \text{when } |i-j| = n$$

Correlation:

$$f_3 = \frac{\sum_{i=1}^{Ng}\sum_{J=1}^{Ng}(ij)p(i,j) - \mu_x\mu_y}{\sigma_x\,\sigma_y}$$

Sum of squares: Variance

$$f_4 = \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} (i-\mu)^2 \, p(i,j)$$

Inverse Difference Moment homogeneity
Homogeneity (HOM) (also called the "Inverse Difference Moment")

$$f_5 = \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} \frac{1}{1+(i-j)^2} p(i,j)$$

Sum Average

$$f_6 = \sum_{i=2}^{2Ng} i p_{x+y}(i)$$

Sum Variance

$$f_7 = \sum_{i=2}^{2Ng} (i - f_8)^2 \, p_{x+y}(i)$$

Sum Entropy

$$f_8 = -\sum_{i=2}^{2Ng} p_x + y^{(i)} \log\{p_x + y^{(i)}\}$$

Entropy

$$f_9 = -\sum_{i=1}^{Ng} \sum_{j=1}^{Ng} p(i,j) \log(p(i,j))$$

Difference Variance

$$f_{10} = E[p_x - y^2] - E[p_x - y]^2$$

Difference Entropy

$$f_{11} = -\sum_{i=0}^{Ng-1} p_{x-y^{(i)}} \log\{p_{x-y^{(i)}}\}$$

Information Measures of Correlation

$$f_{12} = \frac{HXY - HXY1}{\max\{HX, HY\}}$$

$$f_{13} = (1 - \exp[-2.0(HXY2 - HXY)])^{1/2}$$

3.3 Classification

The traditional and simplest classification algorithm is k-nearest neighbour algorithm (k-NN). It is a method of classifying the instances based on the nearest training examples in the feature space. It classifies an object based on a majority vote of its neighbours, with the object being assigned to the class most common amongst its k nearest neighbours. The training set includes the data for classification for each specific.

For every new input, the Haralick textural features are obtained. A sample of Haralick textural features of Syriac, English and Arabic scripts of figure 2 are represented in Table1.

The following are the steps of the algorithm

1. Given an input image X with different rotation angles between 0º and 135º, determine its distance measure based on the computation of textural features.
2. Determine the k (k=3) nearest neighbor in the training set which comprises of the Haralick features.
3. Assign the image X to the closest match.

Table1: The sample Haralick Texture Features of Syriaic, English and Arabic Scripts

script / Features	Syriac	English	Arabic
F1	0.6343	0.3782	0.5194
F2	0.2930	0.7979	0.2831
F3	175.4046	246.0818	221.0589
F4	14.2433	14.4900	16.3956
F5	0.9252	0.7981	0.8971
F6	7.4427	7.4751	8.0417
F7	45.6203	40.2149	50.4000
F8	0.8193	1.2732	1.0232
F9	1.0219	1.7562	1.2327
F10	0.0935	0.0547	0.0801
F11	0.4700	0.8992	0.5703
F12	-0.4320	-0.1738	-0.2773
F13	0.6561	0.5331	0.5725

4. DISCUSSION

Experimentations are carried out with KNN classifier. To evaluate the a sample image of size 600x600 pixels is selected manually from each document image and created 300 text block images. Out of these 300 images Syriac, English, and Arabic are 100 each. The accuracy of the classification achieved for script identification is shown in Tables 2 and 3.

The achieved results of the classification depend on the rotation angle of script.

Table 2. Text block Syriac-English scripts identification results

Type of Documents Syriac –English	No. of documents	Classified correctly	% correct classification
Syriac – with rotation 0˚	100	100	100%
Syriac – with rotation 45˚	100	100	100%
Syriac – with rotation 90˚	100	100	100%
Syriac – with rotation 135˚	100	100	100%
English – with rotation 0˚	100	75	75%
English – with rotation 45˚	100	0	0%
English – with rotation 90˚	100	75	75%
English – with rotation 135˚	100	0	0%

5. ACKNOWLEDGMENTS

My thanks to my late husband **Hormuz Bobo** who had passed away before I publish this paper, and he had contributed towards this paper and supported me and provided the Assyrian (Syriac) scripts but I thank him mostly because he always encouraged me to accomplish such projects about the Assyrian language which are all dedicated to him.

Table 3. Text block Syriac-Arabic scripts identification results

Type of Documents	No. of documents	Classified correctly	% correct classification
Syriac –Arabic			
Syriac – with rotation 0˚	100	100	100%
Syriac – with rotation 45˚	100	100	100%
Syriac – with rotation 90˚	100	100	100%
Syriac – with rotation 135˚	100	100	100%
Arabic– with rotation 0˚	100	100	100%
Arabic– with rotation 45˚	100	0	0%
Arabic– with rotation 90˚	100	100	100%
Arabic– with rotation 135˚	100	0	0%

6. REFERENCES

[1] Santanu C, Gaurav H., Shekar M.i, and Shet R.B., 2000, Identification of scripts of Indian languages by Combining trainable classifiers, Proc. of ICVGIP, India.

[2] Dhanya D., Ramakrishnan A.G. and Pati P.B., 2002, Wavelet Based Co-occurrence Histogram Features for Texture Classification with an Application to Script Identification in a Document Image, Pattern Recognition Letters 29, 2008, pp 1182-1189.

[3] Wood S. L.; Yao X.; Krishnamurthy K. and Dang L., 1995, Language identification for printed text independent of segmentation, Proc. Int. Conf. on Image Processing, 428–431, IEEE 0-8186-7310-9/95.

[4] Basavaraj P. and Subbareddy N. . Neural network based system for script identification in Indian documents, Sadhana Vol. 27, part-i1, pp 83-97, 2002.

[5] Dhandra.B.V, Nagabhushan. P, Mallikarjun H. , Ravindra H., Malemath. V.S, 2006. Script Identification Based On or phological Reconstruction In Document Images, The 18th International Conference on Pattern Recognition (ICPR'06).

[6] Elgammmal.A.M and Ismail.M.A, 2001. Techniques For Language Identification for Hybrid Arabic-English Document Images, Proc. Sixth Int'l Conf. Document Analysis and Recognition, pp. 1100-1104.

[7] Huanfeng M. and David D., 2003**.** Gabor Filter Based Multi-Class Classifier for Scanned Document Images, Proceedings of the Seventh International Conference on Document Image Analysis and Recognition (ICDAR'03).

[8] Pal U. and Chaudhuri.B.B, 2001., Automatic identification of English, Chinese, Arabic, Devnagari and Bangla script line, Proc. 6th Intl. Conf: Document Analysis and Recognition (ICDAR'OI), pages 790-794.

[9] R. M. Haralick, K. Shanmugam, I. Dinstein, 1973. Textural features for image classification, IEEE Transactions on Systems, Man, and Cybernetics, vol. SMC 3, No.6, November, pp. 610-621.

.

.

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 115 - 118, 2015, ISSN:- 2319–8656

SOA for Dynamically Integrated Virtual Learning Environment Systems with Cloud Based Services

Mohammed Eltahir Abdelhag
IT Dept. National Ribat University, Sudan
IS Dept. Jazan University,
Jazan, KSA

Saife Eldin fattoh Osman
Emirates College for Science & Technology
Sudan

Abstract: SOA is structural approach for creating services to be reused and shared, so it provides agility and cost saving in software development by dividing the application into multiple software components to be reused in other systems. Cloud computing is truly scalable and provide virtualized resources which users can subscribe. Using a cloud and SOA in virtual learning systems provide a great chance for learners to enhance gained learning outcomes. The adoption of cloud services also assists in reducing the cost of software, hardware, human resources and infrastructure. This paper will use SOA and cloud computing to transfer virtual learning systems in the cloud to be more integrated and interoperable through showing a conceptual model of distributed virtual learning system and using cloud computing combined with services oriented architecture, to contribute in interoperability and integration of e-learning systems in general

Keywords: Service Oriented Architecture (SOA), Cloud Computing, Systems Integration, virtual learning system

1. INTRODUCTION

Systems with same functionalities want to integrate existing systems to implement Information Technology support for business processes that cover the entire business value chain. A variety of technologies are used, services oriented architecture SOA, web services to cloud computing. By using the Internet, universities and high institutes make their learning systems available to internal departments or external learners, but the interactions are not flexible without standardized architecture.

The goal of this study is to design an integrated virtual learning system which can universally provide end-to-end education services such as learner profile service ,grading service ,course content service and etc. with modern information technologies available in cloud computing which can be accessed anywhere, by anybody, at any time. SOA has provided an important contribution in systems integration and interoperability. The interoperability between distributed virtual learning systems is highly important and it will be achieved through web services based on SOA framework.

Both SOA and cloud are concerning about delivering of services to systems with better flexibility, integration, interoperability and cost effectiveness to achieve a satisfied level of that, the virtual learning systems can be prepared with functions to service students , teachers and other learners. It's necessary to have a system infrastructure in order to use SOA and cloud.

To achieve good transformation into cloud computing a structure that support efficiency and power of cloud computing is required. Beside an organization service oriented architecture to ease the infrastructure is required for truly implementation of the cloud computing. The cloud brings a good means for distributing services in SOA architecture paradigm.

This paper is focusing in developing a SOA based development using the concepts of SOA and cloud computing to provide dynamically integration and interoperability in the case of the virtual learning systems, which can be developed on a cloud platform

2. LITERATURE REVIEW OF USED TECHNOLOGIES

2.1 Service-oriented architecture (SOA)

A service-oriented architecture (SOA) is a collection of services that communicate with each other, for example, passing data from one service to another or coordinating an activity between one or more services. [1]

A service-oriented architecture (SOA) is the underlying structure supporting communications between services. SOA defines how two computing entities, such as programs, interact in such a way as to enable one entity to perform a unit of work on behalf of another entity. [2]

SOA is a set of principles which enable the development of distributed applications. It includes all aspects of creation and usage of business services. SOA provides application platform which integrates business processes with operating resources. It also provides interfaces for a new service based on semantic of an enterprise and functional requests and it maps them to existing systems[1].

Requirements for an SOA: To efficiently use SOA, we have to follow these requirements [1]:

Interoperability between different systems and programming languages.

The most important basis for a simple integration between applications on different platforms is to provide a communication protocol. This protocol is available for most systems and programming languages.

Clear and unambiguous description language.

To use a service offered by a provider, it is not only necessary to be able to access the provider system, but the syntax of the service interface must also be clearly defined in a platform-independent fashion.

Retrieval of the service.

To support a convenient integration at design time or even system run time, a search mechanism is required to retrieve suitable services. Classify these services as computer accessible, hierarchical or taxonomies based on what the services in each category do and how they can be invoke

2.2 Web Services

A Web service is a method of communication between two electronic devices over a network. It is a software function provided at a network address over the web with the service always on as in the concept of utility computing. [1]
The W3C defines a Web service as: a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.[3]
SOA defines three roles in services such as service broker, service provider and service requester [4]:
Service broker: Plays the role of a medium for web services. It can accept registration requests from services providers, and can also process query requests from services requester.
Service provider: Mainly refers to the developer of web service applications; it is also required to describe details of its web services.
Service requester: Sends requests for services; follow-up operations include sending query and linking to the suitable web services

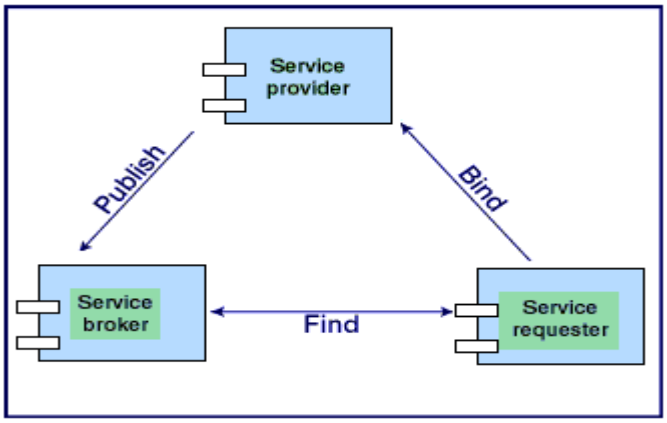


Figure 1. A Conceptual Architecture for Web Services [5]

2.3 Cloud Computing

Cloud computing is the next stage in the Internet's evolution, providing the means through which everything, from computing power to computing infrastructure, applications, business processes to personal collaboration can be delivered to you as a service wherever and whenever you need.
Cloud computing [6] is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams. See Figure 2.

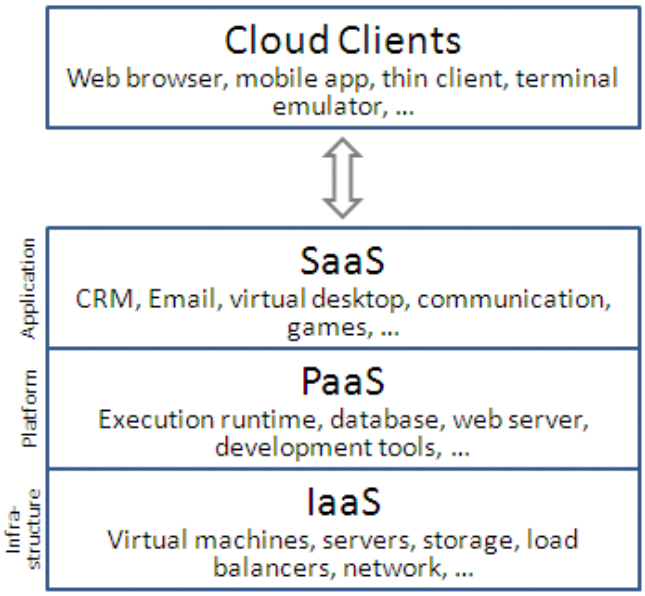


Figure 2 -Cloud computing service layers

2.4 Virtual learning environment (VLE)

A virtual learning environment (VLE)[7], or learning platform, is an e-learning education system based on the web that models conventional in-person education by providing equivalent virtual access to classes, class content, tests, homework, grades, assessments, and other external resources such as academic or museum website links. It is also a social space where students and teacher can interact through threaded discussions or chat. It typically uses Web 2.0 tools for 2-way interaction, and includes a content management system.
Virtual learning is one of the emerging technologies in education field. Many education universities are trying to fulfil increasing demands of improving learning services by facilitating access to e-learning systems, from anywhere at any time.

3. SYSTEM INTEGRATION

In information technology [8], systems integration is the process of linking together different computing systems and software applications physically or functionally, to act as a coordinated whole. Another way to look at computer integration is "making independent applications work as one

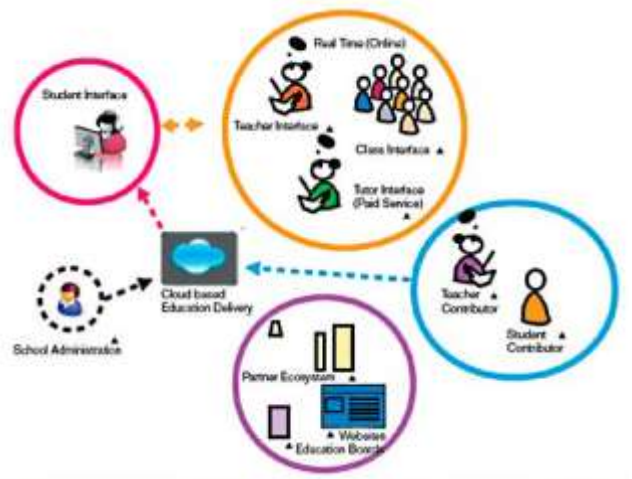


Figure-3 system integration in cloud model

3.1 Methods of integration [9]:

Vertical Integration: (as opposed to "horizontal") is the process of integrating subsystems according to their functionality by creating functional entities also referred to as silos.

Star Integration: or also known as Spaghetti Integration is a process of integration of the systems where each system is interconnected to each of the remaining subsystems.
Horizontal Integration: or Enterprise Service Bus (ESB) is an integration method in which a specialized subsystem is dedicated to communication between other subsystems.

4. VLS SYSTEM REQUIREMENT

The objective of this paper is to develop a SOA based methodology for Cloud Computing environment and apply this system methodology to create architecture for integrated virtual learning systems with the following non-functional requirements. Non-function Requirements [14]:
Ubiquitous Access: The system and its services have to be accessible anywhere and anytime.
Interoperability: The system should provide interoperability to access to other medical systems and external clinical services.
User Interface: The system must provide user-friendly interface for the users and the services available anytime.
Security and Privacy: The system should provide sufficient security and privacy methods for patient medical data and should adhere to the universal standards and guide- lines in encryption and authentication.
Scalability: The system should be scalable to interact with external medical service providers for more vital information.
Accuracy: The system should provide accurate data of the users of the system as well as of the service providers.
Maintainability: The system should be easy to maintain and provide updates as changes occur

5. THE PROPOSED INTEGRATED ARCHITECTURE

The main target of constructing virtual learning with SOA paradigm and cloud service, is to distribute and share the education services and resources to a wide range of users and enable them to benefits from that provided services anywhere, anytime. To build such integrated virtual learning systems based on multiple heterogeneous e-learning systems, there are some problems described below [15]:

Considering the stability and flexibility of e-learning cloud, they are connected by peer-to-peer network. Without a center, how can one system join the cloud and know other systems in the cloud?
To enable users to access resources flexible as while as protecting the copyright of the resource, how can we design the access policy?
Media diversity of resources is the feature of e-Learning cloud. To make the resources accessible cross-system, what would be implemented?
Since e-learning cloud provides services towards different termination equipment, differences of the computing capability and communication protocol among equipment should be a consideration aspect
To achieve the goal of integrated virtual learning systems based on cloud, we proposed an architecture including 3 layers as shown in Figure.3.The model we have applied in designing this system is to divide the VLS into multiple logical components layers, so we designed the system architecture into three tiers user interface tier, services and business component tier and data access tier see figure-4.

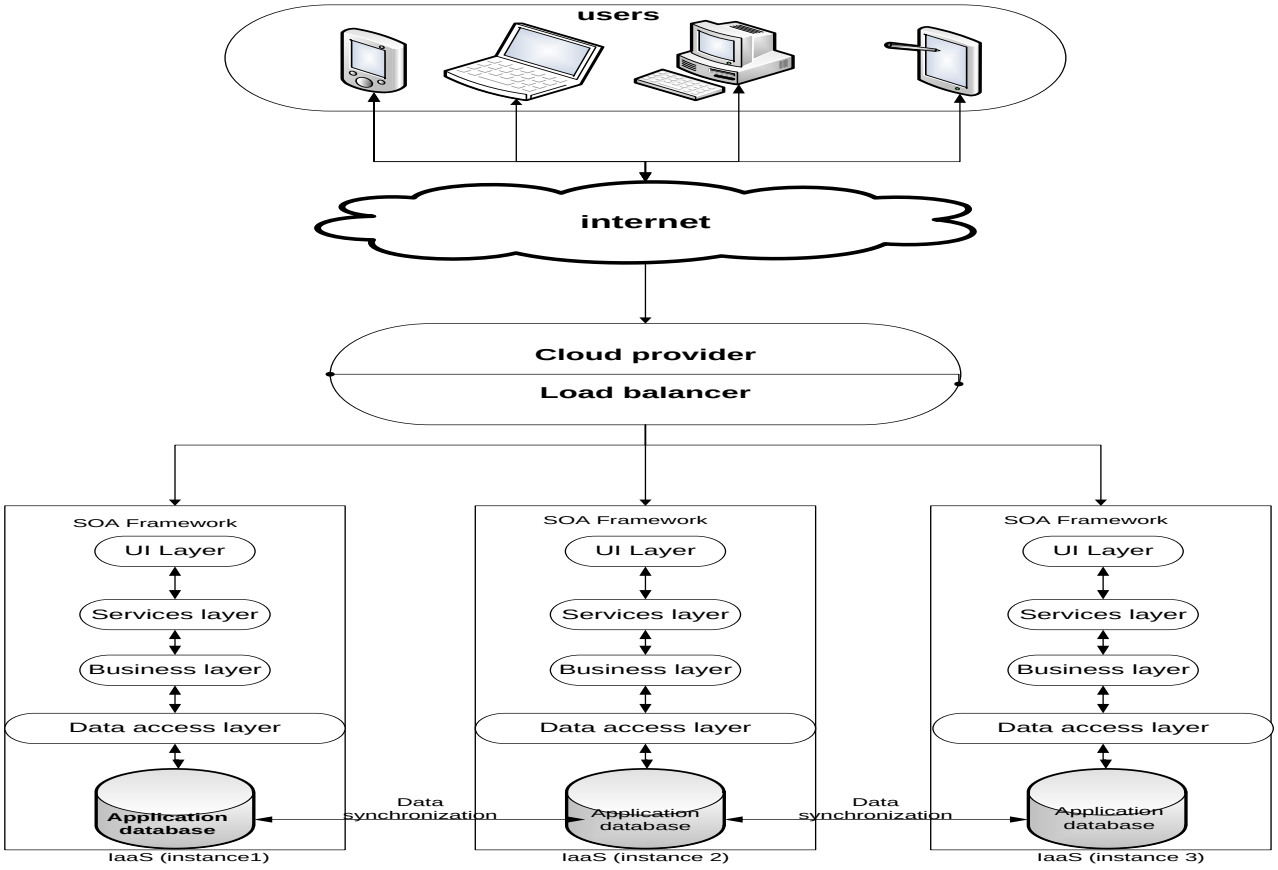


Figure- 4 the proposed VLS Architecture

The user interface tier is built using HTML and ASP, the tier uses the web browser through which the users are rendered the services.
In this system design model we used SOA based approach by means of web services the user request is sent to the services and business logic tier which consist of the web services, the request I XML are sent through SOAP or REST communication model. The third layer is data access tier for which we use SQL the web services in the services and business logic tier communicate with the database using MySQL.
The users of this virtual learning system use the web browser to access the system application the user interface of the application is rendered in the browser, so the users can use any desktop computer, smartphone, tablet etc.

The system will be host in cloud platform the user request will send to the particular cloud provider such as windows Azure or Amazon EC2.According to the number of the requests or the load status in the system the load balancer can route requests to particular instance in which VLS is running.
The application designed using SOA Architecture which consists of a user interface (UI) layer, a service and business component layer and the data access layer. Once the UI layer sends a service request through the rendered GUI, the service request is then sent to the service and business layer for processing. The request reaches to the service layer through SOAP in XML code. This layer consists of all the published web services of the virtual learning system for external interfaces. The service layer communicates with the underlying business layer using web services. The data access layer is also implemented using web services. The business layer invokes the published service to perform operations. The data access layer uses MySQL to interact with the actual database

6. CONCLUSION

The Proposed integrated Architecture is implemented based on the SOA based system development methodology. The methodology has been developed using the concepts in SOA and Cloud Computing Technology, to solve the problems lies in cross system virtual learning access. Cloud can provide advantages in scalability, self-services, pay-as-you-go, flexibility, agility, and device and location independence [11].The systems using SOA based methodology will works well as it uses the architectural approach of designing loosely coupled systems. These loosely coupled systems when deployed on the cloud platform enhance the scalability since the client can invoke the web services on any of the instances in the cloud.
The proposed model composed of various e-learning systems to enable learning and teaching services and resources sharing anywhere anytime by anybody without limitation of cross-system access. So this flexible and integrated architecture will allow the users to use heterogeneous set of services that support deferent learning and teaching activities.
In future we will make to expand and maximize our architecture to include more services which are useful to any one concern in the domain of e-learning such as M-learning. And try to take care of security issues, because all the cloud providers do not have the same capabilities for their services and technologies.

7. AUTHORS PROFILE

Mohammed Eltahir Abdelhag He has bachelor degrees in Information System from International University of Africa, Sudan in 2003, and got Master degree in Information Technology 2007 from Al-Neelain University, Sudan. He is currently working as a lecturer at Department of Information System, Jazan University, KSA and PhD candidate at National Ribat University, His main research interests include services oriented computing, distributed systems architectures for the integration of service-like tools in Learning Management System, cloud computing and e-learning.

Prof.Saife Eldin Osman Fatoh received his MSc and PhD degrees in computer science. He is currently a full professor at National Ribat University, Sudan, and the Dean of Emirates College for Science & Technology, Sudan. His main research interests include artificial intelligence, biometric and services oriented applications.

8. REFERENCES

[1]Service-oriented architecturehttp://publib.boulder.ibm.com/infocenter/wsdoc400/v6r0/index.jsp?topic=/com.ibm.websphere.iseries.doc/info/ae/ae/cwbs_soa.htm2014

[2]service-oriented architecture (SOA) http://searchsoa.techtarget.com/definition/service-oriented-architecture2014

[3] http://en.wikipedia.org/wiki/Web_service. 2014

[4] Y. L. Chi, Introduction to Web Service Technology, Chiun-Hua Publishing Company, Taipei,2004.

[5] Modeling in the Service Oriented Architecture https://software.intel.com/en-us/articles/modeling-in-the-service-oriented-architecture 2014

[6]Cloud computing http://searchcloudcomputing.techtarget.com/definition/cloud-computing

[7] virtual learning environment 2014 http://en.wikipedia.org/wiki/Virtual_learning_environment

[8] systems integration http://en.wikipedia.org/wiki/Systems_integration

[9]Gold-Bernstein, Beth; Ruh, William A (2005), Enterprise integration: the essential guide to integration solutions, Addison Wesley, ISBN 0-321-22390-X

[11] Bowen, F. (2009, November 4). How SOA can ease your move to cloud computing. Retrieved March 8, 2010, from http://www-01.ibm.com/software/solutions/soa/newsletter/nov09/article_soaandcloud. Html

[12] Linthicum, D. S. (2009). Cloud computing and SOA convergence in your enterprise: A step-by-step guide (1st ed.). Reading, MA: Addison-Wesley.

[13] Hood, C. C., & Bougourd, S. (2011). Research essay: The ethics of e-health. International Journal of E-Health and Medical Communications, 2(2),82–85. http://www.irma-international.org/viewtitle/53822/

[14] Huddle, C. (2009, July 24). Cloud computing and EHR/EMR. Retrieved March 8, 2010, from http://www.sevocity.com/index.php?option=com_content&view=article&id=140%3Acloudcomputing-and-ehremr&Itemid=43

[15]Zheng He & Jingxia Vue (2012) Integrating E-Learning System Based on Cloud Computing : 2012 IEEE International Conference on Granular Computing

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 119 - 125, 2015, ISSN:- 2319–8656

Superconductivity and Spin Density Wave (SDW) in $NaFe_{1-x}Co_xAs$

Haftu Brhane
Department of Physics,
College of Natural and Computational Sciences,
Haramaya University, Dire- Dawa,
Ethiopia

Amarendra Rajput
Department of Physics,
College of Natural and Computational Sciences,
Haramaya University, Dire- Dawa,
Ethiopia

Abstract: A model is presented utilizing a Hamiltonian with equal spin singlet and triplet pairings based on quantum field theory and green function formalism, to show the correlation between the superconducting and spin density wave (SDW) order parameters. The model exhibits a distinct possibility of the coexistence of superconductivity and long-range magnetic phase, which are two usually incompatible cooperative phenomena. The work is motivated by the recent experimental evidences on high-T_C superconductivity in the FeAs-based superconductors. The theoretical results are then applied to show the coexistence of superconductivity and spin density wave (SDW) in $NaFe_{1-x}Co_xAs$**.**

Keywords: Retarded double time green's function formalism, Spin singlet and triplet state, superconductivity and spin density wave.

1. INTRODUCTION

Since the discovery of superconductivity in quaternary pnictide-oxides with critical temperatures (T_C) up to 55 K, a lot of tremendous interest has been generated in the study of co-existence of the two cooperative phenomena of superconductivity and magnetism. After first reports on superconductivity in undoped LaNiPO [1, 2] below 5 K, the breakthrough was the discovery of the phenomena at T_C - 26K in the F-doped arsenide LaO1−xFxFeAs system [3].

In addition to this several groups reported an increase of Tc values by replacing La with smaller-size rare-earth ions like $CeO_{1-x}F_xFeAs$ [4], and samarium-arsenide oxides $Sm(O_{1-x}F_x)FeAs$ with a critical temperature T_c of 55K [5,6]. The iron based superconductors promise interesting physics and applications. While the interplay of superconductivity and magnetism, as well as their mechanisms remain the issues of active studies, one thing in FeSC riddle is clear, that it is the complex multi-band electronic structure of these compounds that determines their rich and puzzling properties. What is important and captivating is that this complexity seems to play a positive role in the struggle for understanding the FeSC physics and also for search of the materials with higher T_c [7].

The FeSC is quite promising for applications. Having much higher H_c than cuprates and high isotropic critical currents [8], they are attractive for electrical power and magnet applications, while the coexistence of magnetism and superconductivity makes them interesting for spintronics [9]. All the compounds share similar electronic band structure in which the electronic states at the Fermi level are occupied predominantly by the Fe 3d electrons [7].

Scanning tunnelling microscopy studies of the local electronic structure of an underdoped $NaFe_{1-x}Co_xAs$ near the SDW and SC phase boundary. Spatially resolved spectroscopy directly reveals both SDW and SC gap features at the same atomic location, providing compelling evidence for the microscopic coexistence of the two phases. The strengths of SDW and SC features are shown to anticorrelate with each other, indicating the competition of the two orders. The underlying physical picture is that Cooper pairing in the iron pnictides can occur when portions of the Fermi surface (FS) are already gapped by the SDW order [10].

The above exciting discovery stimulated a lot of interest in the study of coexistence of superconductivity and magnetism. The proximity of the superconductivity state to the spin density wave phase in the phase diagram implies that the interplay between the magnetism and superconductivity might play an important role in understanding the pairing mechanism and other physical properties of the iron-based superconductors. It is generally believed that the magnetic couplings between the itinerant electrons and/or between the itinerant electron and local spin are essential to both spin density wave instability and superconductivity. Besides other experimental and theoretical findings, especially the antiferromagnetic ground state and the SDW anomaly of LaFeAsO strongly suggest that, the pairing mechanism of the electrons is likely to be connected with spin fluctuations, as it has been assumed for the cuprates [11].

In many high T_C superconductors, superconducting mechanism is attributed to strong coulomb interactions of the electrons in the system, which can also be the cause for the appearance of SDW state and this suggests the existence of competition between the two states [12]. The properties of unconventional triplet superconductivity and SDW with an emphasis on the analysis of their order parameters are reviewed.

The relation between the superconducting and spin-density-wave (SDW) order is a central topic in current research on the FeAs-based high T_C superconductors. So, in this paper, we start with a model Hamiltonian which incorporates the BCS theory for iron pnictide superconductors $NaFe_{1-x}Co_xAs$, to examine the coexistence of superconductivity and spin density wave.

2. MODEL HAMILTONIAN OF THE SYSTEM

The purpose of this work is to study theoretically the co-existence of spin density wave and superconductivity

properties in the compound $NaFe_{1-x}Co_xAs$ in general and to find expression for transition temperature and order parameter in particular. For this purpose, we tried to find the mathematical expression for the superconducting critical temperature (T_c), superconducting order parameter (Δ_{sc}) the magnetic order parameter (M) and SDW transition temperature (T_{SDW}). Within the framework of the BCS model, the model of the Hamiltonian for coexistence SDW and superconductivity in the compound can be express as:

$$H = \sum_{p\sigma} \epsilon_p \hat{a}^{\dagger}_{p\sigma}\hat{a}_{p\sigma} + M\sum_{p}(\hat{a}^{\dagger}_{p+q\uparrow}\hat{a}_{-p\downarrow} + \hat{a}^{\dagger}_{-p\downarrow}\hat{a}_{p+q\uparrow}) + \Delta_{SC}\sum_{p}(\hat{a}^{\dagger}_{p\uparrow}\hat{a}^{\dagger}_{-p\downarrow} + \hat{a}_{-p\downarrow}\hat{a}_{p\uparrow}) \quad (1)$$

Where $(\hat{a}^{\dagger}_{p\sigma}\hat{a}_{p\sigma})$ are the creation (annihilation) operators of an electron having the wave number p and spinσ. Whereas (Δ_{SC}) superconducting order parameter and (M) SDW order parameters. The Hamiltonian in (1) will be used to determine the equations of motion in terms of the Green function.

3. COUPLING OF SDW AND SUPERCONDUCTING ORDER PARAMETERS

The Double time dependent Green's function equal to the change of the average value of some dynamic quantity by the time t and useful because they can be used to describe the effect of retarded interactions and all quantities of physical interest can be derived from them. To get the equation of motion we use the double-time temperature dependent retarded Green function is given by Zubarev [13]:

$$G_r(t-t') \equiv \ll \hat{A}(t); \hat{B}(t') \gg$$

$$\text{or } G_r(t,t') = -i\theta(t-t') < [\hat{A}(t), \hat{B}(t')] > \quad (2)$$

Where $\hat{A}$ and $\hat{B}$ are Heisenberg operators and $\theta(t-t')$ is the Heaviside step function. Now, using Dirac delta function and Heisenberg operators, we can write as;

$$i\frac{d}{dt}G_r(t-t') = \delta(t-t') < [\hat{A}(t), \hat{B}(t')] > + << [\hat{A}(t), H], \hat{B}(t')] >>$$

The Fourier transformation $G_r(\omega)$ is given by

$$G_r(t-t') = \int G_r(\omega)\exp[-i\omega(t-t')]d\omega \quad (3)$$

Taking the Fourier transform we get:

$$\omega G_r(\omega) = < [\hat{A}(t), \hat{B}(t')] >_{\omega} + \ll [\hat{A}(t), H], \hat{B}(t')] \gg_{\omega} \quad (4)$$

From (4), it follows that

$$\omega \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = \ll [\hat{a}^{\dagger}{}_{\kappa\uparrow}, H], \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (5)$$

where the anti-commutation relation,

$$\{\hat{a}_{\kappa\sigma}, \hat{a}^{\dagger}{}_{k'\sigma'}\} = \delta_{kk'}\delta_{\sigma\sigma'} \quad (6)$$

has been used. To derive an expression for $\ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg$, we have calculate the commutator $[\hat{a}^{\dagger}{}_{\kappa\uparrow}, H]$, using (1) and using the identities and

$$[A, BC] = \{A, B\}C - B\{A, C\} \quad \text{and} \quad [AB, C] = A\{B, C\} - \{A, C\}B \quad (7)$$

Solving the commutator in eq.(5) by using the Hamiltonian in eq.(1), we get

$$\left[\hat{a}^{\dagger}{}_{\kappa\uparrow}, \sum_{p\sigma}\epsilon_p\hat{a}^{\dagger}_{p\sigma}\hat{a}_{p\sigma}\right] = \sum_{p\sigma}\epsilon_p[\hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{p\sigma}\hat{a}_{p\sigma}]$$

$$= \sum_{p\sigma}\epsilon_p(\{\hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}_{p\sigma}\}\hat{a}_{p\sigma} - \hat{a}^{\dagger}_{p\sigma}\{\hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}_{p\sigma}\}$$

$$\left[\hat{a}^{\dagger}{}_{\kappa\uparrow}, \sum_{p\sigma}\epsilon_p\hat{a}^{\dagger}_{p\sigma}\hat{a}_{p\sigma}\right] = -\epsilon_{\kappa}\hat{a}^{\dagger}{}_{\kappa\uparrow} \quad (8a)$$

After some lengthy but straightforward calculations; we arrive at the following results:

$$\left[\hat{a}^{\dagger}{}_{\kappa\uparrow}, M\sum_{\kappa}(\hat{a}^{\dagger}_{\kappa+q\uparrow}\hat{a}_{-\kappa\downarrow} + \hat{a}^{\dagger}_{-\kappa\downarrow}\hat{a}_{\kappa+q\uparrow})\right] = -M\hat{a}^{\dagger}{}_{\kappa-q\downarrow} \quad (8b)$$

$$\left[\hat{a}^{\dagger}{}_{\kappa\uparrow}, \Delta_{SC}\sum_{p}(\hat{a}^{\dagger}_{p\uparrow}\hat{a}^{\dagger}_{-p\downarrow} + \hat{a}_{-p\downarrow}\hat{a}_{p\uparrow})\right] = -\Delta_{SC}\hat{a}_{-k\downarrow} \quad (8c)$$

Substituting (8) in to (5), we get

$$\omega \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = -\epsilon_{\kappa} \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg -M \ll \hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg -\Delta_{SC} \ll \hat{a}_{-k\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg$$

$$(\omega+\epsilon_{\kappa}) \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = -M \ll \hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg -\Delta_{SC} \ll \hat{a}_{-k\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (9)$$

The equation of motion for the correlation $\ll \hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg$ in (9) can be described as:

$$\omega \ll \hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = \delta_{kk'} + \ll [\hat{a}^{\dagger}{}_{\kappa-q\downarrow}, H], \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg$$

$$\omega \ll \hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = \ll [\hat{a}^{\dagger}{}_{\kappa-q\downarrow}, H], \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (10)$$

Evaluating the commutator in eq.(10) using Hamiltonian:

$$\left[\hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \sum_{p\sigma}\epsilon_p\hat{a}^{\dagger}_{p\sigma}\hat{a}_{p\sigma}\right] = \sum_{p\sigma}\epsilon_p[\hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}^{\dagger}{}_{p\sigma}\hat{a}_{p\sigma}]$$

$$= \sum_{p\sigma}\epsilon_p(\{\hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}^{\dagger}_{p\sigma}\}\hat{a}_{p\sigma} - \hat{a}^{\dagger}_{p\sigma}\{\hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}_{p\sigma}\}$$

$$\left[\hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \sum_{p\sigma}\epsilon_p\hat{a}^{\dagger}_{p\sigma}\hat{a}_{p\sigma}\right] = -\epsilon_{\kappa-q}\hat{a}^{\dagger}{}_{\kappa-q\downarrow} \quad (11a)$$

After some lengthy but straightforward calculations; we arrive at the following results:

$$\left[\hat{a}^{\dagger}{}_{\kappa-q\downarrow}, M\sum_{\kappa}(\hat{a}^{\dagger}_{\kappa+q\uparrow}\hat{a}_{-\kappa\downarrow} + \hat{a}^{\dagger}_{-\kappa\downarrow}\hat{a}_{\kappa+q\uparrow})\right] = -M\hat{a}^{\dagger}{}_{\kappa\uparrow} \quad (11b)$$

$$\left[\hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \Delta_{SC}\sum_{p}(\hat{a}^{\dagger}_{p\uparrow}\hat{a}^{\dagger}_{-p\downarrow} + \hat{a}_{-p\downarrow}\hat{a}_{p\uparrow})\right] = \Delta_{SC}\hat{a}_{-k+q\downarrow} \quad (11c)$$

Substituting (11) in to (10), we get

$$\omega \ll \hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = -\epsilon_{\kappa-q} \ll \hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg -M \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg +\Delta_{SC} \ll \hat{a}_{-k+q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg$$

$$(\omega+\epsilon_{\kappa-q}) \ll \hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = -M \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg + \Delta_{SC} \ll \hat{a}_{-k+q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (12)$$

Similarly as we did in the above the equation of motion for the correlation $\ll \hat{a}_{-\kappa+q\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg$ and $\ll \hat{a}_{-\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg$ is given by:

$$\omega \ll \hat{a}_{-\kappa+q\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = \epsilon_{-\kappa+q} \ll \hat{a}_{-\kappa+q\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg +M \ll \hat{a}_{-\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg + \Delta_{SC} \ll \hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg$$

$$(\omega-\epsilon_{-\kappa+q}) \ll \hat{a}_{-\kappa+q\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = M \ll \hat{a}_{-\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg + \Delta_{SC} \ll \hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (13)$$

and

$$(\omega-\epsilon_{-\kappa}) \ll \hat{a}_{-\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = 1 + M \ll \hat{a}_{-\kappa+q\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg - \Delta_{SC} \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (14)$$

From eq. (12), we obtain:

$$\ll \hat{a}^{\dagger}{}_{\kappa-q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = \frac{-M \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg}{(\omega+\epsilon_{\kappa-q})} + \frac{\Delta_{SC} \ll \hat{a}_{-k+q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg}{(\omega+\epsilon_{\kappa-q})} \quad (15)$$

And from eq. (14):

$$\ll \hat{a}_{-\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = \frac{1}{(\omega-\epsilon_{-\kappa})} + \frac{M \ll \hat{a}_{-\kappa+q\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg}{(\omega-\epsilon_{-\kappa})} - \frac{\Delta_{SC} \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg}{(\omega-\epsilon_{-\kappa})} \quad (16)$$

Plugging eq.(15) and (16) in (9), yields:

$$\left(\omega+\epsilon_{\kappa} - \frac{M^2}{(\omega+\epsilon_{\kappa-q})} - \frac{\Delta_{SC}{}^2}{(\omega-\epsilon_{-\kappa})}\right) \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = -\frac{\Delta_{SC}}{(\omega-\epsilon_{-\kappa})} - \left(\frac{M\Delta_{SC}}{(\omega+\epsilon_{\kappa-q})} + \frac{M\Delta_{SC}}{(\omega-\epsilon_{-\kappa})}\right) \ll \hat{a}_{-k+q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (17)$$

And insert eq. (15) and (16) in (13), we have:

$$\left((\omega-\epsilon_{-\kappa+q}) - \frac{M^2}{(\omega-\epsilon_{-\kappa})} - \frac{\Delta_{SC}{}^2}{(\omega+\epsilon_{\kappa-q})}\right) \ll \hat{a}_{-\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = \gg = -\frac{M}{(\omega-\epsilon_{-\kappa})} - \left(\frac{M\Delta_{SC}}{(\omega-\epsilon_{-\kappa})} + \frac{M\Delta_{SC}}{(\omega+\epsilon_{k-q})}\right) \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (18)$$

Applying nesting condition $\epsilon_{\kappa} = -\epsilon_{\kappa\pm q}$, $\epsilon_{-\kappa} = \epsilon_{\kappa\mp q}$ and use approximation, $\epsilon_{\kappa} = \epsilon_{-\kappa}$; eq.(17) and (14) becomes:

$$\left(\omega+\epsilon_{\kappa} - \frac{M^2}{(\omega-\epsilon_{\kappa})} - \frac{\Delta_{SC}{}^2}{(\omega-\epsilon_{k})}\right) \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = -\frac{\Delta_{SC}}{(\omega-\epsilon_{\kappa})} - \left(\frac{M\Delta_{SC}}{(\omega-\epsilon_{\kappa})} + \frac{M\Delta_{SC}}{(\omega-\epsilon_{\kappa})}\right) \ll \hat{a}_{-k+q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (19)$$

And

$$\left((\omega+\epsilon_{k}) - \frac{M^2}{(\omega-\epsilon_{k})} - \frac{\Delta_{SC}{}^2}{(\omega-\epsilon_{\kappa})}\right) \ll \hat{a}_{-\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = -\frac{M}{(\omega-\epsilon_{k})} - \left(\frac{M\Delta_{SC}}{(\omega-\epsilon_{k})} + \frac{M\Delta_{SC}}{(\omega-\epsilon_{k})}\right) \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (20)$$

Let $x = \omega+\epsilon_k$ and $y = \omega-\epsilon_k$

Then eq. (19) and (20) respectively becomes:

$$\left[xy - M^2 - \Delta_{SC}{}^2\right] \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = -\Delta_{SC} - 2M\,\Delta_{SC} \ll \hat{a}_{-k+q\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (21)$$

$$\left[xy - M^2 - \Delta_{SC}{}^2\right] \ll \hat{a}_{-k+q\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = -\Delta_{SC} - 2M\,\Delta_{SC} \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (22)$$

Finally we can express:

$$\ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = \frac{-1/2\,(\Delta_{SC}+M)}{\omega^2 - \epsilon_{\kappa}{}^2 - (\Delta_{SC}+M)^2} + \frac{-1/2\,(\Delta_{SC}-M)}{\omega^2 - -\epsilon_{\kappa}{}^2 - (\Delta_{SC}-M)^2} \quad (23)$$

Using the expression $\omega \to i\omega_n, \Delta_j(k) = -(-1)^j M$, where $\Delta_j(k)$ is effective order parameter and the Matsubara's frequency, we can write eq. (23) as:

$$\ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = \frac{1}{2}\sum_{j=1,2} \frac{\beta^2 \Delta_j(k)}{(2n+1)^2\pi^2 + \beta^2(\epsilon_{\kappa}{}^2 + \Delta_j{}^2(k))} \quad (24)$$

To take into account the temperature dependence of order parameters, we shall write as:

$$\Delta_{SC} = \frac{V}{\beta}\sum_{\kappa,n} \ll \hat{a}^{\dagger}_{\kappa\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (25)$$

$$M = \frac{U}{\beta}\sum_{k} \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}_{k-q\downarrow} \gg \quad (26)$$

Where $\beta = \frac{1}{KT}$

Using eq.(24) into eq.(25), we obtain

$$\Delta_{SC} = \frac{V}{2}\sum_{\kappa,n,j=1,2} \frac{\beta\Delta_j(k)}{(2n+1)^2\pi^2 + \beta^2(\epsilon_{\kappa}{}^2 + \Delta_j{}^2(k))} \quad (27)$$

Let us use

$$\gamma = \beta(\epsilon_{\kappa}{}^2 + \Delta_j{}^2(k))^{1/2} \quad (28)$$

and

$$\sum_{-\infty}^{\infty} \frac{1}{(2n+1)^2\pi^2 + \gamma} = \frac{tanh\,\gamma/2}{2\gamma} \quad (29)$$

Plugging eq.(28) and eq.(29) in eq.(27), we get:

$$\Delta_{SC} = \frac{V}{4}\sum_{j=1,2} \frac{\Delta_j(k) tanh\frac{\beta}{2}(\epsilon_{\kappa}{}^2 + \Delta_j{}^2(k))^{1/2}}{(\epsilon_{\kappa}{}^2 + \Delta_j{}^2(k))^{1/2}} \quad (30)$$

For mathematical convenience, we replace the summation in (27) by integration. Thus

$$\sum_{k} \equiv \int_{-\hbar\omega_b}^{\hbar\omega_b} N(0) d\epsilon_{\kappa}$$

where $N(0)$ is the density of states at the Fermi level.

The density of state $N(0) = N(2)_1 + N(0)_2$

Assume $N(2)_1 = N(0)_2$ this implies that $N(0)_2 = N(0)/2$. For j=2:

$$\Delta_{SC} = \alpha \int_0^{\hbar\omega_b} (\Delta_{SC} - M) \frac{tanh\frac{\beta}{2}(\epsilon_{\kappa}{}^2 + (\Delta_{SC}-M)^2)^{1/2}}{(\epsilon_{\kappa}{}^2 + (\Delta_{SC}-M)^2)^{1/2}} d\epsilon_{\kappa} \quad 31$$

Where $\alpha = N(0)_2 V$

Finally we can write eq.(31) as:

$$\frac{1}{\alpha} = \int_0^{\hbar\omega_b} (1 - \frac{M}{\Delta_{SC}}) \frac{tanh\frac{\beta}{2}(\epsilon_\kappa{}^2 + (\Delta_{SC} - M)^2)^{1/2}}{(\epsilon_\kappa{}^2 + (\Delta_{SC} - M)^2)^{1/2}} d\epsilon_\kappa \quad (32)$$

From (32), it clearly follows that the order parameters Δ_{SC} *and* M , for superconductivity and SDW are interdependent.

We now consider the equations of motion for SDW, we can write,

$$\omega \ll \hat{a}^\dagger{}_{\kappa\uparrow}, \hat{a}_{k-q\downarrow} \gg = \delta_{Kk'} + \ll [\hat{a}^\dagger{}_{\kappa\uparrow}, H], \hat{a}_{k-q\downarrow} \gg \quad (33)$$

Doing a lot as we did in the above, we finally get:

$$(\omega + \epsilon_\kappa) \ll \hat{a}^\dagger{}_{\kappa\uparrow}, \hat{a}_{k-q\downarrow} \gg = -M \ll \hat{a}^\dagger{}_{\kappa-q\downarrow}, \hat{a}_{k-q\downarrow} \gg - \Delta_{SC} \ll \hat{a}_{-k\downarrow}, \hat{a}_{k-q\downarrow} \gg \quad (34)$$

$$(\omega + \epsilon_{\kappa-q}) \ll \hat{a}^\dagger{}_{\kappa-q\downarrow}, \hat{a}_{k-q\downarrow} \gg = 1 - M \ll \hat{a}^\dagger{}_{\kappa\uparrow}, \hat{a}_{k-q\downarrow} \gg + \Delta_{SC} \ll \hat{a}_{-k+q\uparrow}, \hat{a}_{k-q\downarrow} \gg \quad (35)$$

$$(\omega - \epsilon_{-\kappa+q}) \ll \hat{a}_{-k+q\uparrow}, \hat{a}_{k-q\downarrow} \gg = M \ll \hat{a}_{-k\downarrow}, \hat{a}_{k-q\downarrow} \gg + \Delta_{SC} \ll \hat{a}^\dagger{}_{\kappa-q\downarrow}, \hat{a}_{k-q\downarrow} \gg \quad (36)$$

And

$$(\omega - \epsilon_{-\kappa}) \ll \hat{a}_{-k\downarrow}, \hat{a}_{k-q\downarrow} \gg = M \ll \hat{a}_{-k+q\uparrow}, \hat{a}_{k-q\downarrow} \gg - \Delta_{SC} \ll \hat{a}^\dagger{}_{\kappa\uparrow}, \hat{a}_{k-q\downarrow} \gg \quad (37)$$

Doing a lot as we did in the previous, we finally get:

$$\ll \hat{a}^\dagger{}_{\kappa\uparrow}, \hat{a}_{k-q\downarrow} \gg = \frac{1}{2} \sum_{j=1,2} \frac{(-1)^j \beta^2 \Delta_j(k)}{(2n+1)^2\pi^2 + \beta^2(\epsilon_k^2 + \Delta_j^2(k))} \quad (38)$$

Using eq.(38) in to eq.(26), the SDW order Parameter M is given by:

$$M = -\frac{U}{2} \sum_{k,n,j=1} \frac{\beta \Delta_j(k)}{(2n+1)^2\pi^2 + \beta^2(\epsilon_\kappa{}^2 + \Delta_j{}^2(k))} \quad (39)$$

Or

$$M = \frac{-U}{4} \sum_{j=1} \frac{\Delta_j(k) tanh\frac{\beta}{2}(\epsilon_\kappa{}^2 + \Delta_j{}^2(k))^{1/2}}{(\epsilon_\kappa{}^2 + \Delta_j{}^2(k))^{1/2}} \quad (40)$$

So, finally we get:

$$M = -\alpha_j \Delta_j \int_0^{\hbar\omega_b} \frac{tanh\frac{\beta}{2}(\epsilon_\kappa{}^2 + \Delta_j{}^2(k))^{1/2}}{(\epsilon_\kappa{}^2 + \Delta_j{}^2(k))^{1/2}} d\epsilon_\kappa \quad (41)$$

From (41), it is again evident that the order parameters Δ_{SC} *and* M , for superconductivity and SDW are interdependent, as was the case from (32).

It is, therefore, possible that in some temperature interval, SDW and superconductivity can co-exist, although one phase has a tendency to suppress the critical temperature and the order parameter of the other phase.

4. DEPENDENCE OF THE MAGNETIC ORDER PARAMETER ON THE TRANSITION TEMPERATURE FOR SUPERCONDUCTIVITY AND SDW

To study eq.(32), we consider the case, when $T \to 0K, \beta \to \infty$

We can then replace

$$tanh\frac{\beta}{2}(\epsilon_\kappa{}^2 + (\Delta_{SC} - M)^2)^{1/2} \to 1$$

In (32) and get,

$$\frac{1}{\alpha} = \int_0^{\hbar\omega_b} (1 - \frac{M}{\Delta_{SC}}) \frac{1}{(\epsilon_\kappa{}^2 + (\Delta_{SC} - M)^2)^{1/2}} d\epsilon_\kappa$$

Using the integral relation,

$$\int \frac{y}{\sqrt{y^2 + x^2}} dx = y sin^{-1}(x/y)$$

$$\frac{1}{\alpha} = \left(1 - \frac{M}{\Delta_{SC}}\right) sin^{-1} \frac{(\hbar\omega_b)}{(\Delta_{SC} - M)} \quad (42)$$

the above equation reduces to,

$$\Delta_{SC} - M = 2\hbar\omega_b \exp\left(-\frac{1}{\alpha\left(1 - \frac{M}{\Delta_{SC}}\right)}\right) \quad (43)$$

from the BCS theory, the order parameter Δ_{SC}, at T=0 for a given superconductor with transition temperature T_C is given by

$$2\Delta_{SC}(0) = 3.53 k_B T_c$$

using this result in (43), we obtain

$$M = 1.75 k_B T_c - 2\hbar\omega_b \exp\left(-\frac{1}{\alpha\left(1 - \frac{M}{1.75 k_B T_c}\right)}\right) \quad (45)$$

To solve (45) numerically we use Debay temperature and the interband BCS coupling constant.

To estimate α, we consider the cas $T \to T_c$

which implies, $\Delta_{SC} \to 0$

From (32), we then have

$$\frac{1}{\alpha} = \int_0^{\hbar\omega_b} \frac{tanh\frac{\beta}{2}(\epsilon_\kappa{}^2 + (\Delta_{SC} - M)^2)^{1/2}}{(\epsilon_\kappa{}^2 + (\Delta_{SC} - M)^2)^{1/2}} d\epsilon_\kappa - \int_0^{\hbar\omega_b} \frac{M}{\Delta_{SC}} \frac{tanh\frac{\beta}{2}(\epsilon_\kappa{}^2 + (\Delta_{SC} - M)^2)^{1/2}}{(\epsilon_\kappa{}^2 + (\Delta_{SC} - M)^2)^{1/2}} d\epsilon_\kappa$$

$$\frac{1}{\alpha} = I_1 - I_2 \quad (46)$$

$$\frac{1}{\alpha} = \int_0^{\hbar\omega_b} \frac{tanh\frac{\beta}{2}(\epsilon_\kappa{}^2 + (\Delta_{SC} - M)^2)^{1/2}}{(\epsilon_\kappa{}^2 + (\Delta_{SC} - M)^2)^{1/2}} d\epsilon_\kappa - \lim_{\Delta_{SC}\to 0} \int_0^{\hbar\omega_b} \frac{M}{\Delta_{SC}} \frac{tanh\frac{\beta}{2}(\epsilon_\kappa{}^2 + (\Delta_{SC} - M)^2)^{1/2}}{(\epsilon_\kappa{}^2 + (\Delta_{SC} - M)^2)^{1/2}} d\epsilon_\kappa$$

Putting $\tau^2 = \beta\sqrt{\epsilon_\kappa{}^2 + M^2}$ and for $\Delta_{SC} = 0$

we can write

$$I_1 = \int_0^{\hbar\omega_b} \frac{tanh\frac{\beta}{2}(\epsilon_\kappa{}^2 + M^2)^{1/2}}{(\epsilon_\kappa{}^2 + M^2)^{1/2}} d\epsilon_\kappa = \int_0^{\hbar\omega_b} \frac{2}{2\tau}\beta \tanh\tau/2\, d\epsilon_\kappa \quad (47)$$

Using Laplacian's transformation with Matsuber relation result we can write,

$$\int_0^{\hbar\omega_b} \frac{tanh\frac{\beta}{2}(\epsilon_\kappa{}^2 + M^2)^{1/2}}{(\epsilon_\kappa{}^2 + M^2)^{1/2}} d\epsilon_\kappa = \int_0^{\hbar\omega_b} \frac{tanh\,\beta\epsilon_\kappa/2}{\epsilon_\kappa} d\epsilon_\kappa - \int_0^{\hbar\omega_b} \frac{4}{\beta}\sum_{n=0}^{\infty} \frac{M^2}{a^4(1+x^2)^2}$$

Where $x^2 = \frac{\epsilon_\kappa{}^2}{a^2}$ and $a = (2n+1)\frac{\pi}{\beta}$ and using integrating by part,

$$\int_0^{\hbar\omega_b} \frac{tanh\frac{\beta}{2}(\epsilon_\kappa{}^2 + M^2)^{1/2}}{(\epsilon_\kappa{}^2 + M^2)^{1/2}} d\epsilon_\kappa = (\ln x)(\tanh x)\,\Big|_0^x - \int_0^x \frac{\ln x}{cosh^2 x} dx - \int_0^{\hbar\omega_b} \frac{4}{\beta}\sum_{n=0}^{\infty} \frac{M^2}{a^4(1+x^2)^2}$$

$$\int_0^{\hbar\omega_b} \frac{tanh\frac{\beta}{2}(\epsilon_\kappa{}^2 + M^2)^{1/2}}{(\epsilon_\kappa{}^2 + M^2)^{1/2}} d\epsilon_\kappa = ln\frac{\beta\hbar\omega_b}{2} - \ln(\pi/4\gamma) - M^2\left(\frac{1}{\pi k_\beta T_{SC}}\right)^2 1.052 \quad (48)$$

Using the fact that, for low temperature, $\tanh(\frac{\hbar\omega_b}{2k_BT}) \to 1$,

Where γ is the Euler constant having the value $\gamma = 1.78$ (Hsian) [14] and the last equation can be neglected since M^2 is very small.

we can write (48) as,

$$I_1 = \ln\left(1.14\frac{\hbar\omega_b}{k_B T_{sc}}\right) \quad (49)$$

Using L' Hospital's rule, it is easy to show that

$$I_2 = -\int_0^{\hbar\omega_b} (M^2\beta)\frac{sech^2(\frac{\beta\sqrt{\epsilon_\kappa{}^2 + M^2}}{2})}{2(\epsilon_\kappa{}^2 + M^2)} d\epsilon_\kappa$$

which can be neglected since M_{SDW}^2 is very small.

Substituting (49) in (46), we then obtain

$$\frac{1}{\alpha} = \ln\left(1.14\frac{\hbar\omega_b}{k_B T_C}\right)$$

This implies,

$$T_C = \frac{1.14\hbar\omega_b}{k_B}\exp\left(-\frac{1}{\alpha}\right), \quad (50)$$

which can be used to estimate $\exp\left(-\frac{1}{\alpha}\right)$ for $NaFe_{1-x}Co_xAs$, using the experimental value $T_{sc}$and cut-off energy.

To study how M depends on the magnetic transition temperature T_{SDW}, we consider (41).

$$M = -\alpha_j\Delta_j \int_0^{\hbar\omega_b} \frac{tanh\frac{\beta}{2}(\epsilon_\kappa{}^2 + \Delta_j{}^2(k))^{1/2}}{(\epsilon_\kappa{}^2 + \Delta_j{}^2(k))^{1/2}} d\epsilon_\kappa \quad (51)$$

Proceeding as before, it is easy to show that,

$$M = --\boldsymbol{\alpha_j}\Delta_j\left(\ln\left(1.14\frac{\hbar\omega_b}{k_B T_{SDW}}\right) - \Delta_j{}^2\left(\frac{1}{\pi k_\beta T_{SDW}}\right)^2 1.052\right)$$

Neglecting $\Delta_j{}^2$

$$M = -(\boldsymbol{\alpha_j}\Delta_j)\ln\left(1.14\frac{\hbar\omega_b}{k_B T_{SDW}}\right)$$

This gives;

$$\therefore\ T_{SDW} = \left(\frac{1.14\hbar\omega_b}{k_B}\right)\exp\left(\frac{M}{\boldsymbol{\alpha_j}\Delta_j}\right) \quad (52)$$

We can use (52) to draw the phase diagram for M and T_{SDW}.

5. PAIRING OF SPIN DENSITY WAVE (SDW) AND TRIPLET SUPERCONDUCTIVITY

In this section we want to drive an expressions for the order parameters of SDW, M, and triplet superconductivity, Δ_{SC}, as a function of both of them and temperature, and to compare the variation of each with temperature. Still we can use the Hamiltonian given by equation (1), but in this case the superconducting order parameter depends on spin alignment [15] and they can be expressed as;

$$H = \sum_{p\sigma} \epsilon_p \hat{a}_{p\sigma}^\dagger \hat{a}_{p\sigma} + M\sum_p (\hat{a}_{p+q\uparrow}^\dagger \hat{a}_{-p\downarrow} + \hat{a}_{-p\downarrow}^\dagger \hat{a}_{p+q\uparrow}) + \Delta_{SC}\sum_p (\hat{a}_{p\uparrow}^\dagger \hat{a}_{-p\downarrow}^\dagger + \hat{a}_{-p\downarrow}\hat{a}_{p\uparrow}) \quad (53)$$

where the superconducting order parameter is given by:

$$\Delta = \sum_P < \hat{a}_{k\sigma}^\dagger, \hat{a}^\dagger{}_{-k\sigma} > \quad (54)$$

We now consider the equation of motion:

$$\omega \ll \hat{a}^{\dagger}{}_{k\sigma}, \hat{a}^{\dagger}{}_{-k\sigma} \gg = \ll \left[\hat{a}^{\dagger}{}_{k\sigma}, H\right], \hat{a}^{\dagger}{}_{-k\sigma} \gg \quad (55)$$

Doing a lot as we did in the above for the commutation and using the assumption $\delta_{\sigma,\downarrow} = 1, \delta_{\sigma,\uparrow} = 0$ we finally get:

$$(\omega+\epsilon_{\kappa}) \ll \hat{a}^{\dagger}{}_{\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = -M \ll \hat{a}^{\dagger}{}_{\kappa+q\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg - \Delta_{k\downarrow} \ll \hat{a}_{-k\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (56)$$

The nesting property of the Fermi surface that expected for low dimensional band structure and attributed to the SDW ordering gives as an expression $\Delta_{-k} = -\Delta_{k}$.

Finally:

$$(\omega+\epsilon_{\kappa}) \ll \hat{a}^{\dagger}{}_{\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = -\Delta_{k\downarrow} \ll \hat{a}_{-k\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (57)$$

Since we are dealing with only the triplet pair; we can ignore the singlet correlation.

The equation of motion for correlation in RHS of (57) is written as:

$$(\omega-\epsilon_{-\kappa}) \ll \hat{a}_{-k\downarrow}, \hat{a}^{\dagger}{}_{-k\downarrow} \gg = 1 + M \ll, \hat{a}_{-k+q\uparrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg - \Delta_{k\downarrow} \ll \hat{a}^{\dagger}{}_{\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (58)$$

and

$$\left(\omega-\epsilon_{-\kappa+q}\right) \ll \hat{a}_{-k+q\uparrow}, \hat{a}^{\dagger}{}_{-k\downarrow} \gg = M \ll \hat{a}_{-k\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (59)$$

This can be rewritten, after solving the commutation relation and removing the singlet pair.

From eq.(58) and (59), we will get;

$$(\omega-\epsilon_{-\kappa}) \ll \hat{a}_{-k\downarrow}, \hat{a}^{\dagger}{}_{-k\downarrow} \gg = 1 + \frac{M^2}{(\omega-\epsilon_{\kappa+q})} \ll \hat{a}_{-k\downarrow}, \hat{a}^{\dagger}{}_{-k\downarrow} \gg - \Delta_{k\downarrow} \ll \hat{a}^{\dagger}{}_{\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg \quad (60)$$

With help of eq.(60) and eq.(57):

$$\frac{XYR - XM^2 - R\Delta_{K\downarrow}^2}{YR - M^2} \ll \hat{a}^{\dagger}{}_{\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = \frac{-\Delta_{K\downarrow}}{YR - M^2} \quad (61)$$

This can be written as:

$$\ll \hat{a}^{\dagger}{}_{\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = \frac{-\Delta_{K\downarrow} R}{XYR - XM^2 - R\Delta_{K\downarrow}^2} \quad (62)$$

Applying nesting condition $\epsilon_{\kappa} = -\epsilon_{\kappa\pm q}$, $\epsilon_{-\kappa} = \epsilon_{\kappa\mp q}$ and use approximation, $\epsilon_{\kappa} = \epsilon_{-\kappa}$; eq.(62) becomes:

$$\ll \hat{a}^{\dagger}{}_{\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg = \frac{-\Delta_{K\downarrow}}{XY - M^2 - \Delta_{K\downarrow}^2} \quad (63)$$

Using the expression $\omega \to i\omega_n$, eq.(29) and Matsubara's frequency, we can write eq. (63) as:

$$\Delta_{k'\downarrow} = V \sum_{k} \frac{\Delta_{k\downarrow} tanh \frac{\left(\sqrt{\epsilon_{\kappa}{}^2 + M^2 + \Delta_{k\downarrow}{}^2}\right)}{2k_B T}}{2\sqrt{\epsilon_{\kappa}{}^2 + M^2 + \Delta_{k\downarrow}{}^2}} \quad (64)$$

Where

$$\Delta_{k'\downarrow} = \frac{V}{\beta} \sum_{k,n} \ll \hat{a}^{\dagger}{}_{\kappa\downarrow}, \hat{a}^{\dagger}{}_{-\kappa\downarrow} \gg$$

$$\Delta_{k'\downarrow} = \frac{V}{\beta} \sum_{k,n} \frac{\Delta_{K\downarrow}}{\omega_n^2 + E_k^2}$$

and $E_k^2 = \boldsymbol{\epsilon_{\kappa}}^{\mathbf{2}} + M^2 + \Delta_{\downarrow}^{\mathbf{2}}$

By taking an approximation over the superconducting order parameter, such that it is independent of wave vector, finally we get:

$$1 = V \sum_{k} \frac{tanh \frac{\left(\sqrt{\epsilon_{\kappa}{}^2 + M^2 + \Delta_{\downarrow}{}^2}\right)}{2k_B T}}{2\sqrt{\epsilon_{\kappa}{}^2 + M^2 + \Delta_{\downarrow}{}^2}} \quad (65)$$

We now consider the equations of motion for SDW, we can write,

$$\omega \ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}_{k-q\downarrow}, \gg = \ll \left[\hat{a}^{\dagger}{}_{k\sigma}, H\right], \hat{a}^{\dagger}{}_{-\kappa\sigma} \gg \quad (66)$$

Doing a lot as we did in the above, we finally get:

$$\ll \hat{a}^{\dagger}{}_{\kappa\uparrow}, \hat{a}_{k-q\downarrow}, \gg = \frac{-M}{XZR - \Delta_{k-q\downarrow}^2 X - M^2 R} \quad (67)$$

So,

$$1 = U \sum_{k} \frac{\boldsymbol{tanh} \frac{\left(\sqrt{\boldsymbol{\epsilon^2} + \Delta_{\downarrow}^2 + M^2}\right)}{\boldsymbol{2k_B T}}}{\mathbf{2}\sqrt{\boldsymbol{\epsilon^2} + \Delta_{\downarrow}^2 + \boldsymbol{M^2}}} \quad (\mathbf{68})$$

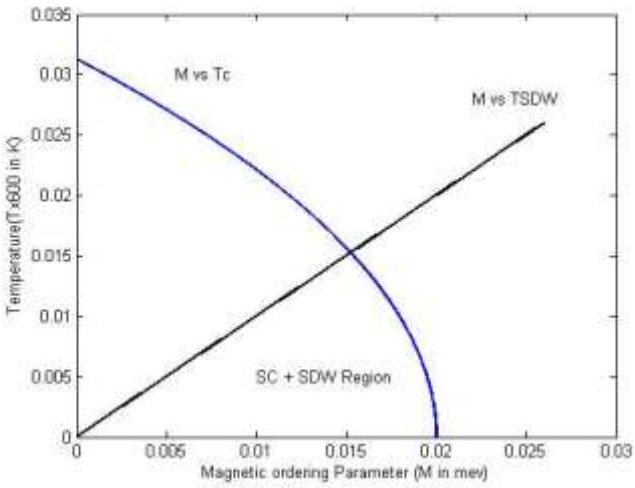


Figure. 1 Co-existence of superconductivity and spin density wave (SDW) in $NaFe_{1-x}Co_xAs$.

6. RESULTS AND CONCLUSION

In Fig. 1 we have presented the theoretical curve of the magnetic order parameter M as a function of the superconducting temperature T_C. For this purpose, we have used (45) which have been numerically solved using the relevant parameters for $NaFe_{1-x}Co_xAs$. In the same figure, we have also plotted the curve of M as a function of T_{SDW}, using (52). This curve is found to be almost linear up to the experimental value of T_{SDW}=18k for $NaFe_{1-x}Co_xAs$.

From Fig. 1 we observe that T_C decreases with increase in M, whereas T_{SDW} increases with increase in M. The superconducting phases and spin density wave, therefore,

resist each other. However, the present work shows that there is a small region of temperature, where both the phases may be in existence together which is indicated by (SC+SDW) in the Figure. Thus using a model Hamiltonian consisting of spin density wave and superconducting part and applying Green's function formalism it is possible to derive an expression which shows the relation of the two order parameters and their variation with temperature. This has been done both for singlet and triplet phases of superconductivity coexisting with spin density wave. In the absence of spin density wave the expression for both singlet and triplet cases reduces to the well known BCS result. Our study explicitly shows that superconductivity and spin density wave truly coexist in $NaFe_{1-x}Co_xAs$.

7. REFERENCES

[1] Watanabe, T., Yanagi, H., Kamiya, T., Kamihara, Y., Hiramatsu, H., Hirano, M. and Hosono, H, Inorg. Chem. 46, 7719 (2007).

[2] Tegel, M., Bichler, D., and Johrendt, D. Solid State Sci. 10, 193 (2008).

[3] Kamihara, Y., Watanabe, Hirano, T., and Hosono, H. 2008. Iron-Based Layered Superconductor La[O1−xFx] FeAs (x = 0.05 – 0.12) with Tc = 26 K. *Journal of the American Chemical Society*, **130**, 3296-3297.

[4] Chen, G.F., Li, Z., Wu, D., Li, G., Hu, W.Z., Dong, J., Zheng, P., Luo, J.L. and Wang, N.L. 2008. Superconductivity at 41˚K and Its Competition with Spin-Density-Wave Instability in Layered CeO1−xFxFeAs. *Physical Review Letters*,

[5] Ren, Z.A., Lu, W., Yang, J., Yi, W., Shen, X.L., Li, Z.C., Che, G.C., Dong, X.L., Sun, L.L., Zhou, F. and Zhao, Z.X.2008. Superconductivity at 55 K in Iron-Based F-Doped Layered Quaternary Compound Sm[O1−xFx]FeAs. *Chinese Physics Letters*, **25**, 2215.

[6] Kenji, I., Yusuke, N. and Hideo H. 2009. To What Extent Iron-Pnictide New Superconductors Have Been Clarified. *Journal of the Physical Society of Japan*, **78**, ArticleID:062001.http://dx.doi.org/10.1143/JPSJ.78.062 01

[7] Kordyuk, A.A. 2012. Iron-Based Superconductors: Magnetism, Superconductivity, and Electronic Structure. *Low Temperature Physics*, **38**, 1119-1134.

[8] M. Putti et al., Supercond. Sci. Technol. 23, 034003 2010.

[9] Patel et al., Appl. Phys. Lett. 94, 082508 2009.

[10] Cai, P. et al. Visualizing the microscopic coexistence of spin density wave and superconductivity in underdoped NaFe1_xCoxAs. Nat. Commun. 4:1596 doi: 10.1038/ncomms2592 (2013).

[11] Marianne Rotter, Marcus Tegel and Dirk Johrendt, 2008. Superconductivity at 38 K in the iron arsenide (Ba1−xKx)Fe2As2. arXiv:0805.4630v1 [cond-mat.supr-con]

[12] Digor D. F. et.al., Moldavian Journal of the Physical Sciences, Vol.4, No. 4 (2005).

[13] Zubarev, D. N., 1960. Double-time green functions in statistical physics.usp. Fiz. Nauk. Sssr 71:7; Translation: Sov. Phys. Usp. 3, 320-345

[14] Hsian, P. C., 2011. Robust based band reed solomon detection over Power line channel. J.of Engg. Sc. and Tech; 6(1), 69 – 81.

[15] Zhou, Y., and Gong, C. D. Europhys. Lett., 74, No. 1, pp.
145150 (2006).

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 126 - 128, 2015, ISSN:- 2319–8656

A Survey on the Clustering Algorithms in Sales Data Mining

Mathew Ngwae Maingi
School Of Computing And Information Technology
Jomo Kenyatta University Of Agriculture And Technology
Nairobi, Kenya

Abstract: This paper discusses different clustering techniques that can be used in sales databases. The advancement of digital data collection and build up of data in data banks as a result of modernization in sales disciplines has brought in great challenges of data processing for better and meaningful results due to mass data deposits. Clustering techniques therefore are quite necessary so that the senior management in sales department can have access to processed data as they engage themselves in decision making processes. In this paper, I focus on the retail sales data mining, classification and clustering techniques. In this study I analyze the attributes for the prediction of buyer's behavior and purchase performance by use of various classification methods like decision trees, C4.5 algorithm and ID3 algorithm.

Keywords: clustering; databases; banks; discipline; management; ID3; algorithm; C4.5.

1. INTRODUCTION

In sales database systems, there exist many varieties of functions for handling many processes such as supply chain management, marketing strategies, market analysis performance in identifying new product issues, diagnosis of manufacturing problems causes and profiling existing customers with more accurate and tangible values. This huge collection of data values is either related or not related at all and thus definitely needs to be clustered otherwise much of the data deposited will not be useful to users. From data mining perspective, clustering method plays a very crucial role in knowledge discovery in such activities as cross marketing: increase the sales in season wise by updating the inventory, discount offers and store layout based on the knowledge discovered in the data.

2. WHAT IS A CLUSTERING ALGORITHM IN SALES DATA?

In today's world, an enterprise that processes over 15 million point-of-sale transactions a day in its database would most likely find that data of less use without analyzing it using data mining software. If that data from the point-of-sale system was properly analyzed using data mining techniques, this will enhance accurate: determination of sales trends, development of marketing campaigns, and prediction of customer dependability. Clustering algorithms therefore seek to group given data sets into groups based on identified features so that the data points within a group are more similar to each other than the points in different groups.

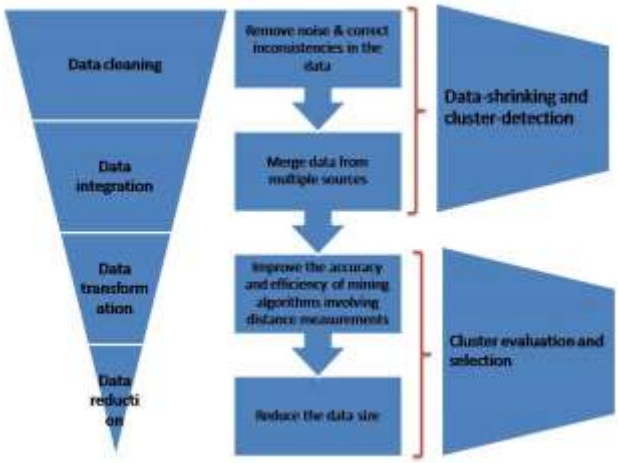


Figure 1 Data processing techniques in cluster formation.

In the figure 1 above, it is shown that there is need to clean data by removing the available outliers inorder to prepare it for use. Data integration entails merging sata from multiple sources so as to centralize it. Data transformation deals with accuracy and efficiency improvement of data mining algorithm hence fine tuning the resultant data. As a result, the sales data set can be extracted from sales transactions since these records are directly linked to the entire sales data. With such a technique, data values can be given as input data where else on the other hand in output it gives recommendations to management functions and extract new knowledge to the managers by using various data mining techniques like clustering, classification or pattern matching.

2.1 Goals and objectives clustering on sales data

Clustering seeks to group given data sets into groups based on identified features so that the data points within a group are more similar to each other than the points in different groups. The following are some of the advantages:

1. Prediction of customer purchasing behavior by grouping similar data points together into clusters hence generating knowledge based models.

2. Upgrading and advancing scientific knowledge discover through tangible analysis.

3. STAGES OF SALES DATA CLUSTERING

Sales data clustering is concerned with group given data sets into groups based on identified features. The process generally consists of three phases:

1. Feature selection and clustering algorithm formation. This phase deals with proper selection of the features on which the clusters are to be formed such as distance definition, clusters to be formed e.t.c.
2. Validation of the results that deals with the assessment of the quality and the reliability of the cluster sets. Clustering algorithms yield results that are not predictable despite the method used and therefore the final partition of data may need reevaluation.
3. Interpretation of the results. In the process of deriving the conclusion of any output, experts from the application areas integrates the clustering results with other experimental output and do the necessary analysis.

3.1 Clustering methods

There are various methods of clustering sales data where each uses a unique induction principle. All kinds of methods fall under one of the following subcategories:

1. **Hierarchical:** This category of clustering seeks to construct a hierachy of clusters using such strategies as: agglomerative and divisive. Agglomerative approach uses "bottom up" strategy where each observation starts in its own cluster, and pairs of clusters are merged as one moves up the hierarchy. Divisive strategy is a "top down" approach where all observations start in one cluster, and splits are performed recursively as one moves down the hierarchy. The major overall limitations of the hierarchical methods are: Inability to scale well—The time complexity of hierarchical algorithms is at least O(m2). Clustering a large number of objects using a hierarchical algorithm is also characterized by huge I/O costs. Hierarchical methods can never undo what was done previously. Hence lack of back-tracking capability. This approach above make the derived hierarchical tree more robust, however, it doesn't indicate how to cut the dendrogram to obtain meaningful clusters, either.
2. **Partitioning:** These methods relocate instances by moving them from one cluster to another starting from an initial partitioning. To achieve overall optimality in this type of clustering, an exhaustive enumeration process of all possible partitions is required. Because this is not feasible, certain greedy heuristics are used in the form of iterative optimization. The following subsections present various types of partitioning methods.
3. **Grid-based Algorithms:** In this method, partitions are created in the space to form finite number of cells that form a grid like structure where all clustering operations are performed. This method however has one advantage of being very fast in processing time regardless of the data size though dependent on the number of segments in each dimension in the quantized space. In the case of spatial data mining, the approach has been improved to reduce cost. Study shows that this approach performs very efficiently in the case where the data sets are very large.
4. **Density-based algorithms:** This method assumes that the points belonging to a specific cluster are drawn from a specific probability distribution. More so, the method describes the distribution of a data set by the density of the data objects hence, the entire process involves the search of the dense areas in the object space. The main aim of this approach is to identify clusters and their distribution parameters and is designed to discover clusters for arbitrary shape that are not convex. This approach is characterized by presence of noise within the data sets and this might interfere with the overall process of data mining. The approach also capitalizes on the ability to discover clusters with arbitrary shape and has good efficiency on large data sets, however, the approach is very sensitive to the input parameters hence it is prone to generating very different clustering results if subjected to slightly different parameter settings.

4. LITERATURE SURVEY

4.1 Predicting customer purchase in an online retail business, a Data Mining approach

In this research, Aniruddha Mazumdar, May 2010, studied, implemented and analyzed some data mining tools as well as techniques and later analyzed the sampled data for interpretation. In this study data mining algorithms were used based on the clustering algorithms in conjunction with an 'Apriori' based Association rule mining algorithm. The research discusses different approaches that were used in interpreting the results. The results clearly prove that:

Using the VQ approach one can easily segment groups of buyers based on the RFM values or all of them all together. However this process needs the initials vectors as its input for it to form clusters.

1. When predicting, different segmentations from the clusters formed can be used and the most populous ones are specifically focused on.
2. Basing on the association rules alongside sufficient coverage, the product which the customer wishes to buy is predictable along with the purchase of particular products.

4.1 Upgrading and advancing scientific knowledge discovery through tangible market analysis.

In this paper by Kavitha .N et al 2013, it is argued that despite the fact that there have been several techniques, like pattern discovery, association rule mining etc, these methods generates a large volume of frequent patterns and rules which are not useful for finding the essential patterns among them,

from the database. Therefore the discovery of hidden information present in databases and can be regarded as a step in overall process of Knowledge Discovery in databases (KDD) (Parashar, 2011)

A research paper by D. Bhanu, Dr. S. Pavai Madeshwari , 2009 proposes an architecture to be used to discover a customer-based rules if a retailer want to open his outlet at an entirely new location. However, if these rules were to be obtained, then a fuzzy clustering method would be used for customer and product domains and be bridged. Association rule mining and Fuzzy clustering get incorporated to analyze the similarity between customer groups and their preferences for products. Once a complete set of rules is generated, this is put in an independent knowledgebase from which any stated or needed customer needs can be categorized with the correspondence to customer groupings hence deducing the cluster to which a customer may belong.

5. CONCLUSION

This research paper describes the sales knowledge discovery, objectives and goals of sales knowledge discovery as well as the stages or phases of sales knowledge discovery together with the existing techniques of classification. It is clear that various techniques of classification can be implemented on the data set however it is worth noting that, the technique of classification to be applied on the data to improve customer analysis in purchasing is very important.
So this paper will provide a beneficial overview of existing solutions for classification and clustering methods with their advantages, limitations as well as the strengths of data clustering in decision making in an enterprise.

6. ACKNOWLEDGMENTS

I would like to express my sincere gratitude to almighty God, my supervisor Dr. Wilson Cheruiyot and his colleagues for helping me to undertake this research from start to completion. God bless you all.

7. REFERENCES

[1] Kaviha N. and Karthikeyan S. 2013. Customer Buying Behavior Analysis: A Clustered Closed Frequent Itemsets for Transactional Databases.
[2] Aniruddha Mazumdar. 2010. Predicting customer purchase in an online retail business-a data mining approach.
[3] D. Bhanu, Dr. S. Pavai Madeshwari 2009. Retail market analysis in targeting sales based on consumer behavior using Fuzzy Clustering – A rule based model.
[4] Wei Li, 2008. Modified K-means clustering algorithm IEEE computer society Congress on Image and Signal Processing, (May 2008), 618-621
[5] James Shields 2008. Getting to Know Your Customers by Clustering on Product Purchase Patterns

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 129 - 132, 2015, ISSN:- 2319–8656

Real Time Simulation of Security Systems using Face Recongnition, a review

Manisha Sajwan
DIT University
Dehradun, India

Abstract: In recent years face recognition has received substantial attention from both research communities and the market, but still remained very challenging in real applications. A lot of face recognition algorithms, along with their medications, have been developed during the past decades. In this paper we are going to present reviews about real time simulation of various security systems. These security systems are based on face detection, face tracking and face recognition. In this paper we will also present applications of real-time systems and some advancement that can be done in future to make security systems much faster. There are various algorithms available for face detection, tracking and recognition of human expressions This paper is the review of research work "spontaneous and different facial expressions and poses of individual person faces are detected and stored in the database of organization by giving appropriate and unique card id number and password. If a person comes for work then his or her face is detected and this detected face image is compared with images in the database of that particular organization and unique card id number and password. If the face image and id number are recognized then person is allowed to enter. If it is not recognized then person is not allowed to enter. An alert message is generated to administrator's cell phone and mail to the administrator's mail id. In the reverse we are changing the password by using random string generation and shut down the system".

Key-Words: Real-Time Simulation, Survey on Face recognition approaches, Application of Real-Time Security Systems.

1: INTRODUCTION:

The very first question that comes in our mind is that what is real time simulation? Real-time is a quantitative notion of time. Real-time is measured using a physical (real) clock. Whenever we quantify time using a physical clock, we deal with real time. In contrast to real time, logical time (also known as virtual time) deals with a qualitative notion of time and is expressed using event ordering relations such as before, after, sometimes, eventually, precedes, succeeds, etc. While dealing with logical time, time readings from a physical clock are not necessary for ordering the events.

A system is called a real-time system, when we need quantitative expression of time (i.e. real-time) to describe the behaviour of the system. This paper is basically a review paper or a survey paper for real time simulation of a security system using face recognition techniques for spontaneous and different human face expressions.

This paper is organised as follows:
Section 2 is the history behind face recognition and detection. Section 3 is the brief explanation of face recognition system. Section 4 outlines the real time system basic model. Section 5 describes conclusion and the last section is the outline of references.

2: LITERATURE SURVEY:

Studies on Facial Expressions and Physiognomy date back to the early Aristotelian era (4th century BC). Physiognomy is the assessment of a person's character or personality from their outer appearance, especially the face. But over the years, while the interest in Physiognomy has been waxing and waning, the study of facial expressions has consistently been an active topic.

Face recognition is one of the applications of image analysis. In 2009, a simple search on "Face Recognition" in the IEEE Digital Library throws 9422 results 1332 articles. Examples are Video surveillance, human-machine interaction, photo cameras, and virtual reality. Face recognition is a relevant term in pattern recognition, neural networks, computer graphics, image processing and psychology.

In the 1950's in psychology the work on this subject hasbeen made. They belong to other issues like face expressions, emotions and perception.

The research on this subject was Woodrow W. Bledsoe. During 1964 and 1965, Bledsoe, along with Helen Chanand Charles Bisson, worked on to recognize faces using computers.

He continued later his researches at Stanford Research Institute. Bledsoe designed and implemented a semi-automatic system. Some face coordinates were selected by a human operator, and then computers used this information for recognition. Face recognition allows variation in illumination, head rotation and aging. Researches trying to measure subjective face features as ear size or between-eye distance. In 1973, Fischler and Elschanger tried to measure similar features automatically.

Algorithm used local template matching to measure facial features. There were approaches back on the 1970's. A face as a set of geometric parameters and based on those parameters

performs some pattern recognition. In 1973 Kenade was developed a fully automated face recognition system. Kenade compares this automated extraction to a human or manual extraction, showing only a small difference. He got a correct identification rate of 45-75%.

In 1986, the Eigen Faces in image processing technique was made by L. Sirovich and Kirby.This methods were based on the Principal Component Analysis. The goal was to represent an image in a lower dimension without losing information, and then reconstructing it.

In 1990's, the recognition of the mentioned Eigen face approach was the first industrial applications. In1992, Mathew Turk and Alex Pentland of the MIT presented a work which used Eigen faces for recognition. Many approaches which has led to different algorithms like PCA, ICA, LDA and their derivatives. That algorithm was able to locate, track the subject's head.

The foundational studies on facial expressions that have formed the basis of today's research can be traced back to the 17th century.

A detailed note on the various expressions and movement of head muscles was given in 1649 by John Bulwer in his book *"Pathomyotomia"*.

Another interesting work on facial expressions (and Physiognomy) was by Le Brun, the French academician and painter. In 1667, Le Brun gave a lecture at the Royal Academy of Painting which was later reproduced as a book in 1734. It is interesting to know that the 18th century actors and artists referred to his book in order to achieve *"the perfect imitation of 'genuine' facial expressions"*. The interested reader can refer to a recent work by J. Montagu on the origin and influence of Le Brun's lectures.

Moving on to the 19th century, one of the important works on facial expression analysis that has a direct relationship to the modern day science of automatic facial expression recognition was the work done by Charles Darwin. In 1872, Darwin wrote a treatise that established the general principles of expression and the means of expressions in both humans and animals.

The first step towards the automatic recognition of facial expressions was taken in 1978 by Suwa et al. By the late 1980s and early 1990s, cheap computing power started becoming available. This led to the development of robust face detection and face tracking algorithms in the early 1990s. At the same time, Human-Computer Interaction and Affective Computing started gaining popularity. Researchers working on these fields realized that without automatic expression and emotion recognition systems4, computers will remain cold and unreceptive to the users' emotional state. All of these factors led to a renewed interest in the development of automatic facial expression recognition systems

Since the 1990s, (due to the above mentioned reasons) research on automatic facial expression recognition has become very active. Comprehensive and widely cited surveys by Pantic and Rothkrantz (2000) and Fasel and Luttin (2003) are available that perform an in-depth study of the published work from 1990 to 2001.

Humans communicate effectively and are responsive to each other's emotional states. Computers must also gain this ability. This is precisely what the Human-Computer Interaction research community is focusing on: namely, Affective Computing. Expression recognition plays a significant role in recognizing one's affect and in turn helps in building meaningful and responsive HCI interfaces. We can refer to Zeng et al.'s comprehensive survey to get a complete picture on the recent advances in Affect-Recognition and its applications to HCI.

Practical real-time applications have also been demonstrated. Bartlett et al. have successfully used their face expression recognition system to develop an animated character that mirrors the expressions of the user (called the *CU Animate*)

The various facial behaviours and motions can be parameterized based on muscle actions. This set of parameters can then be used to represent the various facial expressions. Till date, there have been two important and successful attempts in the creation of these parameter sets:

3: A GENERIC FACE RECOGNITION SYSTEM:

The input of a face recognition system is always an image or video stream. The output is an identification or verification of the subject or subjects that appear in the image or video. Some approaches define a face recognition system as a three step process. From this point of view, the Face Detection and Feature Extraction phases could run simultaneously. Face detection is defined as the process of extracting faces from scenes. So, the system positively identifies a certain region as a face. The procedure has many applications like face tracking, pose estimation or compression.

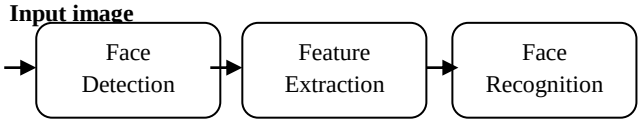


Fig: Face recognition System

The next step -feature extraction- involves obtaining relevant facial features from the data. These features could be certain face regions, variations, angles or measures, which can be human relevant (e.g. eyes spacing) or not. This phase has other applications like facial feature tracking or emotion recognition.

Finally, the system does recognize the face. In an identification task, the system would report an identity from a database. This phase involves a comparison method, a classification algorithm and an accuracy measure. This phase uses methods common to many other areas which also do some classification process -sound engineering, data mining.

These phases can be merged, or new ones could be added. Therefore, we could find many different engineering approaches to a face recognition problem. Face detection and recognition could be performed in tandem, or proceed to an expression analysis before normalizing the face.

4: A BASIC REAL-TIME SYSTEM MODEL:

We need to have a basic conceptual understanding of the underlying hardware. We therefore in this section try to develop a broad understanding of high level issues of the underlying hardware in a real-time system.

Following Figure shows a simple model of a real-time system in terms of its important functional blocks. Unless otherwise mentioned, all our subsequent discussions would implicitly assume such a model.

Observe that in Figure the sensors are interfaced with the input conditioning block, which in turn is connected to the input interface. The output interface, output conditioning, and the actuator are interfaced in a complementary manner.

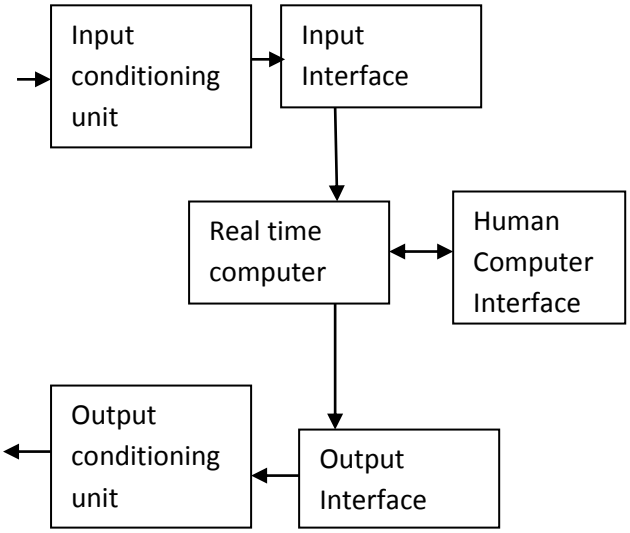


Fig: Basic Model of Real-time system

5: CONCLUSION:

This paper's objective was to introduce the real time security system using face expression recognition and the associated areas in a manner that should be understandable even by the new comers who are interested in this field but have no background knowledge on the same. In order to do so, we have looked at the various aspects of face expression recognition in detail. We have many applications that have been implemented and other possible areas where automatic expression recognition can be applied.

Face expression recognition systems have improved a lot over the past decade. The focus has definitely shifted from posed expression recognition to spontaneous expression recognition. The next decade will be interesting since I think that robust spontaneous expression recognizers will be developed and deployed in real-time systems and used in building emotion sensitive HCI interfaces. This is going to have an impact on our day to day life by enhancing the way we interact with computers or in general, our surrounding living and work spaces.

Artificial neural networks are a popular tool in face recognition. They have been used in pattern recognition and classification. Kohonen was the first to demonstrate that a neuron network could be used to recognize aligned and normalized faces.

Testing of algorithm will be using different additional bias constraints to obtain better results. By decreasing the error rate we can achieve better outputs, although it is more time-consuming that the simple method.

In future Speech recognition and speech processing can be embedded with image processing to make our security system efficient and effective Detecting the motion of the speech is not that easy as it seems to be. Besides human facial expressions speech has proven as one of the most promising modalities for the automatic recognition of human, but accuracy is the major factor of the speech processing. I would involve the classification of voice file using new classification method with combinational of algorithms such as MFCC, SVM and Neural network.

6: REFERENCES:

[1] A Survey of Face Recognition Techniques,Journal of Information Processing Systems, Vol.5, No.2, June 2009

[2] Introduction to real time systems, version 2, IIT kharagpur.

[3] Face Recognition Algorithms,Proyecto Fin de Carrera, June 16, 2010 ,Ion Marques,Supervisor: Manuel Grana.

[4] Hadid, "The local binary pattern and its applications to face analysis," in *Proc. Int.Workshops Image Process. Theor., Tools Appl.*, 2008, pp. 28– 36.

[5] Bhumika G. Bhatt , Zankhana H. Shah Face Feature Extraction Techniques: A Survey National Conference on Recent Trends in Engineering & Technology 2013

[6] B. Froba and A. Ernst, "Face detection with the modified census transform,"in *Proc. IEEE Int. Conf. Autom. Face Gesture Recog.*, 2004, pp. 91–96.

[7] Chennamma, H. R., Ragrajan, L., Rao, M. S. Robustnear-duplicate image matching for digital image forensics. *International Journal of Digital Crime and Forensics*, 2009, vol. 1, no. 3, 18 p.

[8] Mohamed A. Berbar ,Hamdy M. Kelash, and Amany A. Kandeel, Faces and Facial Features Detection in Color Images, Proceedings of the Geometric

[9] Modeling and Imaging— New Trends (GMAI'06) 0-7695-2604-7/06 $20.00 © 2006 IEEE

[10] Mrs.Smita Patil Prof. Mrs. A. A. Junnarkar, Overview of Colour Image Segmentation Techniques, IJARCSSE Volume 3, Issue 9, September 2013, ISSN: 2277 128X

[11] Nikita Sharma, D.S.Singh, A Survey on various Feature Extraction Techniques for Face Recognition, IJCA, ISSUE 2, Volume 4 (August 2012) ,ISSN: 2250-1797, Page 18

[12] Roopashree.S, Sachin Saini, Rohan Ranjan Singh. Enhancement and Preprocessing of Images using filtering, IJEAT, ISSN: 2249-8958 Volume-1 Issue-5,

[13] TusharGajame, C.L. Chandrakar Face Detection with Skin Color Segmentation & Recognition using Genetic Algorithm International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-2, July 2013

[14] K. Sung and T. Poggio, Example-based Learning for View-based Human Face Detection, A.I. Memo 1521, MIT A.I. Laboratory, 1994.

[15] Miss.Renke Pradnya Su nil Automatic Face Recognition Using Principle Component Analysis with DCT, Journal of Electronicsl and Communication Engineering (IOSR-JECE-2013) ISSN: 2278- 2834- , ISBN: 2278-8735, PP: 01-07.

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 142 - 148, 2015, ISSN:- 2319–8656

Performance Evaluation using Blackboard Technique in Software Architecture

Fatemeh majidi
Department of Computer Engineering, Ardabil Science and Research branch, Islamic Azad University,
Ardabil, Iran

Department of Computer Engineering, Ardabil Branch, Islamic Azad University,
Ardabil, Iran

Ali Harounabadi
Department of Computer Engineering, Central Branch, Islamic Azad University,
Tehran, Iran

Abstract: Validation of software systems is very useful at the primary stages of their development cycle. Evaluation of functional requirements is supported by clear and appropriate approaches, but there is no similar strategy for evaluation of non-functional requirements (such as performance). Whereas establishing the non-functional requirements have significant effect on success of software systems, therefore considerable necessities are needed for evaluation of non-functional requirements. Also, if the software performance has been specified based on performance models, may be evaluated at the primary stages of software development cycle. Therefore, modeling and evaluation of non-functional requirements in software architecture level, that are designed at the primary stages of software systems development cycle and prior to implementation, will be very effective.
We propose an approach for evaluate the performance of software systems, based on black board technique in software architecture level. In this approach, at first, software architecture using blackboard technique is described by UML use case, activity and component diagrams. then UML model is transformed to an executable model based on timed colored petri nets(TCPN) Consequently, upon execution of an executive model and analysis of its results, non-functional requirements including performance (such as response time) may be evaluated in software architecture level.

Keywords: Software Architecture, Blackboard Technique, Performance Evaluation and time colored Petri net.

1. INTRODUCTION

Within the recent decades, the software complexities have been increased day to day and demands for more powerful and high quality software have been increased. Therefore, software development based on principles and methodologies that in addition to reduction of costs, meet all expected features of shareholders (functional and non-functional requirements) seems to be necessary. Establishing non-functional requirements in software engineering was raised recently whilst they have considerable effect on success of software systems. Software Architecture (SA) is established at the first stages of design and has a significant effect on access to nonfunctional requirements of software system. Therefore, establishment of an executive model of SA and evaluation of nonfunctional requirements thereby is a cheap solution for prevention of time and cost waste for achieving the qualitative goals for development of software systems. using the patterns and styles of software architecture is a procedure to exploit the possibilities of a design which is based on architecture and architectural styles promote the characteristics like having the possibility of reusability, providing with supporting documents, finding risks at early stages, and upgrating.

One of important goals that are followed during analysis of architecture quality is verifying the architecture's access to qualitative features such as performance [1]. In the most software systems, special methods are used for evaluation of qualitative features. Special methods are applicable commonly after architectural implementation means when an executable specimen of system is available. If after applying the special methods, it is revealed that the architecture selected for system may not respond the nonfunctional needs, more time and cost is needed for system architecture changing. In consideration of this subject, we need alternative methods for evaluation of qualitative features which are applicable in initial stages of production process. Establishment of executable models of system architecture is one of solution that may respond the raised problems. An executable model of architecture is assumed as a formal description of architecture through which may analyze the behavior of final system before architecture implementation and get aware of problems and their in performance and take measure for architecture implementation more confidently and so avoid extra costs and even its failure. In continue, different parts of paper are explained: in second part, a general description of blackboard technique, performance model in unified modeling language (UML) and time color Petri net (TCPN) is presented. In third part, some works related to the subject of this paper are reviewed. In fourth part, the offered model is described. In fifth part, a case study is analyzed for evaluation of offered method and in sixth part, a general conclusion of suggested method is explained.

2. BACKGROUND

In this section, a general description of performance modeling in UML, blackboard technique and timed colored petri net models is presented.

2.1 Blackboard technique

In the codified classification of techniques, blackboard is placed in the centralized group. One user is executed on a distinct control set and includes common data which is accessible by these users.
Blackboard is a technique therein independent processing components are referred to as knowledge resource that is operated on the common storage in the name of blackboard. Knowledge resources have no direct interaction with each

other, when blackboard is executable, knowledge resources run on the blackboard as an opportunity seeking [2].
This architectural style is always promoting and extending and a structural solution for reaching to the integrity. In plenty of systems particularly systems consisted of prefabricated components, data integrity is provided by blackboard mechanism. Major advantage of this method is that the users are available separate from each other. In addition, common data is an independent part of users. Therefore, this style is scalable and new users may be added easily.

2.2 Performance Modeling in UML

Software architecture describes the system in high abstraction levels through specifying the structural and behavioral aspects. But, unified molding language diagrams may not be used to evaluate the software architecture, because some architectural features are not executable using them. In consideration of this subject, a strategy was offered by OMG including performance sub index, similar to other indices for supporting the extension process, stereotypes and labeled values that improves the applicability of these features [3].

2.3 Time colored Petri net

Colored petri nets are used for formal description of activities flow in the complex systems and provide the requirements of concurrency and parallelism exhibition. Classic petri nets are not suitable for modeling the systems with large space or a complex temporary behavior. In these cases, we must use a developed petri net model having color and time. This model is the base of a framework that is used for solving the problems related to design and control in complex systems. In these networks, the concept of time is introduced by global element called global time. The values selected by this time explains the model time. This model may be an integral number that indicates the discrete time or maybe a true number explaining the continuous time. This value of time that is pertained to each token is referred to as stamp time that indicates the first time of model therein token may be used. As a result, these nets will be appropriate for evaluation of qualitative requirements (response time etc.) in SA[4].

3. RELATED WORKS

Model-based methods development for evaluation of systems and computer nets is referred to a long time ago. Correct application of these models may provide appropriate attitudes for evaluation of nonfunctional needs. Due to low knowledge level of software architect, evaluation of these features is not applicable for software architecture, because software architecture for describing the software architecture uses specific marks and signs which are not usable for experts evaluating these features. Therefore, a solution must be found to fill the gap between software designers and nonfunctional features evaluation experts. One of solutions is using the tools and markings of software modeling together with options added thereto that may considerably remove this gap.
Fukuzawa and Saeki [5] presented a method therein software architecture is described by UML Component diagram. Then, the above algorithm has been transformed to colored petri net by an algorithm and ultimately the performance is evaluated, so that the own component and its connector are transformed to a colored petri net but its interface is transformed to a place of colored petri net.
Balsamo and Marzolla [6] presented a method therein software architecture is described by UML Use Case, Activity and Deployment diagrams, then operational profiles related to performance are annotated therein. Ultimately, to evaluate the performance, UML diagrams are transformed to an executive model based on Queuing Networks.
Petit and Gamma [7] described the software architecture by collaboration diagram and then converted to Petri net. This method is used for evaluation of performance and reliability. In this method, a collection of predetermined molds in colored Petri nets formed based on objects' behavioral roles are used. These behavioral roles are formed based on available objects structuring in COMMET method, but are not dependent to a specific method and used within different application ranges. Later, results obtained for colored Petri net are reflected in unified modeling language diagrams and the designer may improve the design quality and consequently improve the performance and reliability of system.
Gyarmati et al [8] offered a model therein software performance engineering (SPE) is used for evaluation of performance specifications of software architecture and fabrication and analysis of software executive model resulted from ordinal diagram of unified modeling language. In this method, class diagram and unified modeling language placing is used for describing the software architecture completely, but is not used in the conversion process. Architectural descriptions are converted to the developed queue net to evaluate the performance specifications.
In this paper, three major objectives are under consideration as follows:
-Evaluation of information system performance based on blackboard technique;
-An algorithm for converting blackboard technique to component diagram;
-Converting UML diagrams to the formal models based on features available in blackboard technique for evaluation of its performance.

4. THE PROPOSED METHOD

The main method in this paper is performance evaluation using blackboard technique in software architecture. For this purpose, firstly software architecture based on blackboard technique is described by UML, later operational profiles related to performance feature is annotated therein. In continue, an algorithm is offered for transformation of UML model to TCPN model and ultimately the said nonfunctional requirements are evaluated by suggested techniques at the SA level.

4.1 Description of Software Architecture by UML Diagrams

In this article, to describe the software architectural structure and behavior, use case, component and activity diagrams are used. In continue these diagrams and notations related to performance are explained.

4.1.1 The Role of Use Case Diagram and Annotation of Performance Specification Therein

Use case diagram describes the functional requirements of system and interaction between system and environment [9]. In this paper, this diagram is used for exhibition of functional requirements and working load applied to the system in SA description. Annotations related to performance in this diagram are related to actors that requesting service from system.
The actors indicating a sequence of unlimited requests out of system are annotated by "PAopenLoad" stereotype and actors indicating a fixed population of requests from system are annotated by "PAclosedLoad" stereotype. "PAclosedLoad" stereotype has a tag called PAoccurrence that indicates the interarrival time between two subsequent requests. "PAclosedLoad" stereotype has two tags named PApopulation and PAextDelay that respectively indicates "the number of

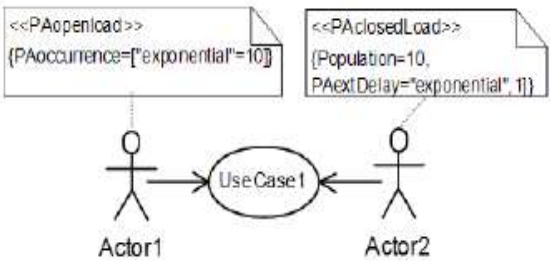
requests" and "the time spent by each completed request before the next interaction with the system". An annotated use case diagram is exhibited in figure 1.

4.1.2 The Role of Component Diagram and annotation of Performance Specifications Therein

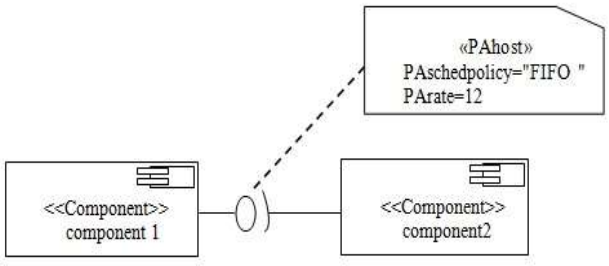
Component diagram describes the software system. In this paper, this diagram is used for describing the architectural structure based on blackboard technique. Moreover, a component includes interfaces that each interface defines a collection of component performed operation. Notations related to performance of this diagram are related to the interfaces and components. In this diagram, each component is noted with <<PAhost>> stereotype that specifies the software resource used in this project. This stereotype includes PAschedpolicy label that specifies the system schedule policy. Each interface is noted by <<PAstep>> stereotype that specifies the tasks performance time by the component together with PAdelay and PAdemand labels [10], [11]. Figure (1) shows an annotated component diagram. In addition, PArate label indicates the processing rate of processing source related to respective component.

4.1.3 The Role of Activity Diagram and Annotation of Performance Specifications Therein

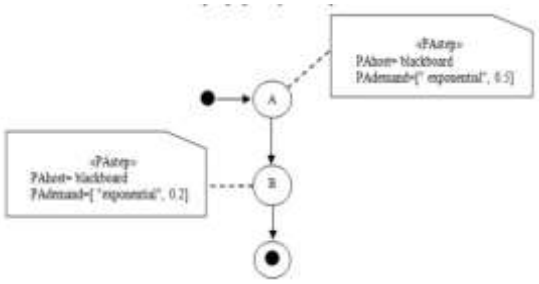
Activity diagram describes the software system behavior. This diagram is a graphic exhibition that shows the control flow from one activity to another. Notations related to performance in this diagram are related to transfers [9]. Each transfer is noted with <<PAstep>> stereotype which demonstrates the service provided in a component and according to its location and includes PAhost and PAdemand labels that each one denotes component location and service request, respectively. An annotated ctivity diagram is exhibited in figure 1.



(a) Annotated UML Use Case Diagram



(b) Annotated of integrated modeling language component diagram



(c) Annotated of integrated modeling language activity diagram

Figure 1. Annotated of integrated modeling language diagrams

4.2 The offered algorithm for converting modeling language diagrams to time colored Petri net

The offered algorithm in this paper for converting unified modeling language to time colored Petri net is raised for incorporating an executable model for evaluation of software architecture that includes following stages:

First stage: Description of architectural structure based on blackboard technique component diagram and determination of performance specifications in this diagram, blackboard-based architectural structure is described.

Second stage: Description of blackboard-based architectural behavior In this paper, to describe the software architecture behavior, case use and unified modeling language activity diagrams are used. In the suggested course of action, case use diagram is used to exhibit the functional needs and function load applied on the system during software architecture description. Activity diagram describes also the system behavior and shows the control process from one activity to another one.

Third stage: Evaluation of the blackboard-based architecture Whereas various agents have varied function loads in the system, T-CPN model contains following models which are independent from each other and each one will has their own functional load. Furthermore, requests related to one sub model may have several classes that each one is shown with different colors in T-CPN. Each color is unique and may not be repeated in other classes.

Open Petri net contains input and output to the external environment and shown by <<PAopenload>> stereotype that is used in the case use diagram. Whereas several methods can use a source in the system, we have following definitions in T-CPN model:

If it is assumed that sources are exhibited as RES= {res1, res2 ... res n} for each source, res ϵ RES is defined as a feature called [count [res]]. [Count [res]] denotes total requests that request service from res, index feature is a unique index for identification of sources. Places which use res resource are shown by}ACTION={ action1,action2,..., actionn}, it is obvious that count[res]=a for each source labels total requests in {action ϵ ACTION | resource(action)= res} set by a unique number in range [1,2,...,count[res]]. This unique number is shown by index [action] feature.

If agent x is noted by <<PAopenload>> stereotype, feature values are determined as below:

Count [res] $\forall$ res ϵ RES

Index [action] $\forall$ actionϵ ACTION

C = MAX res ϵ {COUNT [res]} (1)

To show the customers service rate with class r, SR [i,r] in transfer i is used. M is an action in activity diagram.

SR [i,r]= rate[r]/demand [action] where i = index [resource[m]]. (2)

r = index [action]. (3)

λ]r] for is considered for showing the customer input rate with class r that is defined as below:

λ [r] = arrival rate [x] (4)

The input rate is used based on labeled case use that resulted in use of activity diagram.

4.3 Evaluation of response time in software architecture Level

Performance metrics such as response time, queue length etc. may be evaluated using the said evaluation method. To compute the response time, time interval between request and first received response by the other side must be analyzed. In fact:

$$T_R=T_S+T_D \quad (5)$$

T_R: Response time

T_S: Service time

T_D: Delay time

Delay time may be defined as delay time in processing queue To analyze the queue length, tokens number in place must be calculated.

5. CASE STUDY

In this paper, hotel reservation system was assumed as case study, so that this system was implemented on blackboard technique and ultimately is evaluated using the offered method. Blackboard technique is shown in Figure 2. Figure 3,4 and 5 show case use, component and activity diagrams of unified modeling language of hotel reservation system. Figure 6 show activity diagram of hotel reservation system. In this scenario, firstly the user declares its request on hotel reservation and the system during some stages responds by its agents in consideration of the user request. For evaluation of nonfunctional needs (such as performance), diagrams shown in Figure 4 and 5 are converted to time colored Petri net model. Final model of time colored Petri net is exhibited in Figure 6. To evaluate the performance (such as response), 4 requests are input to the system by users and upon their execution on time colored Petri net, valuable results are obtained for evaluation of nonfunctional needs on SA level. Table 1 shows the response time related to users.

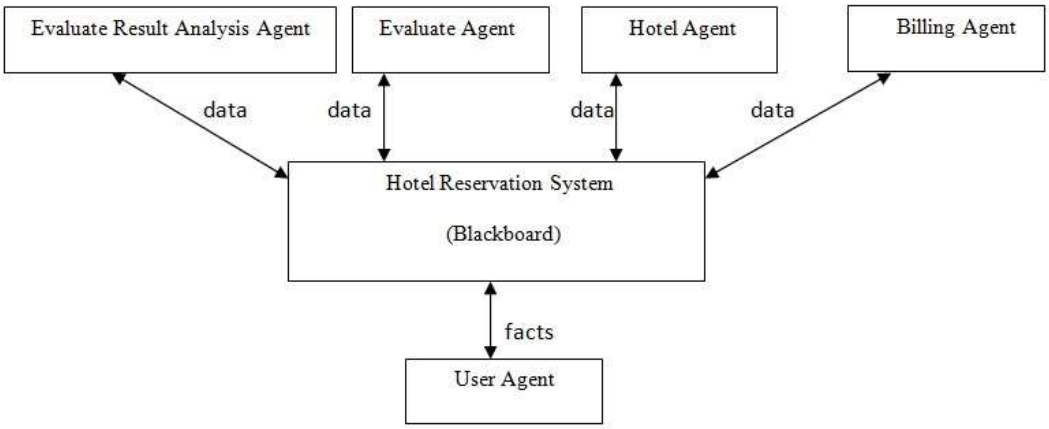


Figure 2. Abstract model of hotel reservation system

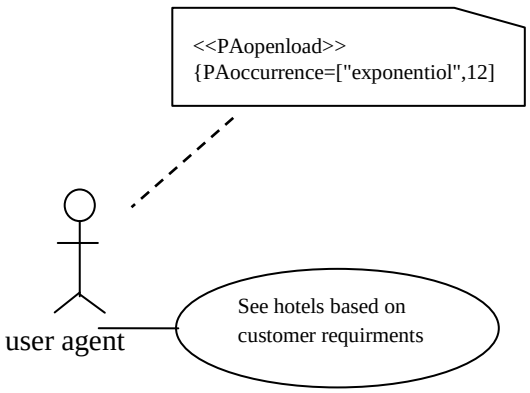


Figure 3. Exhibition of hotel reservation system with CR card

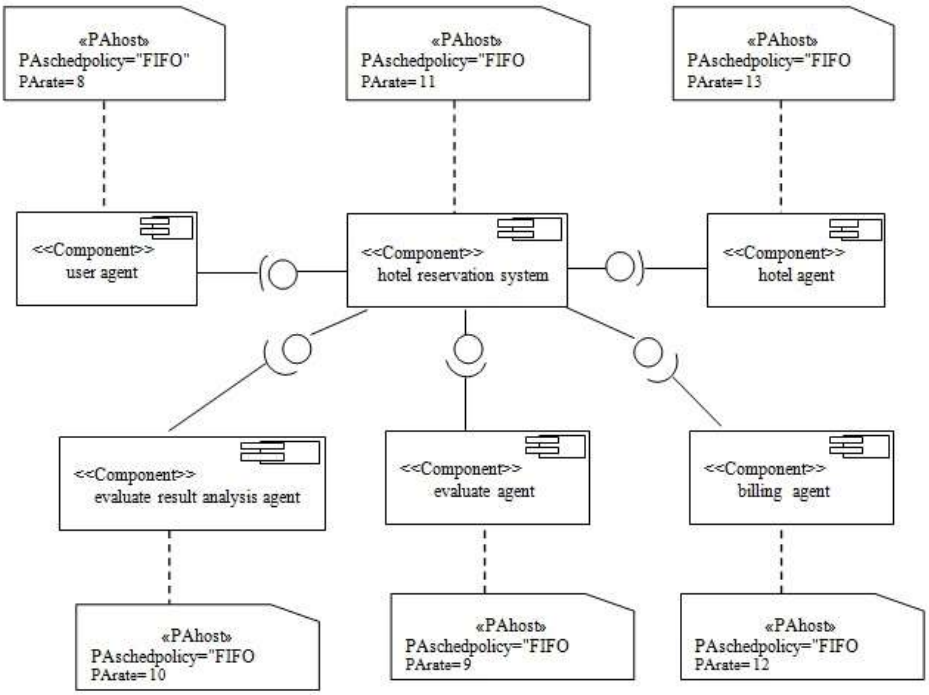


Figure 4. Annotated of performance in component diagram

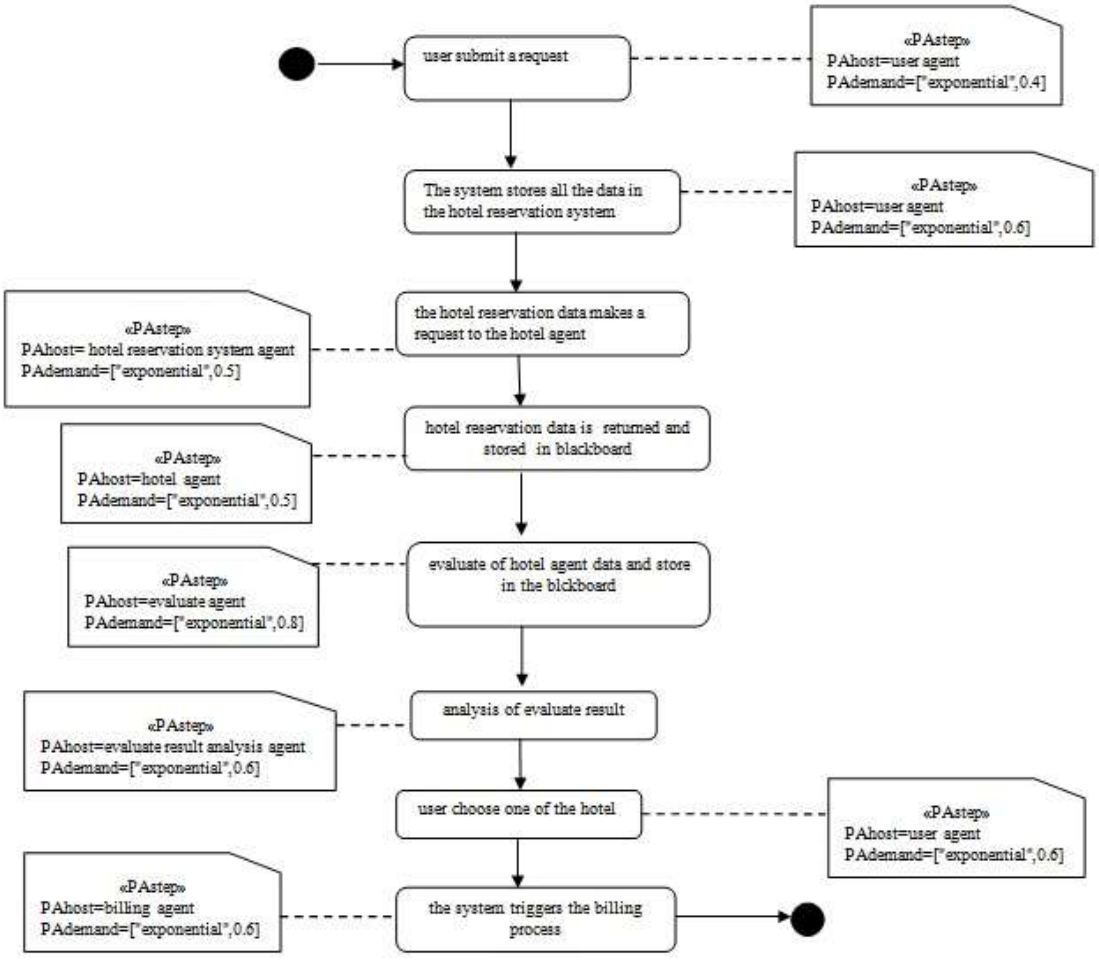


Figure 5. Hotel reservation activity diagram

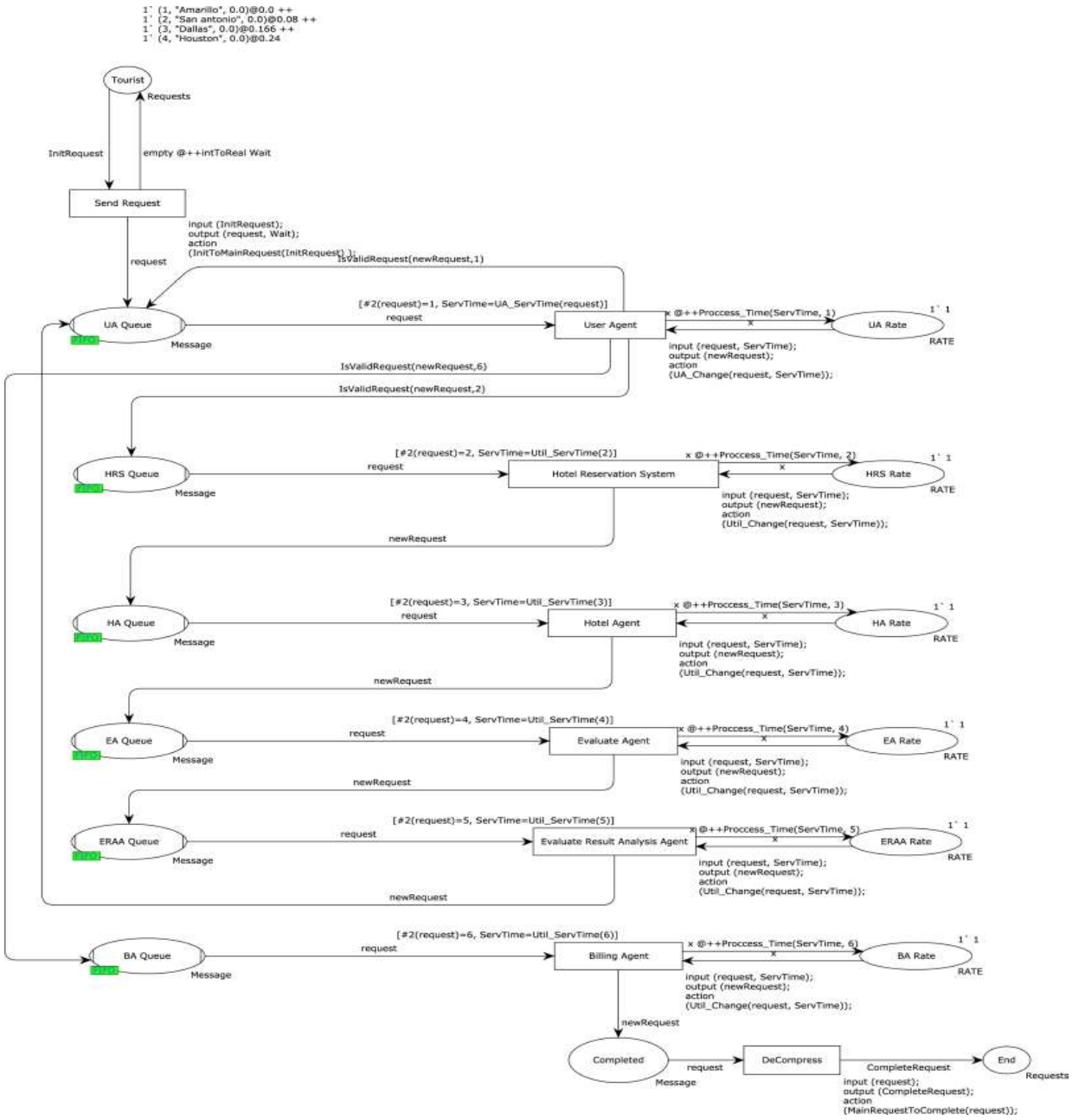


Figure 6. Time colored Petri net

Table 1. Response time

Number of request	Response time
1	0.16861
2	0.56993
3	0.52483
4	0.295

6. CONCLUSIONS

In this paper, we have presented a strategy for evaluation of performance of nonfunctional requirements in software architecture using blackboard technique modeled by UML diagrams. So, the software system may be validated for meeting or not meeting the nonfunctional requirements of case at the primary stages of software systems development cycle. The general analysis framework in this method is formed based on formal models (TCPN) that accordingly is free of ambiguity. Whereas in this method, UML diagrams are used for description of software architecture based on blackboard technique, therefore description of SA by means of achievements of analysis and design stages will be very reasonable and low-cost. on the other hand, a transformation has been presented for establishment of a TCPN-based executive model from UML model .There are a lot of tools for working with UML models and UML models may be transformed to TCPN-based executive model automatically. In addition, other nonfunctional requirements may be evaluated by means of other architectural specifications.

7. REFERENCES

[1] Technical Report IEEE P1471-2000. Recommended Practice for Architectural Description of Software Intensive Systems, IEEE Standards Department, The Architecture Working Group of the Software Engineering Committee, (September 2000).

[2] Clements, P., Bass, L., Garlan, D., Ivers, J. Little, R. Nord, R. and Stafford, J. 2010. Documenting Software Architectures: Views and Beyond. Second Edition, Publication City/Country New Jersey, Addison Wesley.

[3] Object Management Group (OMG). 2002. UML Profile for Reliability, Schedulability, Performance and Time Specification.

[4] Jensen, K. and Kristensen, L. 2009. Coloured Petri nets: modeling and validation of concurrent systems. Springer-Verlag.

[5] Fukuzawa, K. and Saeki, M. 2002. Evaluating Software Architectures by Coloured Petri Nets. in SEKE02 14th International Conference on Software Engineering and Knowledge Engineering, ACM, Ischia, Italy.

[6] Balsamo, S. and Marzolla, M. 2005. Performance Evaluation of UML Software Architectures with Multiclass Queueing Network Models. ACM Workshop on Software and Performance (*WOSP*).

[7] Pettit, R. G. and Gomaa, H. 2004. Improving the Reliability of Concurrent Object Oriented Software Designs. proceeding of the ninth IEEE international workshop on object oriented real time dependable systems.

[8] Gyarmati, E. and Strakendal, P. 2002. Software Performance Prediction-Using SPE. Master Thesis Software Engineering, Department of Software Engineering and Computer Science Blekinge Institute of Technology, Sweden.

[9] Object Management Group (OMG). 2005. Unified Modeling Language (UML). Version 2.0.

[10] Merseguer, S. Bernardi, S., Campos, J. and Donatelli, S. 2002. A Compositional Semantics for NML State Machines Aimed at performance Evaluation. proce. Of the 6th International Workshop on Discrete Event Systems, 295-302.

[11] Merseguer, J., Campos, J. and Mena, E. 2003. Analysing Internet Software Retrieval System: Modeling and Performance Comparison. Wireless Networks: the Journal of Mobile Computation and Information, vol. 9, no. 3, 223-238.

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 149 - 152, 2015, ISSN:- 2319–8656

Design and Analysis of Robotic Rover with Gripper Arm using Embedded C

Harmeet Singh, Sangeeta
Department of Computer Science
Punjab College of Technical Education (PCTE)
Baddowal, Punjab, India

Harpreet Kaur
Department of Electronics and Communication Engineering
Sant Longowal Institute of Engineering and Technology (SLIET) Longowal, Punjab, India

Abstract: This paper confers the development and working of robotic rover performing various autonomous tasks to identify, pick and drop an object at an appropriate position using microcontroller 8051 in conjunction with embedded C programming. The system employs infrared proximity sensors, DC geared motors, microcontroller board, *etc.* Robotic rover technology offers many applications in space explorations, military operations, *etc.* The motive of this research work is to design a wireless robotic rover being autonomous controlled that is capable of completing tasks with proliferated accuracy in smooth terrain.

Keywords: Robotic Rover; Embedded C; Microcontroller; Programming; Sensor

1. INTRODUCTION

Robotics technology is emanating at an expeditious pace, contributing new possibilities for automating tasks in many demanding applications, peculiarly in space explorations, military operations, underwater missions, *etc.* Especially, in space exploration, robotic devices are known as planetary rovers or simply rovers who aim at administering physical analysis of planetary terrains and astronomical bodies. The supervision of data about air pressure, climate, temperature, and other atmospheric aspects can be done by this advanced technology [1,5,9]. It is a space exploration vehicle designed to move across the surface of a planet or other heavenly body. Primarily, rovers can be self-governing or can be remotely controlled from the ground stations called as Remote Collaboration Center having very definite scientific objectives. Some rovers have been devised in the transportation of members of a human spaceflight crew; others have been partially or fully autonomous robots. Rovers or Unmanned Ground Vehicles (UGV) usually arrive at the planetary surface on a lander-style spacecraft [2,7-8]. The investigation of territories at the microscopic level, investigating the biological aspects of planetary surfaces, analyzing the composition of minerals, rocks, and soils, searching for liquid water in minerals, and measuring the ambient temperature, air pressure, and amount of dust in the landing site are some of its imperative appositeness [3]. Therefore, rovers are eminently computing systems that use complicated embedded software and algorithms to handle computational and processing functionalities.

Figure.1 Schematic of Curiosity Rover on Mars

An autonomous robot has the competence to:

- Collect information about the environment, such as building maps of building interiors.
- Detect objects of interest such as people and vehicles.
- Travel between targets without human navigation and intervention.
- Disarm, or remove explosives.
- Repair itself without outside assistance.

The ongoing Mars exploration focuses around surface exploration using satellites and small, autonomous land-exploration rovers which are used in predilection to manned missions as the cost is substantially lower and the rovers are more suited to the harsh planetary environment. Manned missions are still regarded as the 'holy grail' of topographical exploration; a current rover mission is aiming to scrutinize Mars with a pair of rovers, providing scope for coordination which was hitherto only possible with human exploration [1,3-4,6]. This paper is intended to study and discuss the design and development of robotic rover, its fully autonomous functionalities with various other capabilities.

2. ROBOTIC ROVER DESIGN

The structural part involves use of frames, beams, linkages, axles, etc. The mechanical parts/accessories comprise various types of gears (spurs, crowns, bevels, worms and differential gear systems), pulleys and belts, drive systems (differentials, castors, wheels and steering), etc. Pneumatics plays a vital role in generating specific pushing and pulling movements such as those simulating arms or leg movements. Pneumatic grippers are also used with advantage in robotics because of their simplicity and cost-effectiveness. The electrical items include DC and stepper motors, actuators, electrical grips, clutches and their control. The electronics part involves remote control, sensors (touch sensor, light sensor, collision sensor, etc), their interface circuitry and a microcontroller for overall control function.

The main objectives of the robotic rover project are given below:

- It automatically senses the object of interest using infrared sensor.
- It picks up the object.
- It places the object at proper position.
- It moves forward in search of another object

Figure.2 Robotic rover with gripper arm

2.1 Hardware Design of Proposed Rover

In this research work, an elementary robotic land rover that can be controlled remotely using primarily radio frequency (RF) module is presented. The tasks are autonomously controlled by the rover itself which is pre-programmed using embedded C programming. The RF remote control has the advantage of adequate range (up to 200 metres with proper antennae) besides being omnidirectional. On the other hand, an IR remote would function over a limited range of about a few metres.

The proposed land rover as shown in Figure 2 can move in forward and reverse directions with the gripper arm capable of advancing in left and right directions. While being deviated to left or right, the blinking of the corresponding LEDs takes place to indicate the direction of its turning. Similarly, during reverse movement, reversing LEDs would be lit. Front and rear bumpers are provided using long operating lever of micro switches to switch off the drive motors during any collision.

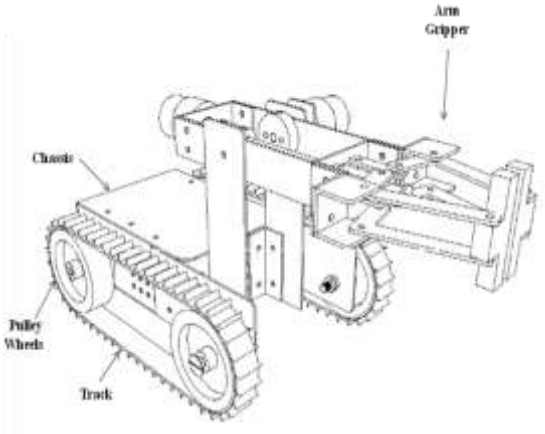


Figure. 3 Schematic diagram of robotic rover

The basic hardware of robotic rover as shown in Figure 3 consists of following parts:

- Aluminum Chassis
- Microcontroller board
- Infrared Proximity Sensor
- RF sensor
- Plastic wheels
- Four DC geared
- Gripper arm

The influential part of the robotic rover design is the gripper arm capable of picking up an object and doing functions of opening and closing the arm. Figure 4 delineates gripper arm consisting of various components. The individual parts were assembled to combine them into a single functional unit. The procedure of agglutination of components is also described in this section as described in Figure 5.

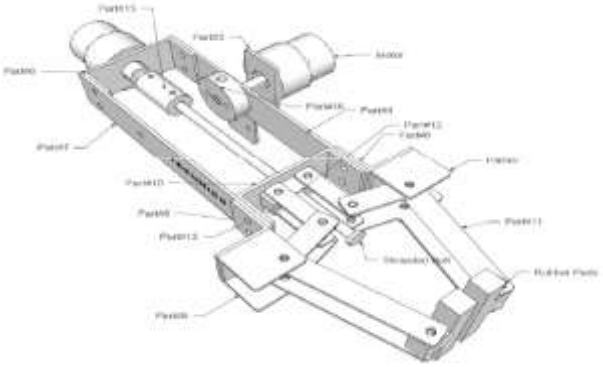


Figure. 4 Schematic diagram of gripper arm (reference: technido.com)

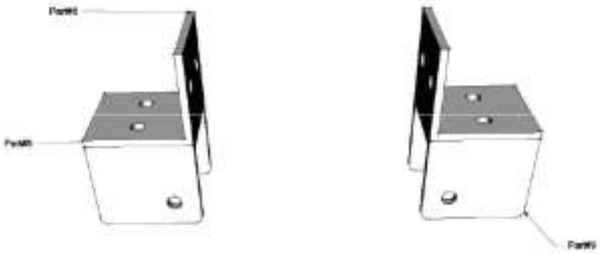


Figure. 5(a) Schematic diagram of gripper arm placing part#8 over part#9 and fixed using screw and nuts

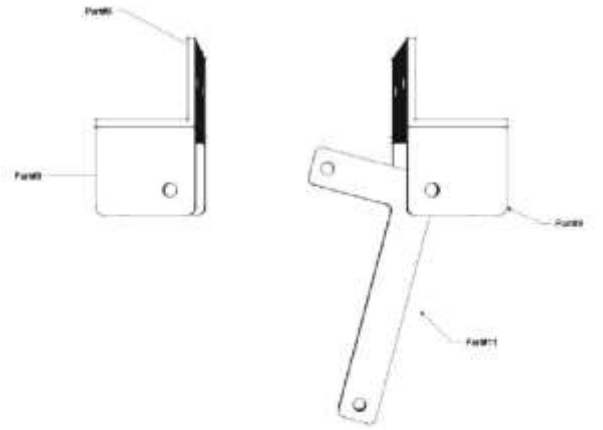


Figure. 5(b) Schematic diagram of gripper arm adding part#11 to previous assembly

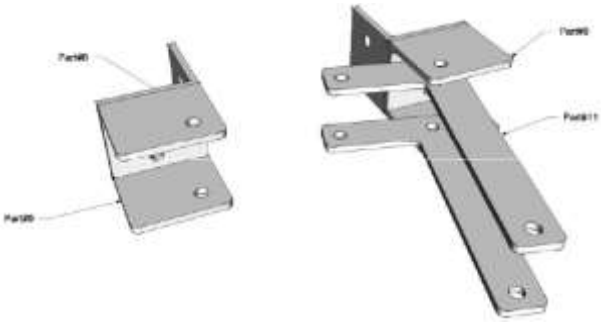


Figure. 5(c) Schematic diagram of gripper arm placing two L shaped part#11 opposite to each other one above and one below

Figure. 5(d) Schematic diagram of gripper arm placing four L shaped part#11 opposite to each other one above and one below

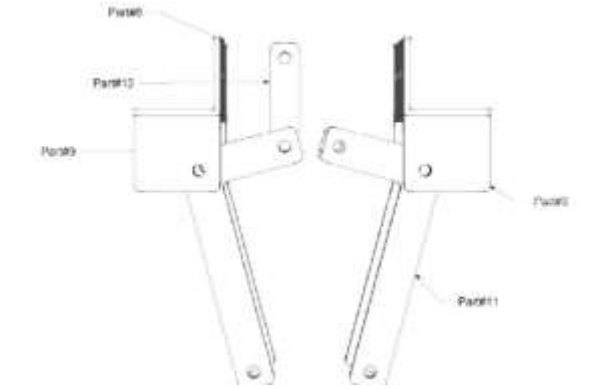


Figure. 5(e) Schematic diagram of gripper arm placing part#13 loosely with previously fixed part#11

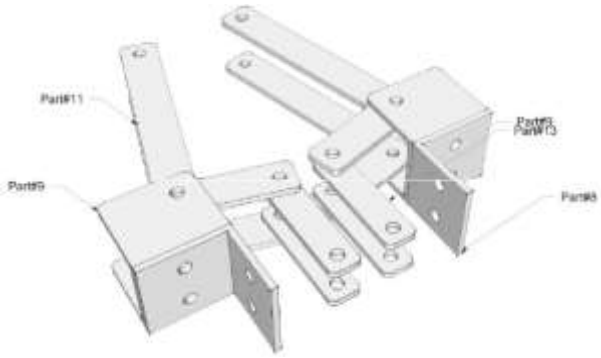


Figure. 5(f) Schematic diagram of gripper arm placing four part#13 loosely with previously fixed part#11

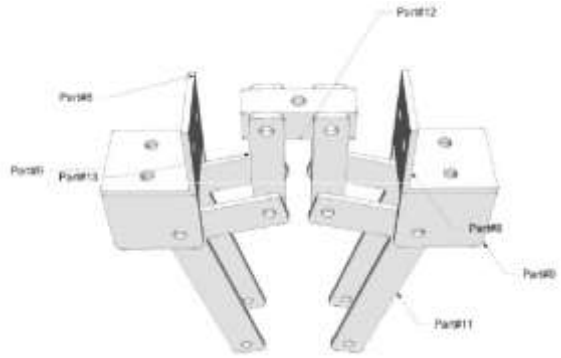


Figure. 5(g) Schematic diagram of gripper arm adding part#12 made up of Aluminium holding all part#13 in place

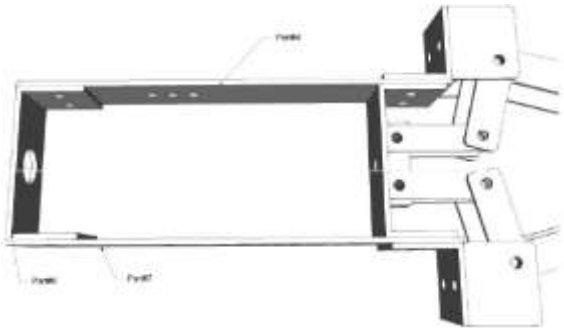


Figure. 5(h) Schematic diagram of gripper arm locating part#6 in box and fixing it with part#4 and part#7

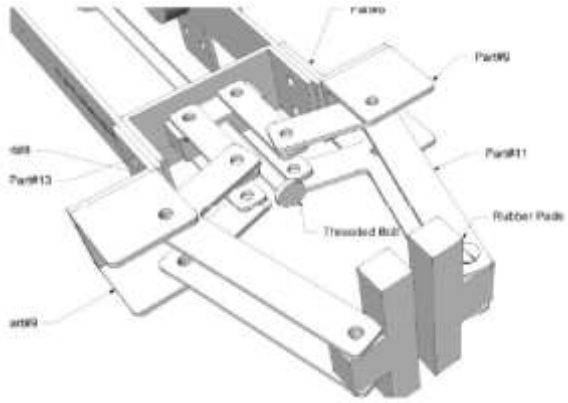


Figure. 5(i) Schematic diagram of gripper arm with threaded bolt and rubber pads

2.2 Embedded C Programming

The robotic rover programming was accomplished using microcontroller 8051 from NXP (founded by Philips) model P89V51RD2 which is a 40MHz, 5 Volt microcontroller with 32 I/O lines, 3 Timers/Counters, 9 Interrupts/4 priority levels, 64K+8K FLASH, 1K on-chip RAM, SPI, Dual Data Pointers, WDT, 5-channel PCA. Keil µVision software was availed which combines project management, making facilities, source code editing, program debugging, and complete simulation in one powerful environment. The µVision development platform is easy-to-use and helps in quickly creating embedded programs. The µVision editor and

debugger are assimilated in a single application that provides a seamless embedded project development environment. Flash magic software was used as program burner which is a PC tool for programming flash based microcontrollers from NXP using a serial or Ethernet protocol while in the target hardware.

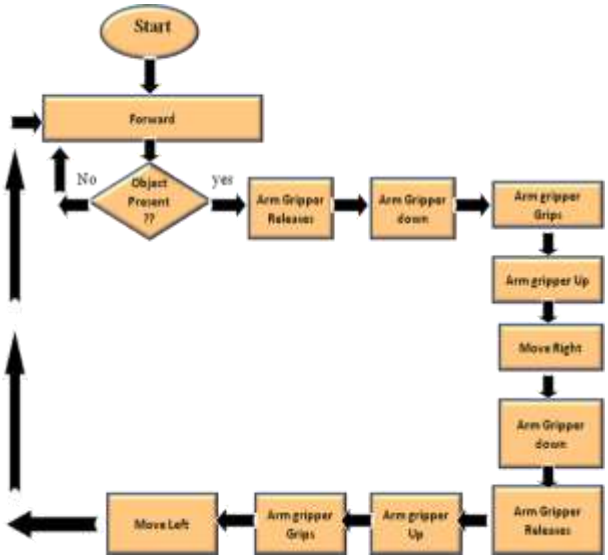


Figure. 6 Flow chart depicting working of proposed robotic rover

2.3 Working of Robotic Rover

Figure 6 illustrates the dynamics of robotic rover with gripper arm facility. This robot firstly moves in forward direction in search of an object. Here, the IR sensor plays a crucial role. The object is detected when the distance between the IR sensor and the object of interest is approximately 12 cm (the range can be further increased). If the object is encountered, its arm grip is released and moved in downward direction. Then the arm grip grasps again and picks up the object. It is placed in right direction where the arm gripper releases the object. It maneuvers in upward direction and robotic rover proceeds in forward direction. The programming of the whole operation is done in embedded C language using Keil µVision 3 tool from ARM Ltd.

3. RESULTS

Table 1. Table captions should be placed above the table

Steps	Operations	Time taken to complete (sec)
Step 1	Release of Gripper arm	15
Step 2	Down	4
Step 3	Grip (object)	11
Step 4	Up	5
Step 5	Right/left	5
Step 6	Down	3
Step 7	Release	12
Step 8	Up	5
Step 9	Grip (empty)	15
Step 10	Left/right	5

The robotic rover functionality comprises of some basic steps which were made fully autonomous using embedded C programming. The RF module was used to switch on/off the rover. Firstly, the release of empty gripper arm has taken a considerable time of 15 sec followed by down movement of 4 sec. Due to presence of gravity of earth, down movement took minimum time among all other operations. Thenceforth, the object was grasped by the gripper arm covering a total of 11 sec. The gripping and releasing operations done by gripper arm clutched substantial seconds as shown in table 1. Hereafter, the up movement of gripper arm took place with 5 seconds and positioning the object left/right. The object was then placed by a down release of 3 seconds since both the law of gravity and the weight of object exerted a downward force. Placing the object at proper place was the most momentous task. It took a second highest time of 12 sec with release operation of the arm. Consequently, the arm was moved in upward direction with gripping of the arm. These operations were continued until and unless an object of interest was discovered.

4. CONCLUSIONS

This paper has bestowed an overview of the proposed robotic rover which can be used for sensing and navigation. It can be made fully autonomous with in-built camera, high performance controller, ultrasound sensors for future work. These enhancements will foster its capability for long range navigation. Being a latest technology in India, it would be benefaction for our space and defense applications.

5. ACKNOWLEDGMENTS

The authors are indebted to Kits‘n’Spares, New Delhi and Technido Indore, India for providing Robotic Rover parts and technical help for making this work successful.

6. REFERENCES

[1] Zerigui A., WU X., Deng Z., “A Survey of Rover Control Systems”, International Journal of Computer Sciences and Engineering Systems, Vol. 1, No. 4, pp. 105-109, 2007.

[2] Siegwart R., Nourbakhsh I., Scaramuzza D., Introduction to Autonomous Mobile Robots, 2nd edition, The MIT Press, 2011.

[3] Young A., Lunar and Planetary Rovers: The Wheels of Apollo and the Quest for Mars, Springer, 2006.

[4] Svitak, Amy, Cost of NASA's Next Mars Rover Hits Nearly $2.5 Billion, http://www.space.com/10762-nasa-mars-rover-overbudget.html, retrieved 2011-02-03.

[5] Wesley T. Huntress JR., Mikhail Ya Marov, Soviet Robots in the Solar System: Mission Technologies and Discoveries, Springer, 2011.

[6] E. Colon, H. Sahli, and Y. Baudoin, ―CoRoBa, a multi mobile robot control and simulation framework, International Journal of Advanced Robotic Systems, Vol. 3, No. 1, pp. 073-078, 2006.

[7] iRobot, Mobility Integration Software User's Guide, 2002.

[8] Cherry S., Robots, IEEE Spectrum, 2007.

[9] B. Gerkey, R. Vaughan, K. Sty, A. Howard, G. Sukhatme, and M. Mataric, ―Most valuable player: A robot device server for distributed control‖, In Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2001.

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 153 - 156, 2015, ISSN:- 2319–8656

Android Based Remote Surveillance System and Content Sharing Between PC And Mobile

S. A. Ahirrao
Sandip Foundation (SIEM)
Nashik, India

Sayali S. Ballal
Sandip Foundation (SIEM)
Nashik, India

Divya K. Sawant
Sandip Foundation (SIEM)
Nashik, India

Harsha H. Chahira
Sandip Foundation (SIEM)
Nashik, India

Amisha A. Savaliya
Sandip Foundation (SIEM)
Nashik, India

Abstract: This paper presents the Video Surveillance System architecture to improve surveillance applications which are best on the use of the service oriented paradigm, with Android Smartphone's as user terminal. It increases the flexibility of the system. This system allows to access the videos from different localization anywhere and anytime.

This paper also presents the content sharing, which is based on peer to peer technology [3]. In this, mobile will be considered as one peer of the network & the PC will be considered as the other peer of the network [4]. Using internet connection at both the ends, we can connect two discrete system in a network & peer to peer networking is possible. This system is used for applications like Uploading or downloading the files which is there in a remote computer, Storing the files and images in a remote computer through the mobile phone and also we can control remote computer by using mobile phone.

Keywords: Android; Surveillance; Peer to Peer; Internet Connection.

1. INTRODUCTION

In our day-to-day life, people don't want to waste their valuable time in monitoring the videos of institutes or any organization for security purpose. People want everything to happen at their door step without making so much effort. In this system the user can view/share the videos, also we can upload/download the files from anywhere in the world. That means we want multitasking facilities to happen at any remote area[1].

In video surveillance system, videos can be monitored from anywhere through mobile phone with web camera which can be inbuilt web camera or external using android. There are different surveillance methodologies like alarm system, CCTV, PC based video system are use to ensure the security[1]. But using all these systems, it is not possible for a user to monitor the security of his or her institute (Location) when they are outside. Means using all these systems, the person requires to continuously monitoring the video for security purpose and this is main drawback. Because now-a-days anybody can communicate with anyone at any time around the globe with the help of mobile phone technology. By using mobile, people can monitor the videos of their institution/organization even they are at outside. This video is recorded in the system by using web camera & people can monitor the videos through the mobile. So this will ensure more security.

The security problem is resolved by video surveillance system, but there exits also another problem which we are overcoming like insufficient storage in mobile phone. This problem is resolved by content sharing system. Sometimes whenever there is less memory space available to store the data in to our mobile phones, at that time we can transfer the data to remote PC in the network and free some memory from our mobile phone by uploading some of the files in remote PC which is at remote location. This helps us to quickly access the data instead of manually connecting our mobile phone to some PC and transfer data. Also by using content sharing system, we can transfer the data from Mobile to PC and from PC to Mobile. We can view the information through the mobile from remote PC from anywhere in the world[5].

Also we are providing security for Simple Users and Administrator. Simple users can access only those drives which are allocated to them during their Registration process. One simple user can not access the other simple users information as the users individually are allocated the access rights and the administrator have full access to the system.

Utilization of memory space is more when application is kept in cloud. Here instead of IP camera we are using Web camera as IP camera uses concept of cloud and cloud incurs more cost when android server is stored in cloud. Also using cloud is not affordable to many users.

The mobile will specify the file name and the system will search the directories for the particular file name, from which the contents are viewed through the mobile. The main requirement is that the system must be switched ON with internet connection enabled and the mobile should have GPRS connection.[1]

2. LITERATURE SURVEY

In our day to day life, people want multitasking facilities to happen at their door steps. So continuously monitoring the system for security is not possible every time for them which will take more time and efforts in monitoring. We are overcoming this drawback by using Video Surveillance system by using mobile phone. Because now-a-days anybody can communicate with anyone at anytime around the globe with the help of mobile phone technology. By using mobile phone, people can monitor the videos of their institute or organization when they are outside of their organization or institutes. The video is recorded in the system by using web camera and user can monitor through the mobile phone anytime. This will ensure more security. [1]

The security problem is resolved by video surveillance system, but their exists another problem which we overcoming like insufficient storage in mobile phone. This problem is resolved by content sharing system. Sometimes whenever there is less memory space into our mobile phone available to store the data, at that time we can transfer the data to remote PC in the network and free some memory from mobile p hone by uploading some of the files in remote PC which is at remote location. This helps us to quickly access the data, instead of manually connecting our mobile phone to some PC and transfer data. By using content sharing system, we can transfer the data from mobile to PC as well as from PC to mobile. We can view the information through mobile phone from remote PC from anywhere in the world.

Also we are overcoming the drawbacks of team viewer software by providing the security for simple users and administrator. Simple users can access only those drives which are allocated to them during their registration process. One simple user cannot access other simple user information as the users individually are allocated the access rights and administrator has full access to the system.

3. THE BUILDING BLOCKS: OVERVIEW

3.1 System Architecture

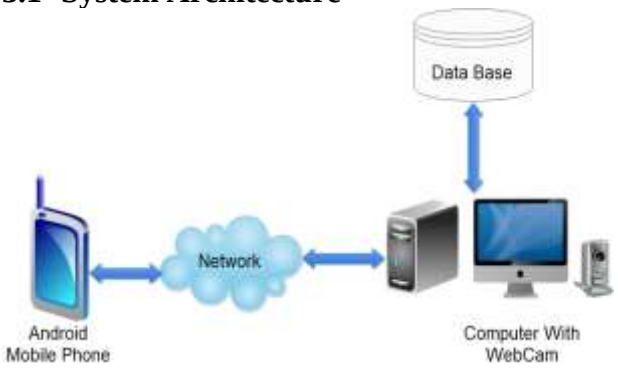


Fig 3.1: System Architecture Diagram.

As shown in Fig 3.1, Mobile and System are considered as two peers of the network. Android mobile phone is considered as a client and system with web camera is considered as a server, also internet connection is required at both the ends that is client side and server side. Database is connected to server system. Suppose user wants to access particular file, then he/she can login form his/her mobile by login id and password and request for particular file. The server computer search the particular requested file. If that file is found in database then server PC fetch that file from database and send to the user.

3.2 Proposed System

3.2.1 Content Sharing

Fig 3.2.1 (i): Content Sharing.

It is a peer to peer technology. The data is transfer between PC and Mobile in a secured way. User can upload file as well as download the file which are stored in to the system.

Fig 3.2.1 (ii): Algorithm for Content Sharing.

3.2.2 Video Surveillance

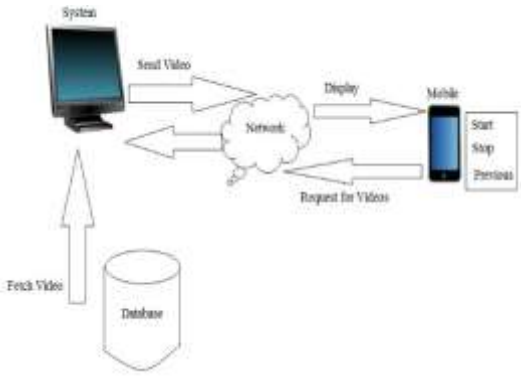


Fig 3.2.2 (i): Video Surveillance

The PC at remote location will fetch the videos from database and send those videos over the network which are displayed on mobile phone which is end user.

The process of sending and receiving video is done using socket programming and TCP protocol at the both the ends that is at client and server side.

At server side PC that is Remote PC one background thread is continuously running and this background thread slice the video which is continuously captured by the web camera.

This slice videos are being numbered and store into the database. And while fetching videos from mobile that videos are being stored into the SD card. The database will store the videos according to their date and time.

The SD card will store only the latest 10-12 videos and other videos if user wishes to see so the user can request it from the database.

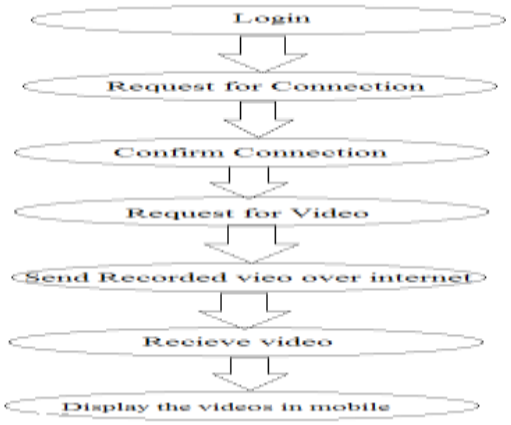


Fig 3.2.2 (ii): Algorithm for Video Surveillance.

3.3 Overview Of Android

The mobile application would be develop in Android. Android is a mobile Operating System which is based on Linux Kernel that is developed by Google. In android, user interface is user friendly. Android is designed mainly for touch screen mobiles such as smart phones and tablets. Android is not only designed for touch screen input, but also it has been used in games, digital cameras, electronics, etc.

The main goal of the Android project is to create a successful real-world product that improves the mobile experience for end users.

Android is a software platform developed by Google. It allows developers to write and manage code in a Java language, that uses Java libraries which are developed by Google. Java is platform-independent language as it can run on any operating system. Also java is portable and robust in nature. In this paper we are using mobile application in android and desktop application in Java.[2]

4. MATHEMATICAL MODEL

Input:

I= {I1, I2}

Where,

I1= Video Surveillance

I2= Content Sharing

I1 contains the set of input values which perform various operations such as play, pause, previous.

Operations are,

opA = {opA1, opA2, opA3}……. (1)

Where, opA1= Play

opA2= Pause

opA3= Previous

The following Venn diagram shows the relation is one to many as shown in fig 4.1

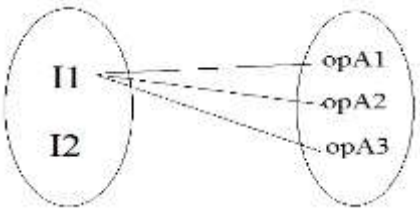


Fig 4.1

Input I2 contains the set of input values which performs various operations such as upload and download files.

Operations are,

opB = {opB1, opB2}……. (2)

Where,

opB1= Upload

opB2= Download

The following Venn diagram shows the relation is one to many as shown in fig 4.2

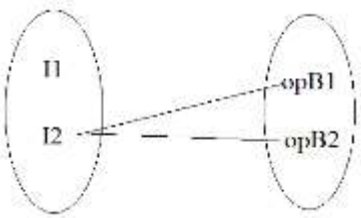


Fig 4.2

Output:

The output functions defines the output 'O' of the system i.e. O1, O2, O3.

O= {O1, O2, O3}……. (3)

Where,

O1= Play Video

O2= Uploaded File on server side PC / Remote PC

O3= Download File on client side / Mobile Phone

From the above equations (1), (2) & (3) the following fig 4.3 depicts the set of input values operations or functions performed on it and the set of output generated based on the given Inputs.

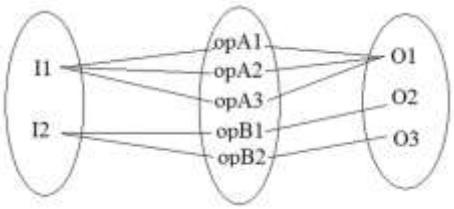


Fig 4.3

5. ACKNOWLEDGMENTS

We are extremely grateful to our guide Prof. S. A. Ahirrao, Assistant Professor, Department of Computer Engineering, SIEM for providing all the required resources for the successful completion of our Paper.

6. REFERENCES

[1] D. Shiny Irene PG Scholar," Video Surveillance System And Content Sharing Between Mobile And PC Using Android",Dept of Computer Science and Engineering RMK Engineering College, Anna University of Technology, Kavaraipettai, Chennai, Pages(s),Year 2012.

[2] Jae Kyu Lee, Jong Yeol Lee,"Android Programming Techniques for Improving Performance",IEEE 3rd International Conference on Awareness Science and Technology(iCAST),Page(s) 386-389, Year 2011.

[3] Choon Hoong Ding, Sarana Nutanong, and Rajkumar Buyya," Peer-to-Peer Networks for Content Sharing", Grid Computing and Distributed Systems Laboratory, Department of Computer Science and Software Engineering, The University of Melbourne, Australia.

[4] Jari Porras, Petri Hiirsalmi and Ari Valtaoja,"Peer-to-peer Communication Approach for a Mobile Environment",Lappeenranta University of Technology P.O. Box 20 53851 Lappeenranta Finland.

[5] Masahiro Hamasaki, Hideaki Takeda,"Proposal of Decentralized Information Sharing System using Local Matchmaking",Graduate Universities of Advanced Studies National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo JAPAN.

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 157 - 164, 2015, ISSN:- 2319–8656

Assistive Examination System for Visually Impaired

Manvi Breja
Manav Rachna College of
Engineering
Faridabad, Haryana, India

Abstract: This paper presents a design of voice enabled examination system which can be used by the visually challenged students. The system uses Text-to-Speech (TTS) and Speech-to-Text (STT) technology. The text-to-speech and speech-to-text web based academic testing software would provide an interaction for blind students to enhance their educational experiences by providing them with a tool to give the exams. This system will aid the differently-abled to appear for online tests and enable them to come at par with the other students. This system can also be used by students with learning disabilities or by people who wish to take the examination in a combined auditory and visual way.

Keywords: Speech recognition, speech synthesis, prosody analysis, phonemes, speech API.

1. INTRODUCTION

In today's era of rapidly evolving technological advances, a major change has occurred in the educational system prevalent in schools and colleges. Along with other changes in the teaching system, the examination system has evolved significantly Voice Enabled Examination System for the visually impaired people has been a very active research area for a long time and much more success is also achieved in this area.. According to the National Center for Educational Statistics , "*The number of students with disabilities attending higher education has increased. In a recent study, the number of postsecondary undergraduate students identified as having disabilities in the United States was found to be 428,280, representing 6% of the student body.*" With the growing number of blind people attending college, there has been a growing need for such system that can aid these visually impaired students .In today's era, the conventional pen and paper tests have been replaced by online examination systems. The word 'Online' here refers to not necessarily web-based or browser-dependent, but to a network that links all of the test takers to a common server. As of now, there are many companies in the industry that offer testing solutions, but none of them has on offer an examination system which is voice-enabled and assists the differently abled.

2. RELATED WORK

Technology has removed many barriers to education and employment for visually impaired individuals. Various technology exists for students with visual impairements. These include:

2.1 Screen Magnification

Screen magnification software is used by people with visual impairments to access information on computer screens. The software enlarges information on the screen by incremental factors (2 x magnification, 3x up to 20x magnification). Most screen magnification programs have the flexibility to magnify the full screen, parts of the screen, or a magnifying glass view of the area around the cursor or pointer. Commonly used screen magnification software are-

• MAGic, developed by Freedom Scientific Inc. Blind/Low Vision Group.
• ZoomText, developed by Ai Squared
• BigShot, developed by Ai Squared .

2.2 Screen Readers

A screen reader is a software application that attempts to identify and interpret what is being displayed on the screen. Screen reading software reads aloud everything on computer screens, including text, pull-down menus, icons, dialog boxes, and web pages. Screen readers run simultaneously with the computer's operating system and applications. There are mainly two types of screen readers- the CLI screen readers and the GUI screen readers.

2.3 Optical Character Recognition Systems

Optical character recognition (OCR) technology offers blind and visually impaired persons the capacity to scan printed text and then speak it back in synthetic speech or save it to a computer. There are three essential elements to OCR technology—scanning, recognition, and reading text. Initially, a printed document is scanned by a camera. OCR software then converts the images into recognized characters and words. Some of the most popular OCR systems are:

- Kurzweil 1000, developed by Kurzweil Educational Systems
- OpenBook, developed by Freedom Scientific Inc.
- Eye-Pal, developed by ABISee, Inc.

2.4 Electronic Portable Note-Takers

Electronic Braille note takers are small, portable devices with Braille keyboards for entering information. They use a speech synthesizer or Braille display for output. The user enters the information on the Braille keyboard and has the option of transferring it to a larger computer with more memory, reviewing it using the built in speech synthesizer or Braille display, or printing it on a Braille or ink print printer.
The commonly used note takers are:

- Braille 'n' Speak, developed by Freedom Scientific, Inc.
- Type 'n' Speak, developed by Freedom Scientific, Inc.
- PacMate Series, developed by Freedom Scientific, Inc.
- VoiceNote, developed by Pulse Data.

2.5 Portable Reading Devices

One of newer blind technologies is the portable reading device, which downloads books and then reads them out loud in a synthesized voice. They are specially designed with the blind and visually impaired community in mind. The Victor Reader Stream and the BookSense audio book are popular models.

3. PROPOSED SYSTEM

The prime interest behind the development of this system is to implement speech technology in an application in such a way that it enables the visually-challenged candidates to appear for a computer-adaptive online examination. The system is a stand-alone application which uses Speech-To-Text (STT) and Text-To-Speech (TTS) technology to provide the users almost all of the capabilities of a conventional online examination.

The online examination system is adaptable to different types of questions pertaining to different subjects, different time limits and different marking schemes, and can be customized according to the needs of any organization. All the data pertaining to the test is stored in a database which is linked to the application.

The Voice Enabled Examination System is able to read aloud the questions and the different options available to the test-taker. The candidate has to answer the question by speaking out the option number. The system registers the answer given by the candidate and moves on to the next question. At the end of the test, a report is generated by the system.

This system is equipped with the following functionalities:-

- Authentication of candidates via a mechanism of unique registration id and FolderLocking.
- Reading out of the questions by the application.
- Registering the answer of the candidate which has been spoken by him/her.
- Announcement of score to the candidate at the end of the exam.
- Folder Locking which ensures encryption of candidates' data in a folder and allows only the administrator to unlock that folder containing the candidates' details of the exam.
- Sending the resultant score sheet of the Examination to the registered mail id of the Candidate as well as to the Administrator.
- Generating the Certificate of scored marks and printing it at the end of the exam.
- Voice notifications to the candidates about the status of time left for each question.
- will inculcate the feature of Photograph Matching of the candidate while he appears for an exam from the administrator side for the security purposes.

The remainder of this paper is organized as follows. Section IV introduces some introduction on speech synthesis, Section V presents the concepts of speech recognition, Section VI discusses the application frameworks used, Section VII presents the snapshots of the results, Section VIII presents the future scope. Finally Section IX concludes the paper.

4. SPEECH SYNTHESIS

Speech synthesis is the artificial production of human speech. A synthesizer can be implemented in software or hardware.. A Text-To-Speech (TTS) synthesizer is a computer-based system that should be able to read any text aloud, whether it was directly introduced in the computer by an operator or scanned and submitted to an Optical Character Recognition (OCR) system. A text-to-speech (TTS) system converts normal language text into speech; other systems render symbolic linguistic representations like phonetic transcriptions into speech Synthesized speech can be created by concatenating pieces of recorded speech that are stored in a database. Systems that simply concatenate isolated words or parts of sentences, denoted as Voice Response Systems, are only applicable when a limited vocabulary is required (typically a few one hundreds of words), and when the sentences to be pronounced respect a very restricted structure. It is thus more suitable to define Text-To-Speech as the automatic production of speech, through a grapheme-to-phoneme transcription of the sentences to utter [4].

The quality of a speech synthesizer is judged by its similarity to the human voice and by its ability to be understood. An intelligible text-to-speech program allows people with visual impairments or reading disabilities to listen to written works on a home computer. Many computer operating systems have included speech synthesizers since the early 1980s. The text-to-speech (TTS) synthesis procedure consists of two main phases. The first one is text analysis, where the input text is transcribed into a phonetic or some other linguistic representation, and the second one is the generation of speech waveforms, where the acoustic output is produced from this phonetic and prosodic information. These two phases are usually called as high- and low-level synthesis. A simplified version of the procedure is presented in Figure.

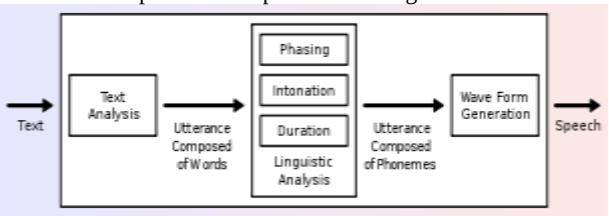


Figure 1: Process of Text-to-Speech Synthesizer

The input text might be for example data from a word processor, standard ASCII from e-mail, a mobile text-message, orscanned text from a newspaper. The character string is then preprocessed and analyzed into phonetic representation which is usually a string of phonemes with some additional information for correct intonation, duration, and stress. Speech sound is finally generated with the low-level synthesizer by the information from high-level one [8].

4.1. Process of Speech Synthesis

4.1.1. Structure analysis

Processes the input text to determine where paragraphs, sentences, and other structures start and end. For most languages, punctuation and formatting data are used in this stage.

4.1.2. Text pre-processing:

Analyzes the input text for special constructs of the language. In English, special treatment is required for abbreviations, acronyms, dates, times, numbers, currency amounts, e-mail addresses, and many other forms. Other languages need special processing for these forms, and most languages have other specialized requirements.

The remaining steps convert the spoken text to speech:

4.1.3. Text-to-phoneme conversion:

Converts each word to phonemes. A phoneme is a basic unit of sound in a language.

4.1.4. Prosody analysis:
Processes the sentence structure, words, and phonemes to determine the appropriate prosody for the sentence.

4.1.5. Waveform production:
Uses the phonemes and prosody information to produce the audio waveform for each sentence [3].

4.2. Synthesizer Technologies

The most important qualities of a speech synthesis system are naturalness and intelligibility. The ideal speech synthesizer is both natural and intelligible. Speech synthesis systems usually try to maximize both characteristics.
The two primary technologies for generating synthetic speech waveforms are concatenative synthesis and formant synthesis. Each technology has strengths and weaknesses, and the intended uses of a synthesis system will typically determine which approach is used [7].

5. SPEECH RECOGNITION SYSTEM

The speech is primary mode of communication among human being and also the most natural and efficient form of exchanging information among human in speech. Speech Recognition can be defined as the process of converting speech signal to a sequence of words by means of an algorithm implemented as a computer program. Speech processing is one of the exciting areas of signal processing[1]. Since the 1960s computer scientists have been researching ways and means to make computers able to record interpret and understand human speech. Throughout the decades this has been a daunting task. Even the most rudimentary in the early years. It took until the 1980s before the first systems problem such as digitalizing (sampling) voice was a huge challenge arrived which could actually decipher speech. Off course these early systems were very limited in scope and power. Communication among the human being is dominated by spoken language, therefore it is natural for people to expect speech interfaces with computer .computer which can speak and recognize speech in native language[2]. Machine recognisation of speech involves generating a sequence of words best matches the given speech signal. Some of known applications include virtual reality, Multimedia searches, auto-attendants, travel Information and reservation, translators, natural language understanding and many more Applications.

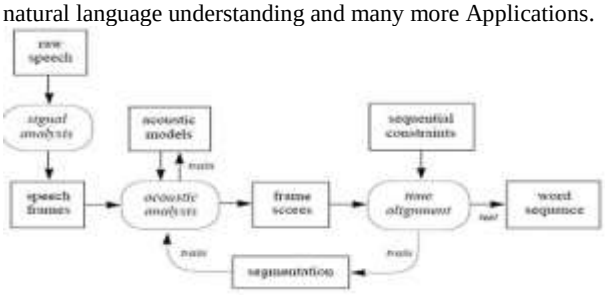


Figure 2: Structure of a standard speech recognition system.

A standard speech recognition system consists of the following components [5] **:-**

Raw speech. Speech is typically sampled at a high frequency, e.g., 16 KHz over a microphone or 8 KHz over a telephone. This yields a sequence of amplitude values over time.

Signal analysis. Raw speech should be initially transformed and compressed, in order to simplify subsequent processing. Many signal analysis techniques are available which can extract useful features and compress the data by a factor of ten without losing any important information.

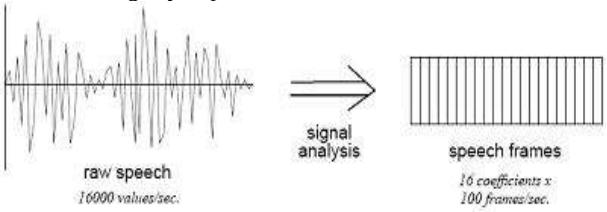


Figure 3: Conversion of raw speech to speech frames through signal anaysis

Speech frames. The result of signal analysis is a sequence of speech frames, typically at 10 msec intervals, with about 16 coefficients per frame. These frames may be augmented by their own first and/or second derivatives, providing explicit information about speech dynamics; this typically leads to improved performance. The speech frames are used for acoustic analysis.

Acoustic models. In order to analyze the speech frames for their acoustic content, we need a set of acoustic models. There are many kinds of acoustic models, varying in their representation, granularity, context dependence, and other properties.

The major steps of a typical speech recognizer are as follows:

Grammar design:
Defines the words that may be spoken by a user and the patterns in which they may be spoken.

Signal processing:
Analyzes the spectrum (i.e., the frequency) characteristics of the incoming audio.

Phoneme recognition:
Compares the spectrum patterns to the patterns of the phonemes of the language being recognized.

Word recognition:
Compares the sequence of likely phonemes against the words and patterns of words specified by the active grammars.

Result generation:
Provides the application with information about the words the recognizer has detected in the incoming audio.

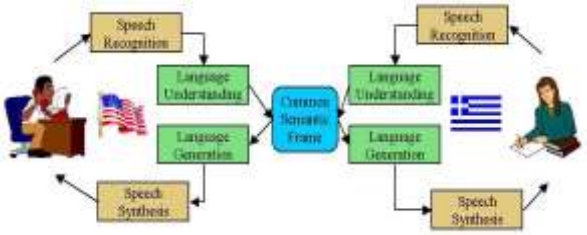


Figure 4: Process of Speech Recognition and Speech synthesis

5.1. Speech Recognition Techniques

The goal of speech recognition is for a machine to be able to "hear," understand," and "act upon" spoken information. The

earliest speech recognition systems were first attempted in the early 1950s at Bell Laboratories, Davis, Biddulph and Balashek developed an isolated digit Recognition system for a single speaker. The goal of automatic speaker recognisation is to analyze, extract characterize and recognize information about the speaker identity. The speaker recognisation system may be viewed as working in a four stages

1. Analysis
2. Feature extraction
3. Modeling
4. Testing

5.1.1. Speech analysis technique
Speech data contain different type of information that shows a speaker identity. This includes speaker specific information due to vocal tract, excitation source and behavior feature. The information about the behavior feature also embedded in signal and that can be used for speaker recognition. The speech analysis stage deals with stage with suitable frame size for segmenting speech signal for further analysis and extracting [6] .

5.1.2. Feature Extraction Technique
The speech feature extraction in a categorization problem is about reducing the dimensionality of the input vector while maintaining the discriminating power of the signal. As we know from fundamental formation of speaker identification and verification system, that the number of training and test vector needed for the classification problem grows with the dimension of the given input so we need feature extraction of speech signal

5.1.3 Modeling Technique
The objective of modeling technique is to generate speaker models using speaker specific feature vector. The speaker modeling technique divided into two classification speaker recognition and speaker identification. The speaker identification technique automatically identify who is speaking on basis of individual information integrated in speech signal The speaker recognisation is also divided into two parts that means speaker dependant and speaker independent. In the speaker independent mode of the speech recognisation the computer should ignore the speaker specific characteristics of the speech signal and extract the intended message .on the other hand in case of speaker recognisation machine should extract speaker characteristics in the acoustic signal. The main aim of speaker identification is comparing a speech signal from an unknown speaker to a database of known speaker. Speaker recognition can also be divide into two methods, text- dependent and text independent methods. In text dependent method the speaker say key words or sentences having the same text for both training and recognition trials. Whereas text independent does not rely on a specific texts being spoken

5.1.4 Matching Techniques
Speech-recognition engines match a detected word to a known word using one of the following techniques:
.
5.1.4.1. Whole-word matching
The engine compares the incoming digital-audio signal against a prerecorded template of the word. This technique takes much less processing than sub-word matching, but it requires that the user (or someone) prerecord every word that will be recognized - sometimes several hundred thousand words. Whole-word templates also require large amounts of storage (between 50 and 512 bytes per word) and are practical only if the recognition vocabulary is known when the application is developed .

5.1.4.2. Sub-word matching
The engine looks for sub-words – usually phonemes and then performs further pattern recognition on those. This technique takes more processing than whole-word matching, but it requires much less storage (between 5 and 20 bytes per word). In addition, the pronunciation of the word can be guessed from English text without requiring the user to speak the word beforehand to discuss that research in the area of automatic speech recognition had been pursued for the last three decades.

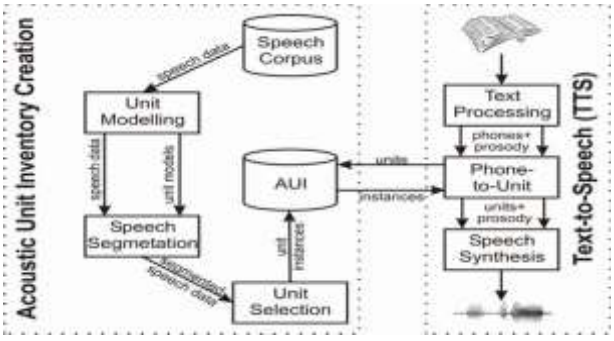


Figure 5: The general scheme of a concatenative text-to-speech system.

6. APPLICATION FRAMEWORKS

Several methods and interfaces for making the implementation of synthesized speech in desired applications easier have been developed during this decade. It is quite clear that it is impossible to create a standard for speech synthesis methods because most systems
act as stand alone device which means they are incompatible with each other and do not share common parts. However, it is possible to standardize the interface of data flow between the application and the synthesizer. Usually, the interface contains a set of control characters or variables for controlling the synthesizer output and features. The output is usually controlled by normal play, stop, pause, and resume type commands and the controllable features are usually pitch baseline and range, speech rate, volume, and in some cases even different voices, ages, and genders are available. Most of the present synthesis systems support so called Speech Application Programming Interface (SAPI) which makes easier the implementation of speech in any kind of application. For Internet purposes several kind of speech synthesis markup languages have been developed to make it possible to listen to synthesized speech without having to transfer the actual speech signal through network.

6.1. Speech Application Programming Interface

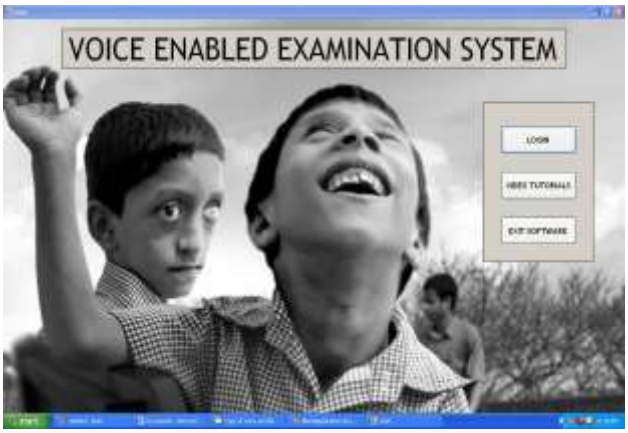
SAPI is an interface between applications and speech technology engines, both text-tospeech and speech recognition (Amundsen 1996). The interface allows multiple applications to share the available speech resources on a computer without having to program the speech engine itself. Speech synthesis and recognition applications usually require plenty of computational resources and with SAPI approach

lots of these resources may be saved. The user of an application can also choose the synthesizer used as long as it supports SAPI. Currently SAPIs are available for several environments, such as MS-SAPI for Microsoft Windows operating systems and Sun Microsystems Java SAPI (JSAPI) for JAVA based applications. SAPI text-to-speech part consists of three interfaces. The *voice text* interface which provides methods to start, pause, resume, fast *attribute interface* allows access to control the basic behavior of the forward, rewind, and stop the TTS engine during speech. The TTS engine, such as the audio device to be used, the playback speed (in words per minute), and turning the speech on and off. With some TTS systems the attribute interface may also be used to select the speaking mode from predefined list of voices, such as female, male, child, or alien. Finally, the *dialog interface* can be used to set and retrieve information regarding the TTS engine to for example identify the TTS engine and alter the pronunciation lexicon.

7. RESULTS

The proposed system opens up with the interface which has the two functionalities: login for the administrator and the student and watching the video tutorials on the related test topic.

Figure 6: Cover Page that is opened when the project is run



After clicking the login button, login page for candidate opens and from that administrator can also login. Login requires the authenticated username and password.

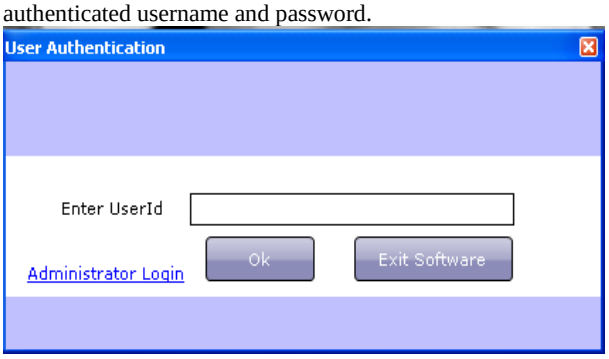


Figure 7: Login form for candidate

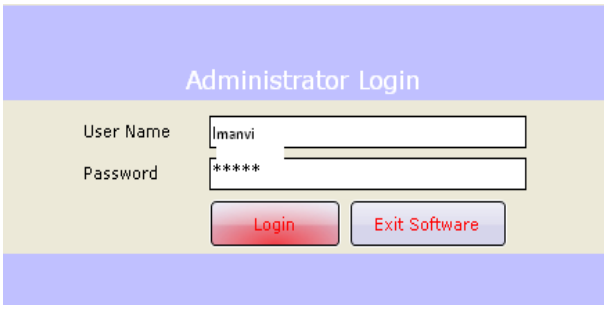


Figure 8: Login form for administrator

The administrator has the functionalities of registering the user for the system, adding the details of the users, ability to view all the user's details, folder lock facility so that the folder is authenticated, can be viewed by only the adminstrator.

Figure 9: Admin panel that opens up whenever administrator logins

The users who have come to appear for the test need to give their details to administrator for maintaining the record.

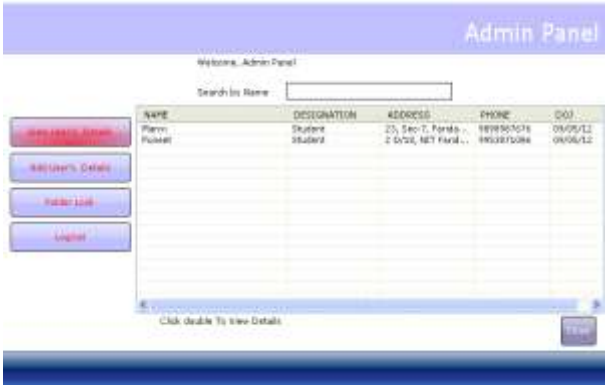


Figure 10: Display of user's details in grid layout format

The administrator has the ability to search the record of any candidate, adding the new candidate, deleting, updating the details, adding the photograph of the candidate.

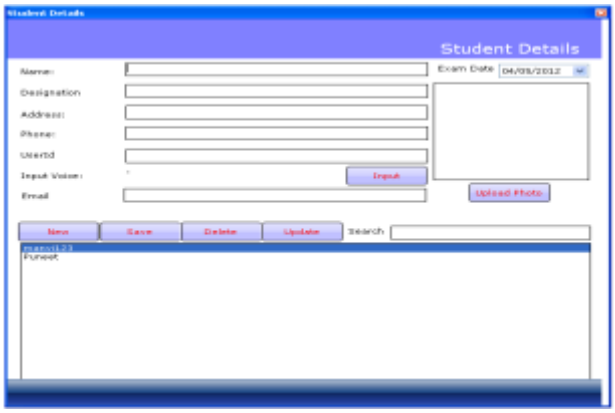


Figure 11: Add user detail form to be filled for each candidate

The administrator uses the facility of the folder lock i.e. folder in which candidate's records are kept can be accessible by only the administrator.

Figure 12: When the administrator clicks on folder lock

Figure 13: choosing the password to lock the desired folder

Figure 14: Displaying the locked status of folder

Authentication for the candidate who have come to appear for the test is also done. Since the candidate are blind, more security needs to be encorporated. Voice clip is taken when the students comes for registration. When the student will come to appear for the test, his voice clip is matched. Only when the authentication is done, the user is allowed to appear for the test.

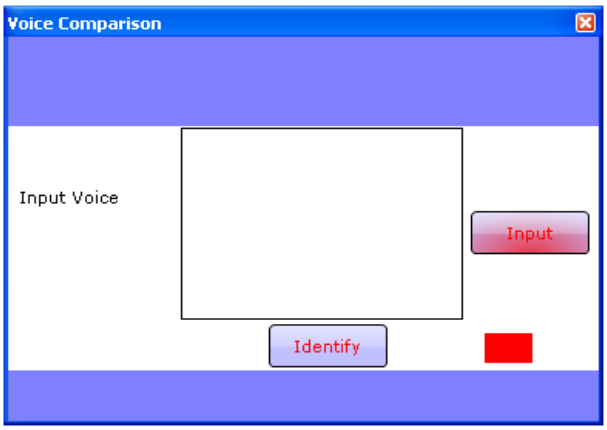


Figure 15: If authentication succeeds, matching video clip is to be browsed

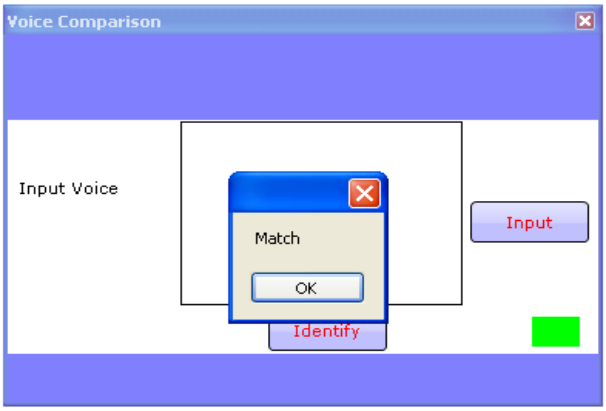


Figure 16: Displaying the status that the voice clip is matched

Now when the authenticated user login for the test, the system read aloud the initial instructions for the test.

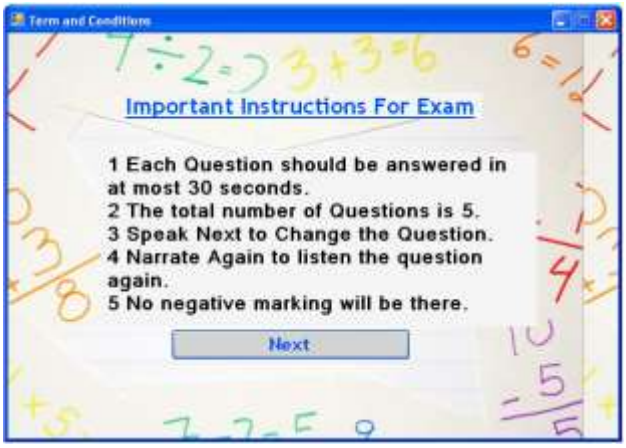


Figure 17: Instructions and guidelines for the exam

When the student listens the instruction and speaks Next, the test starts. The system reads aloud the questions and options, the student in turns speaks the option for answer. If the candidate wants to skip a certain question, he can simply go to the next one by speaking 'Next Question' or to the previous one by saying 'Previous Question'. The sytem is having the facility to tell the status of the left out time also.

Figure 18: Displaying the voice enabled exam screen

After the completion of the test, the system will announce the candidates score to him. Also, the system will generate a print of his score card and will mail a copy of the same to his e-mail id also. When the test has been completed, the system will encrypt the candidate's score and store it in the database.

8. FUTURE SCOPE

The applications of speaker recognition technology are quite varied and continually growing. Below is an outline of some broad areas where speaker recognition technology has been or is currently used.

8.1. Access Control:

Originally for physical facilities, more recent applications are for controlling access to computer networks (add biometric factor to usual password and/or token) or websites (thwart password sharing for access to subscription sites). Also used for automated password reset services.

8.2. Transaction Authentication:

For telephone banking, in addition to account access control, higher levels of verification can be used for more sensitive transactions. More recent applications are in user verification for remote electronic and mobile purchases (e- and m-commerce).

8.3. Law Enforcement:

Some applications are home-parole monitoring (call parolees at random times to verify they are at home) and prison call monitoring (validate inmate prior to outbound call). There has also been discussion of using automatic systems to corroborate aural/spectral inspections of voice samples for forensic analysis.

8.4. Speech Data Management:

In voice mail browsing or intelligent answering machines, use speaker recognition to label incoming voice mail with speaker name for browsing and/or action (personal reply). For speech skimming or audio mining applications, annotate recorded meetings or video with speaker labels for quick indexing and filing.

8.5. Personalization:

In voice-web or device customization, store and retrieve personal setting/preferences based on user verification for multi-user site or device (car climate and radio settings). There is also interest in using recognition techniques for directed advertisement or services, where, for example, repeat users could be recognized or advertisements focused based on recognition of broad speaker characteristics (e.g. gender or age).

8.6. Aids for the disabled:

One of the longest-established applications of TTS synthesis is in reading machines for the blind. The first such machine, combining an optical character reader with a TTS synthesizer, was produced by Kurzweil Computer Products in the 1970s. Even now, this speech synthesis task is very difficult as the machine must cope with any arbitrary text, and the quality of the speech that is generated would be regarded as insufficient by many people. However, these systems provide the visually impaired with the facility to read text that would not otherwise be available to them.

8.7. Remote e-mail readers:

A specialized but very useful application of TTS synthesis is to provide remote access to e-mail from any fixed or mobile telephone. For an e-mail reader, a full TTS conversion facility is required because the messages may contain any text characters.

E-mail messages are often especially challenging, due to the tendency to errors of spelling and grammar as well as the special nature of the language, abbreviations and so on that are often used. There are also many formatting features that are specific to e-mail.

9. CONCLUSION

The system has led to the development of a voice enabled examination system, as a tool for giving voice enabled exam. The system has been designed keeping in view the requirements of visually impaired students to aid them to keep pace with ordinary people in the field of education.

The testing application was based on Text-to-Speech(TTS) and Speech-to-Text(STT) technology which was implemented using Microsoft Speech API(SAPI). This web based academic testing software would provide an interaction medium for blind or partially sighted students to enhance their educational experiences.

While designing the software, the developers have used the natural voice that read aloud the questions in the test which the blind students have to answer and taken care of the accuracy of the synthetic pronunciation so as to provide the appropriate answer to the question.

The developers have made the use of Speech Application Programming Interface (SAPI) which act as an interface between applications and speech technology engines, both text-to-speech and speech recognition.

Many assistive technologies was present but no such system was offering an easy, accessible and intelligible interaction of the visually challenged with the computer. This system will prove to be an indispensable tool.

Incorporating and implementing the accessibility technology during the development of this testing application provided numerous advantages to the sighted users, thereby giving the test more efficiently. Thus voice enabled examination system, is a vital technology that can be beneficial for all types of users.

10. REFERENCES

[1] R. Klevansand, R. Rodman, “Voice Recognition, Artech House, Boston, London,1997.

[2] Samudravijaya K. Speech and Speaker recognition tutorial TIFR

[3] http://www.w3.org/TR/speech-synthesis/

[4] Nurulisma Ismail and Halimah Badioze Zaman, Search Engine Module in Voice Recognition Browser to Facilitate the Visually Impaired in Virtual Learning (MGSYS VISI-VL), World Academy of Science, Engineering and Technology, Volume 71, 2010.

[5] Michael Koerner, 1996, Speech Recognition: The Future Now, Prentice Hall Professional Technical Reference, 306.

[6] GIN-DER WU AND YING LEI “ A Register Array based Low power FFT Processor for speech recognition” Department of Electrical engineering national Chi Nan university Puli ,545 Taiwan

[7] .Dutoit, T. (1999). A short introduction to text-to-speech synthesis [Web page]. Mons: TCTS Lab, Faculté Polytechnique de Mons. Retrieved from http://tcts.fpms.ac.be/synthesis/introtts_old.html.

[8] http://en.wikipedia.org/wiki/Speech_synthesis- speech

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 165 - 169, 2015, ISSN:- 2319–8656

New Technique for Image Encryption Based on Choas and Change of MSB

Fariba Ghorbany beram
Sama Technical and Vocational Training College
Islamic Azad University
Shoushtar Branch, Shoushtar
Iran

Mojtaba khayt
Sama Technical and Vocational Training College
Islamic Azad University
Shoushtar Branch, Shoushtar
Iran

Sajjad Ghorbany Beram
Sama Technical and Vocational Training College
Islamic Azad University
Shoushtar Branch, Shoushtar
Iran

Abstract:
In this paper, an algorithm for image encryption using chaotic systems and techniques to change the pixel values are proposed for protecting digital images in an efficient and safe manner will be offered. In the proposed algorithm, the stochastic properties of chaotic Logistic system is used. To evaluate the performance of the proposed algorithm, we have implemented it in MATLAB using parameters such as visual analysis, key space analysis, histogram analysis. Implementation results show that the proposed algorithm, the algorithm is efficient and safe.

1. INTRODUCTION

Cryptography is the science of code and secrets. It is an ancient art and it has been used for several centuries amang commeders, informers and others to protect the message amang them and to keep the messages privately. When we are dealing with the data safety, we need the identity sender and receiver of the message and also we should make sure about the content of message has not been manipulated. These three subjects, in other words, confidentiality, confirming the identity and generality are at the center of safety of modern data communication and can make use of cryptography. As a whole, this issue should be guaranteed that a message can only be decoded(read) by means of the people to whom the message has been sent and others are not allowed to read them. The method wich provides this issue is called cryptography[1,2,3].

2.CHAOS

Chaos is a phenomenon wich takes place in the definable nonlinear systems that have a lot of sensitivity against the primary conditions and their uasi randomized behavior suchlike systems satisfy the liapanof appearance they will be in a stable condition in the peak of chaos. The out put of this system is always under the effect of primary amounts of input. On the other hand prediction of this kind of signal is almost impossible with having the primary amounts and the physical appearance(shape) of this signal is similar to noise. The chaos environs have the following specifications:high sensitivity in relation to the primary conditions, exactness and lack of statistical prediction[4,5,6].

Formula1

$$X_{n+1}=r.xn(1-x_n)$$

x_n is the state variable being in the interval [0, 1] and r is system parameter which might have any value between 1 and 4. In this paper we have used the logistic function to generate the secret key.

3. THE PROPOSED METHOD

In this study an algoritm is presented which changes the order of pixels in the input image in a way that there will be very difference between the input and output image. At first we divide the input image into three sub-bands, namely red, green, blue to satisfy our expectation, and the current place of pixels is randomly changed into a place which is determined by means of fourmalu2,3. In order to change the mounts of the pixels which are fixed in new places with ane of the lines of table1 which is randomly assigned by fourmala4. table 1 includes 16 lines that each line with 4 valuable bits is xor with the pixels amounts.

Fourmalu2

$$X_{n+1}=(r.xn(1-x_n))*a \quad 1<a<\text{number of rows}$$

Fourmalu3

$$X_{n+1}=(r.xn(1-x_n))*b \quad 1<b<\text{number of columns}$$

fourmalu14

$$X_{n+1}=(r.xn(1-x_n))*c \quad 1<c<16$$

a, b are selected so that the Chaos integer between 1 to Number of rows and 1 columns are generated, and c are

determined by a number between one and sixteen production so that each execution of the scalar random selection row of table 1 is selected.

For example, if the pixel value 150 is a binary value of 10010110 is then based on the value of the Formula 4 comes a row of Table 1 is selected and a four digit value of number(10010110), XOR, and the new value replaces the pixel values of previous that is, if the number 14 is derived from the logistic map, 4MSB(most sign bit of number) with the number 150 (1001) with row 1 of table (1110), XOR is and result is 118(Figure1,2).

Table1

ROWES	XOR
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111

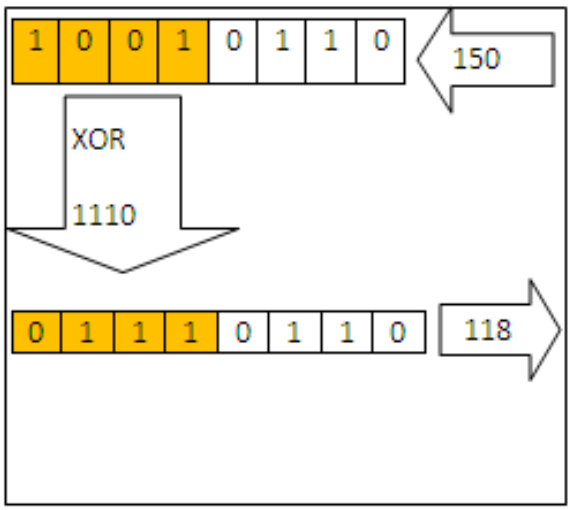


Figure1-change MSb of pixel with the selected rows

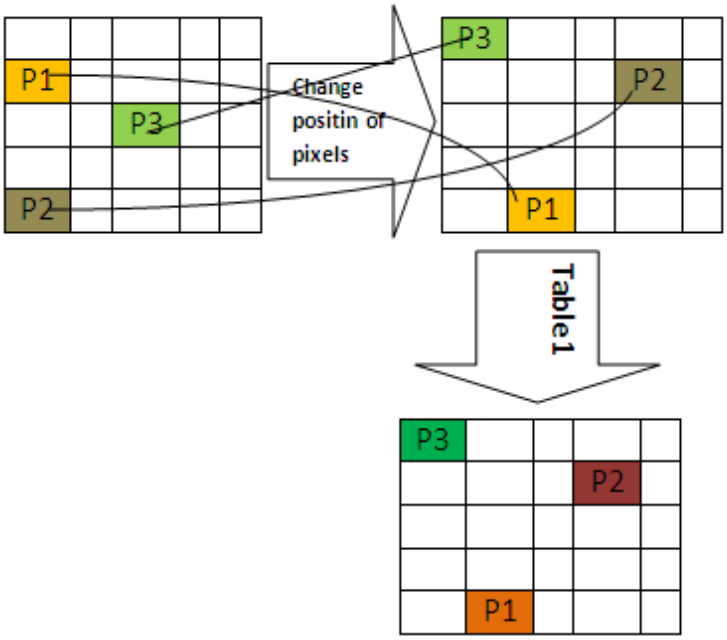


Figure 2-Flowchart of the data encryption process

The image is composed of pixels, the pixel values are in hiding and encryption technique for digital images. Change in the least significant bit[7,8,9] of a pixel, which is technically referred to as steganogeraphy[10,11,12](Figure 3).

As shown in Figure 4, we change a bit in the pixel values of images will not cause a visual change .in this paper we have used the change in the msb. As we see in Figure 5, this change is very real.
We also intend to change the values of the pixels in such a way that the basic shape vary.

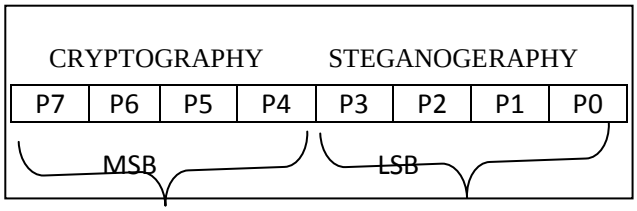


Figure 3

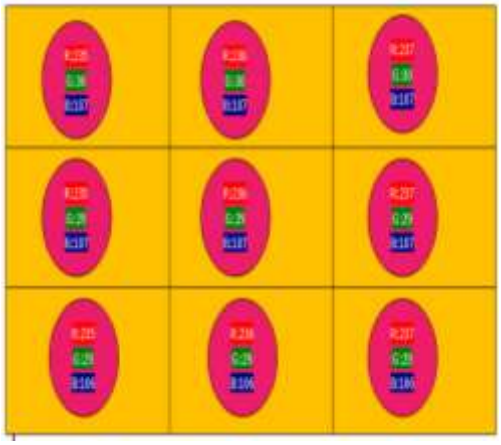


Figure4.change of LSB bits of pixel

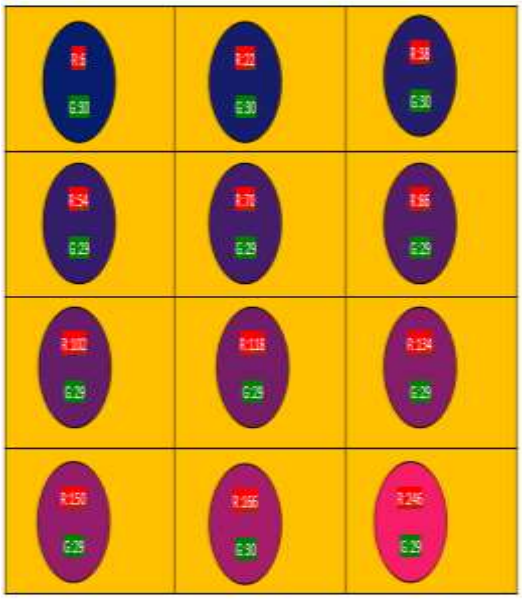


Figure5.change of MSB bits of pixel

A. Encryption algorithm

1) The original image into three sub-bands of red, green and blue break

2) change position of pixel(row and column) based on the logistic map.

3) Changing the pixel values given in Table 1.

4. IMPLEMENTATION

A method of good cryptography must be resistant against difference kinds of code-detection and statistical attacks. In the continuation the suggested algoritm will be analysis, the analysis of sensitivity of this method in relation to key changing, the analysis of The key space and **histogram**.

A. THE HISTOGRAM CHART

it is a kind of method of examining the encoded image of observation, a good cryptography algoritm should arrange the image in such a way that its specifications not to be specifiable. Also, no kind of information in the encoded image by comparing the encoded image with the main image should be observed. The main image and the encoded image should be seprate visually. The analysis of histogram expresses that pixels are distributed. In the images by means of drawing the observations numbers of the light severity. However we con not find the major image by prossessing the chart. In cryptography the greater difference between the main image histogram and encoded image will cause the safer algoritm. As it come be clearly seen in Figure6, Figure7, Figure8 and Figure 9 , that the histogram of cryptography image is totally different from the main image histogram. This problem increases th risk of possibility of statistical attacks. The analysis of random of randomization:an algoritm should have certain suitable probable features such as good distribution, high complexity and efficiency in order to have more security.

Figure 6-original image

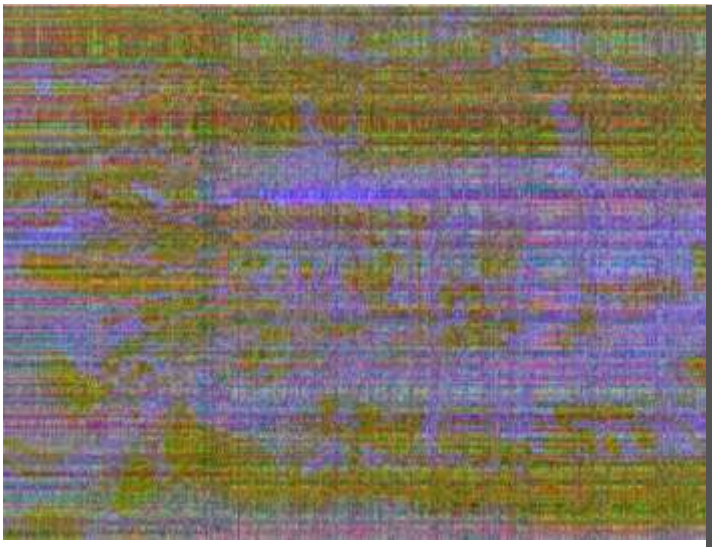


Figure7-encrypted image

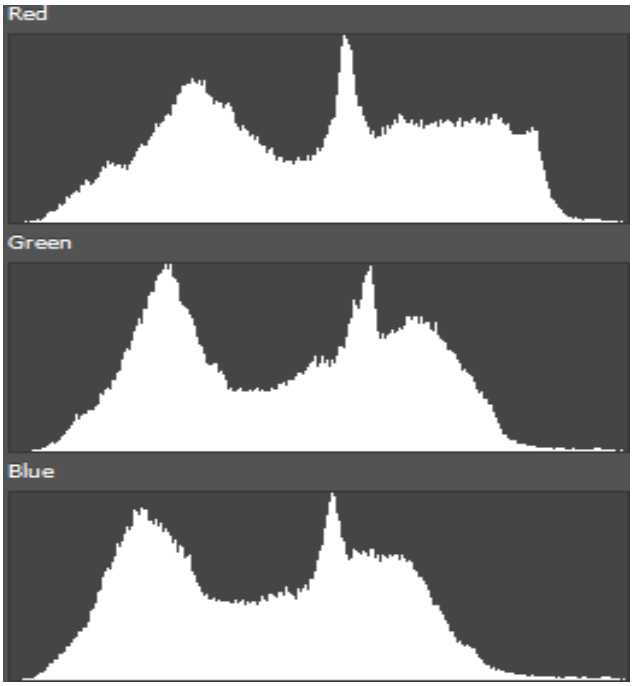


Figure8- histogram of original image

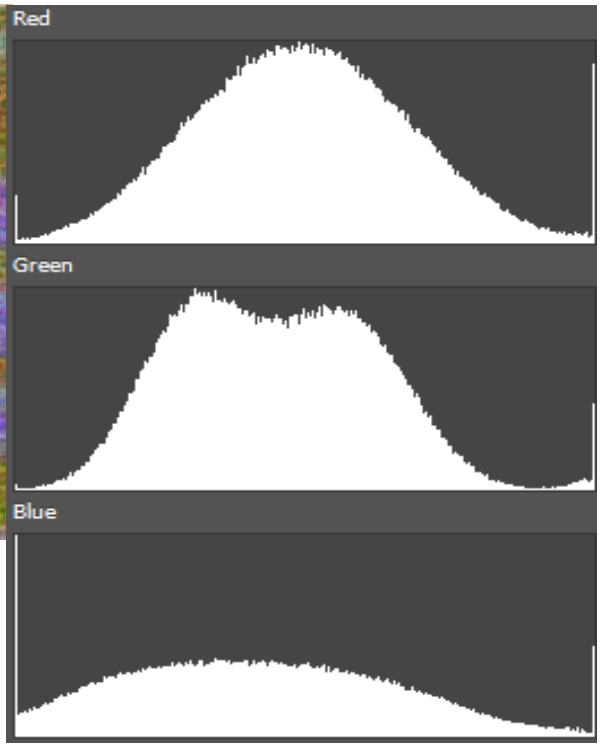


Figure9- histogram **of** encrypted image

B. THERE ARE VARIOUS WAYS IN ORDER TO CREATE RANDOM NUMBERS

Today, researchers have paied special attention to chaos systems. We applied logestic chaos system to make random number in this paper. Fourm1 shows one of most famous signals which has chaos behavior and it is called logestic map. While r[3.57 4] the behavior of system is generally like a chaos.

As a whole one ideal feature for an encrypted image is its sensitivity in relation with the partial changes in the main image, in other words changing one pixel. The invader tries to create some partial changes in the input images to observe the result changes in the secret image. By usig this method the meaningful relation between the main image and the encrypted image will be obvious. This activity itself made the key to be diagnosed and to be known in more simple way. one of the feauures of evaluating the cryptography algoritms is the analysis of sensitivity to the key[9]. Namely, making changes in the key should create a totally different encrypted image.to do this, it is enough to change the amounts of x,y,r in the suggested algoritm, as a result, regarding the feature of chaos environs which are related to the primary elements, the produced amounts change and the result of it is creating different encrypted images(Figure10,11).

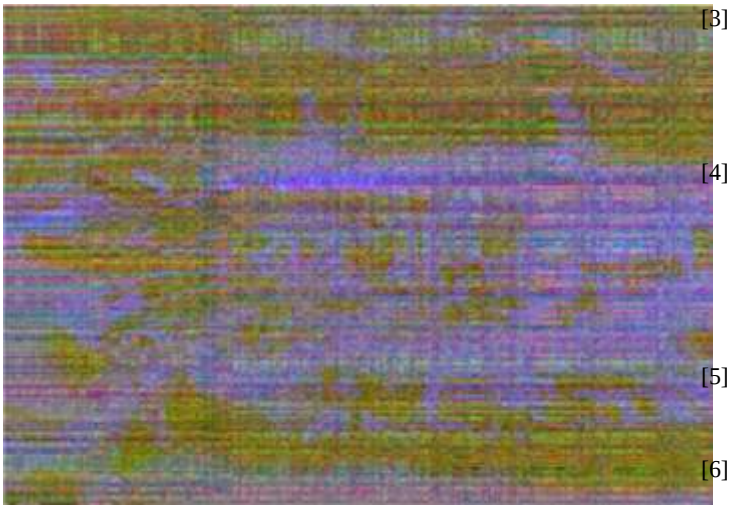


Figure10.image encrypted based on initial x_1,y_1,r_1

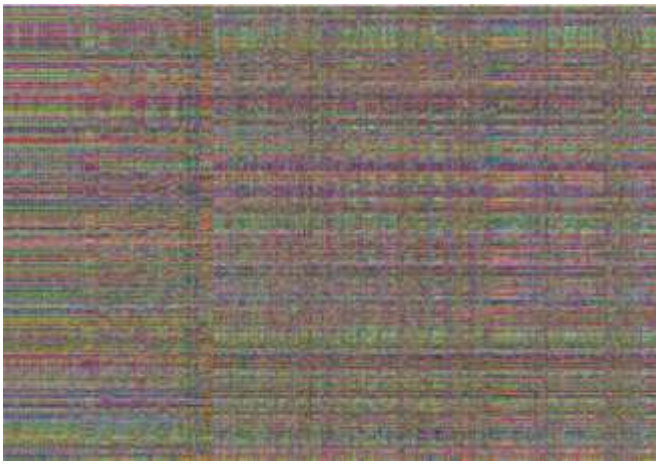


Figure11.image encrypted based on initial x_2,y_2,r_2

5. CONCLUSION

An algoritm for cryptography of image was introduced in this article. The suggested algoritm was evaluated by means of some exams to assess the efficacy of the algoritm. The result of visual tests and the analysis of histogram showed that there is not any obvious fiber in the encrypted images by suggested algoritm and there is no similarity between the main image and the encrypted image from the viewpoint of statistics. The result of the analysis of sensitivity to the key showed that the suggested algoritm is very sensitive regarding switching the key.

6. REFERENCES

[1] Shiguo Lian_, JinshengSun, Zhiquan Wang, "Security analysis ofa chaos-based image encryption algorithm", Elsevier, Physica A, Vol. 351, pp. 645–661,2005.

[2] B. Schneier, "Applied Cryptography Second Edition : protocols, algorithms, and source code in C", ISBN 9971-51-348-X, John Wiley & Sons,1996.

[3] Fethi Belkhouche, Uvais Qidwai, Ibrahim Gokcen, Dale Joachim, "Binary Image Transformation Using Two-Dimensional Chaotic Maps", IEEE, Proceedings of the 17th International Conference on Pattern Recognition (ICPR), 2004.

[4] Grummt, E., Ackermann, R.: Proof of Possession: Using RFID for large-scale Authorization Management. In: Mhlhuser, M., Ferscha, A., Aitenbichler, E. (eds.) Constructing Ambient Intelligence, AmI-07 Workshops Proceedings. Communications in Computer and Information Science, pp. 174, 182 (2008)

[5] Pecorra, L.M., Carroll, T. L.,"Synchronization in chaotic systems", Phys. Rev. Lett., Vol. 64, No. 8, pp. 821–824, 1990.

[6] Pareek, N.K., Patidar, V., Sud, K.K., "A Random Bit Generator Using Chaotic Maps", International Journal of Network Security, Vol. 10, No. 1, pp. 32-38, 2010.

[7] Mohammad Ahmad Alia, A.A.Y., Public–Key Steganography Based on Matching Method, in European Journal of Scientific Research.2010.p.209

[8] D. Bret, A detailed look at Steganographic Techniques,US:SANS institute, 2002.

[9] Belkacem, S. Dibi, Z. Bouridane, "Color Image Watermarking based on Chaotic Map", 14th IEEE International Conference of Electronics, Circuits and Systems, 2007.

[10] Masoud Nosrati , Ronak Karimi," A Survey on Usage of Genetic Algorithmsin Recent Steganography Researches", World Applied Programming, Vol (2), No (3), March 2012. 206-210,ISSN: 2222-2510,©2011 WAP journal. www.waprogramming.com

[11] Indradip Banerjee, Souvik Bhattacharyya, Gautam Sanyal," A Procedure of Text Steganography Using Indian Regional Language", J. Computer Network and Information Security, 2012, 8, 65-73 Published Online August 2012 in MECS (http://www.mecs-press.org/)

[12] Seyyed Amin Seyyedi, Rauf.Kh Sadykhov," Digital Image Steganography Concept and Evaluation", International Journal of Computer Applications (0975 – 8887) Volume 66– No.5, March 2013

International Journal of Computer Applications Technology and Research
Volume 4– Issue 2, 170 - 174, 2015, ISSN:- 2319–8656

Adaptive Steganography Based on Logistic Map

Fariba Ghorbany Beram
Sama Technical and Vocational Training College
Islamic Azad University,
Masjedsoleyman Branch, Masjedsoleyman,
Iran

Sajjad Ghorbany Beram
Sama Technical and Vocational Training College
Islamic Azad University,
Masjedsoleyman Branch, Masjedsoleyman,
Iran

Abstract:
umerous novel algorithms have been proposed in the fields of steganography with the goals of increase security,capacity and imperceptibility. In this paper, we introduced a new blind adaptive algorithm in image steganography technique to Improving that goals. The existing methods hide the information using constant bit length in integer wavelet coefficients. This paper uses variable bit length based on float wavelet coefficients to hide the data in a particular positions using secret key. The proposed method try to obtain an optimal mapping function to reduce the difference error between original coefficients values and modified values. we provided with the double security by using a secret key only known to both sender and receiver, therefore improving goals compared to the existing algorithm.

Keywords: Steganography; Security; Logistic Map; capacity; image

1. INTRODUCTION

over the last decade, one of the most significant current discussions in computer science is the field of information security. In general, information security is the techniques, policies and strategies used to protect and secure computer systems, in maintaining the operations of an organization. One of the concerns in information security is the concept of information hiding. It is the process of embedding information into digital content without causing perceptual degradation. Steganography of current information hiding has shown that steganography is one of the recent important subdisciplines. This is because most of the proposed information hiding system is designed based on steganography. Today, steganography is most often associated with the high-tech application where data are hidden with other information in an electronic file[1]. Generally speaking, a good steganographic technique should have good visual imperceptibility and a sufficient capacity of hidden secret data[2]. Steganographic methods can be classified into spatial domain embedding and frequency domain embedding[3,4]. Almost all digital file formats can be used for steganography, but the image and audio files are more suitable because of their high degree of redundancy [5].

2. RELATED WORKS

In this section we introduce some of the methods described Steganography . For this purpose, two groups of methods in the spatial domain and transform domain techniques will be examined.In the spatial domain techniques, secret messages are placed in a carrier media, without prior information hiding, on a carrier medium, the conversion will be done. Confidential data is actually placed directly on the carrier media. One of the first Steganography techniques, using the least significant bits of the carrier media. The use of this technique for placement of confidential information on a carrier media, not a tangible change in the media.

Steganography the images presented in lots of different techniques, the goal of all of them is the availability of high capacity, security, and resistance. These three criteria are in conflict with each other and simultaneously achieve all three simultaneously is very difficult and perhaps impossible. Three objectives are stated at the three vertices of a triangle. The matter requires attention to each other and not all of these parameters simultaneously met in the best way.Wavelet transform gives the best result for image transformation[6]. the frequency domain transform we applied in this research is Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT consists of two operations: Discrete Wavelet Transformation has its own excellent space frequency localization property. Applying DWT in 2D images corresponds to 2D filter image processing in each dimension. The input image is divided into 4 non-overlapping multi-resolution sub-bands by the filters, namely LL1 (Approximation coefficients), LH1 (vertical details), HL1 (horizontal details) and HH1 (diagonal details). The sub-band (LL1) is processed further to obtain the next coarser scale of wavelet coefficients, until some final scale “N” is reached. When “N” is reached, we’ll have 3N+1 sub-bands consisting of the multi-resolution sub-bands (LLN) and (LHX), (HLX) and (HHX) where “X” ranges from 1 until “N”. Generally most of the Image energy is stored in these sub-bands[7,8,9,10]. The least significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image in spatial domain but it has some limitations such as it is easier to understand using steganalysis[11,12]. Variable Embedding Ratio and LSB is used in [13]. paper[14] proposes a method for image steganography. The chosen Variable Embedding Ratio [VER] is 4:2 that is 4 bits are embedded in edge pixels and 2 bits in other pixels.In[15] uses variable bit length based on integer wavelet coefficients to hide the data in a particular positions using secret key by LSB substitution method. In smooth areas they embed three bits of secret information. In the complicated areas, variable rate bits are embedded[16].

3. SECRET KEY

we use chaos theory to produce secret key. The name "chaos theory" comes from the fact that the systems that the theory describes are apparently disordered, but chaos theory is really about finding the underlying order in apparently random data. The nonlinear dynamics researchers have observed an interesting relationship between chaotic behavior and Random number generator systems as many properties of the chaotic systems such as their sensitivity to initial conditions can be considered to the confusion in generation of secret keys. Deterministic pseudorandom numbers are used for the generation of secret key in cryptography system. The logistic map is a very simple mathematical model often used to describe the growth of biological populations. The simple mathematical form of the logistic map is given as [17]:

$$X_{n+1}=r.xn(1-x_n) \quad (1)$$

x_n is the state variable being in the interval [0, 1] and r is system parameter which might have any value between 1 and 4. In this paper we have used the logistic function to generate the secret key. If this function is quite Chaotic behavior, you would have x_0=0.3 amnd 3.57<r<4.

4. PROPOSED METHOD

wavelet transform is applied to the cover image to get the wavelet coefficients. the wavelet coefficients is splitted into RGB planes .The obtained wavelet coefficients from the RGB planes, select one or two or three planes according to the secret key and Each selected plane is decomposed into m*m blocks according to the secret key.Range, the number of bits that can be replaced, between 1 to logarithm biggest coefficient value. According to the value of coefficients, the number of bits replaced The secret message is determined. It makes Optimal Use of the Wavelet Coefficients. While fewer number of coefficients are modified, More bits can be replaced. After replacement, inverse wavelet transform applied to restore the image (Fig 1).

4.1 Embedding procedure:

cover image is splitted into R, G, B planes .
Each RGB is converted into frequency domain by using Haar wavelet transform.
Select RGB plans based on secret key .
selected RGB plane is decomposed into blocks based on secret key .
Value of wavelet coefficient are classified

{D=2^{n-1} –2^n-1,n =log (coefficient)}D is range value of wavelet coefficient, n-1 is number of secret data bits to be embedded and coefficient is value of wavelet coefficient ,dec(n) is the decimal value of secret data bits.

If 2^{n-1} < coefficient <2^n-1 then

(2^n–dec(n bit of secret data))/2

1) Determine the inverse wavelet transform(idwt) on each RGB planes to restore the image.

4.2 Extraction procedure:

1) stego image is splitted into RGB planes .
2) Select RGB plans based on secret key .
3) Each RGB is converted into frequency domain by using Haar wavelet transform.
4) Each RGB plane selected is decomposed into blocks.
5) Select blocks based on secret key.
6) Value of wavelet coefficient are classified :

If 2^{n-1} < coefficient <2^n-1 then

x=(2^n – coefficient)*2

message[]=dec2bin(x)

coefficient is value of wavelet coefficient stego image and message is data extraction from stego image .

If coefficient=18 and secret message is 111011 then
16<23<32 ,n=5, number of bits is 4.select 4 bits of secret message(1110) .dec(1110) is 14.
32-14/2=25
We put 25 instead of 23 in the picture .
For extract,if stego coefficient is 25 then
16<25<32
Secret mesage=dec2bin((32-25)*2)= dec2bin(14)=1110
So we had to replace bits that just were extracted.

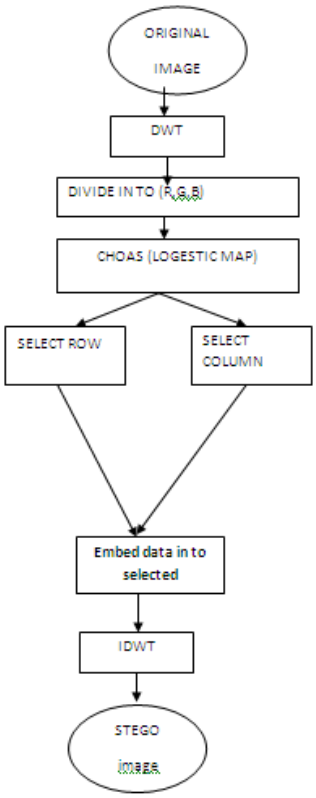


Fig 1. Proposed Block Diagram Data Embedding

5. RESULTS AND DISCUSSION

My proposed algorithm was implemented in MATLAB and are tested with many colored images. In this paper We selected 512x512 "Lena" jpeg image to perform our testing. Fig 2 has been shown cover image, Fig 3 has been shown stego image. The performance of various steganographic methods can be rated by the three parameters: security,capacity and imperceptibility. The steganographic methods proposed in this paper are very secure as variable number of bits are hidden in different coefficient of wavelet. This method embeds secret information in a random order using a secret key only known to both sender and receiver So it is very difficult to find out the hidden data from the stego image. The same stego image can also bear different secret image for different receiver depending on their secret key. Capacity means the amount of message that can be embedded. Table I, show Average PSNR values and Embedding Rate achieved using standard images.

Table I. Average PSNR values achieved using standard images

Embedding Rate	0.01	0.02	0.05	0.20	0.25	0.35
PSNR	64	61	55	49	48	46

Fig 2.Cover Image Stego image

Fig3 indicative of the blue before placing a secret message in an image and then paste the information is confidential, tangible change in the color chart, as we will be created.

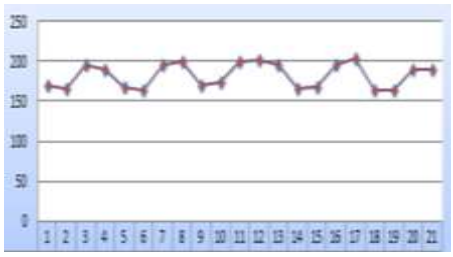


Fig 3. blue before and after placement

In the proposed algorithm [18] The image edges are detected by using the cany operator. In this way, four bits per pixel that are on the edge, and two bits in the others pixels are hidden hidden. Since a variable number of bits of the secret message in different parts of the image data, the method is safe, Because if that person is suspected of carrying forward the media until the algorithm is not available, the least significant bits of the secret message can not be retrieved. The disadvantage of the method is to extract the secret message from the carrier at destination media, the media must also be present. We have the advantage of variable bit rate method [18] in the proposed algorithm, we use the other hand to eliminate the disadvantage of my method.

Compare the signal to noise of the proposed method and algorithm [18] shown in Fig 4. As we observe the same replacement rate, the proposed algorithm provides better results.

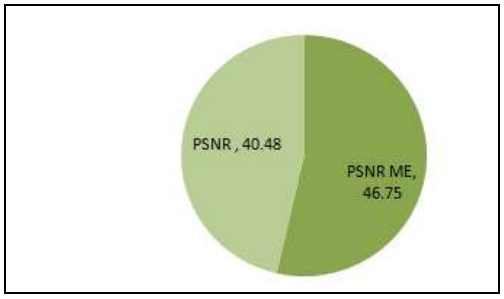


Fig4. compares the psnr in the replacement rate of 262,144

If Steganography image H1 and original image H ,HWIDTH, HLEN number of rows and columns of the image are calculated PSNR and MSE of the Equation (2) , Equation (3) is calculated.

(2)

$$MSE=\frac{\sum_{i=1}^{H\ LEN}\sum_{j=1}^{H\ WIDTH}[H(i,j)-H1(i,j)][H(i,j)-H1(i,j)]}{HLEN*HWIDTH}$$

(3)

PSNR=10* $log_{10}\left(\frac{255*255}{MSE}\right)$

The mean square error (MSE) is reduced, the image quality was high. Low value, the maximum amount of signal to noise ratio (PSNR) of the carrier image is of poor quality

6. CONCLUSION

In this paper we proposed a data hiding scheme that hides data into the float wavelet coefficients of an image. The system combines a float wavelet transform and the variable rate of embedding to maximize performance of steganographic method proposed. Because of the the chaos system is used, the proposed method is secure.

entirely By using this method the data hiding capacity is improved and secrecy of the embedded data bits can be provided. It is also seen that the stego image formed is of good quality. Future work may be carried out to increase the capacity and enhance the visual quality of the stego image by improving the PSNR value . The methods proposed in this paper are:

- very secure
- capacity is good.
- PSNR obtained is approximately maximum compared to the existing algorithm which confirm imperceptibility of the host and the stego image.
- The proposed system also reduces the difference between original coefficients values and modified values by using the adaptive float coefficient adjustment.
- Blind steganogeraphy method

7. REFERENCES

[1] Roshidi Din and Azman Samsudin," Digital Steganalysis: Computational Intelligence Approach", INTERNATIONAL JOURNAL OF COMPUTERS Issue 1, Volume 3, 2009

[2] Arun Rana, Nitin Sharma, Amandeep Kaur," IMAGE STEGANOGRAPHY METHOD BASED ON KOHONEN NEURAL NETWORK", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.2234-2236

[3] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal,"A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier", Journal of Global Research in Computer Science ISSN:2229-371X www.jgrcs.info, Volume 2, No. 4, April 2011

[4] Lifang Yu, Yao Zhao, Rongrong Ni (EURASIPMember), and Ting Li,"Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm", EURASIP Journal on Advances in Signal Processing,Volume 2010, Article ID 876946, 6 pages

[5] Souvik Bhattacharyya, Gautam Sanyal,"A Robust Image Steganography using DWT Difference Modulation (DWTDM)", I. J. Computer Network and Information Security, 2012, 7, 27-40 Published Online July 2012 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2012.07.04

[6] Saddaf Rubab, M. Younus," 29 Improved Image Steganography Technique for Colored Images using Wavelet Transform", International Journal of Computer Applications (0975 – 8887) Volume 39– No.14, February 2012

[7] Po-Yueh Chen* and Hung-Ju Lin,"A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

[8] Tanmay Bhattacharya, Nilanjan Dey, S. R. Bhadra Chaudhuri,"A Session based Multiple Image Hiding Technique using DWT and DCT", International Journal of Computer Applications (0975 – 8887) Volume 38– No.5, January 2012

[9] S. Jayasudha," Integer Wavelet Transform based Steganographic Method using OPA Algorithm", International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012

[10] N S T Sai, R C Patil," Image Retrieval using DWT with Row and Column Pixel Distributions of BMP Image", N S T Sai et al. / (IJCSE) International Journal on Computer Science and Engineering ,Vol. 02, No. 08, 2010, 2559-2566

[11] Dr. Mohammed Abbas Fadhil Al-Husainy,"COMPARISON STUDY BETWEEN CLASSIC-LSB, SLSB AND DSLSB IMAGE STEGANOGRAPHY", ICIT 2013 The 6th International Conference on Information Technology

[12] S.Shanmuga Priya, K.Mahesh, Dr.K.Kuppusamy,"Efficient Steganography Method to Implement Selected Lease Significant Bits in Spatial Domain (SLSB – SD)", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622

[13] Tanmay Bhattacharya, Bikash Debnath,S. R. Bhadra Chaudhuri," A Session based Spatial Domain Multiple Image Hiding Technique using Variable Bit Replacement and Multiple Passwords", International Journal of Computer Applications (0975 – 8887) Volume 56– No.13, October 2012

[14] Geetha C.R, H. D. Giriprakash," Image Steganography by Variable Embedding and Multiple Edge Detection using Canny Operator", International Journal of Computer Applications (0975 – 888) Volume 48– No.16, June 2012

[15] Sumanth Sakkara.,Akkamahadevi D.H, K. Somashekar," Integer Wavelet based Secret Data Hiding By Selecting Variable Bit Length", International Journal of Computer Applications (0975 – 888) Volume 48– No.19, June 2012

[16] Moazzam Hossain, Sadia Al Haque, and Farhana Sharmin," Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information", The International Arab Journal of Information Technology, Vol. 7, No. 1, January 2010

[17] Grummt, E., Ackermann, R.: Proof of Possession: Using RFID for large-scale Authorization Management.
In: Mhlhuser, M., Ferscha, A., Aitenbichler, E. (eds.) Constructing Ambient Intelligence, AmI-07 Workshops

Proceedings. Communications in Computer and Information Science, pp. 174, 182 (2008)

[18] Geetha C, Giriprakash H.2012. image steganography by variable embedding and multiple edge detection using canny operator . International Journal of Computer Applications (0975 – 888) 48:15-19