International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 01-02, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1001

Design of Bit Width Converter Based on PCIE4.0

Linjun Liu
Chengdu University of Information Technology
Chengdu, China

Hai Nie
Chengdu University of Information Technology
Chengdu, China

Weiwei Ling
Chengdu University of Information Technology
Chengdu, China

Abstract: Aiming at the data bit width conversion module used in PCIE4.0 physical coding layer, this paper designs a backwards compatibility-capable implementation method, which combines the version below backwards compatibility 4.0. According to the data bit width selection signal BusWidth of MAC layer in PCIE protocol, the current running speed of PCIE is selected. So as to select the form of bit width conversion. The designed PCIE internal strobe signal is 32 bits wide, and the correctness of its coding operation mode is verified by using the description language of Verilog hardware and the joint simulation form of Verdi and VCS.

Keywords: compatibility; Bit width selection; High speed interface; PCIE4.0;

1. INTRODUCTION

PCI Express(PCIE) was originally designed as a local bus interconnection technology to connect CPU, GPU and I/O devices inside the machine, and has developed into a mature switching network, which is characterized by point-to-point end-to-end. Bus is a bridge connecting the interfaces between computer subsystems, and the interfaces between each subsystem are connected with each other through bus[1]. In the era of information technology explosion, people's demand for information transmission and data processing is increasing day by day. Compaq company puts forward the concept of distinguishing the system bus from I/O interface bus[2], which makes the high-speed processor develop rapidly. Compared with bus, the development of I/O bus is relatively slow, which makes I/O bus gradually become a major bottleneck in computer development. With the improvement of technology, PCIE has gradually moved towards a broader stage. PCIE is the most widely used industry standard for connecting hardware peripherals to computer systems. It uses point-to-point links, one of which contains 1 to 16 channels, and each channel is a full-duplex serial connection. In 1991[3], Intel Company proposed that when the bit width is expanded to 32 bits, its bandwidth can reach 133MB/s, and the data of this bus can be read and written suddenly, and the peripheral components of the supporting device can work in multiple groups at the same time[4]. PCIE4.0, the speed has been increased from 8Gbps to 16Gbps. In the PCIE version, the encoding form adopted for Gen1/Gen2 is 8b/10bde, but in Gen3/Gen4, it is 128b/130b. When developing to a high version protocol, the bit width of data changes with the setting of internal channels. This paper will design a bit width conversion module that can change the designed bit width only by modifying the code of the bit width conversion module.

2. DATA BIT WIDTH CONVERSION

The sending part of PCIE mainly converts the parallel data bit width transmitted by the MAC layer. The inner part width is defined as 32 bits, and the control signal of PCIE4.0 data is processed synchronously[5]. In this case, the processing of bit width is different due to the selection of BusWidth of bitwidth signal. When the selected bit width signal is in PCIE Gen1/Gen2, the encoding mode of the data is 8b/10b, and the input data bit width of this part can be selected as 8, 16 and 32[6]. However, the set data bit width channel is 32 bit width, so there are three ways to adjust the data bit width. When the data is in Gen3/Gen4, at this time the encoding mode of data processing is 128b/130b at this time the internal selection of the data communication number is still set to 32 bits wide, but at this time the expenditure of data input only 16, 32 two, so there are two ways to adjust the data. Therefore, according to the above data bit width selection, different bit width selection processing will be carried out[7].

3. DESIGN AND IMPLEMENTATION

Data bit width conversion mainly synchronizes the input data at the same bit width and rate during PCIE Gen3/Gen4. This data bit width conversion is mainly used to synchronize the input data with different bit width and rate under Gen3.0 and Gen4.0 protocols[8].

The design essence of data bit width conversion is signal processing under asynchronous clock. The TxstartBlock signal and the Tx_DataValid signal in the sys_clk clock domain need to be converted to the pclk clock domain according to the current rate requirement. The internal channel bit width is defined as 32 bits in the following three cases:

1. When the BUS_WIDTH signal is 00, the width of the data bit in the sys_clk clock field is the same as the width of the data bit inside the sys_clk clock field. The input signal only needs to be beaten and synchronized.

2. When the BUS_WIDTH signal is 01, the data bit width under sys_clk clock field is 16 bits, which is different from the internal data bit width, and the two clocks are different. Under PCle4.0, sys_clk is 1Ghz and pclk is 500Mhz, which is single-ratio fast to slow cross-clock domain processing. In order to prevent data leakage, level extension (handshake) is adopted.

3. When the BUS_Width signal is 10, the data bit width of sys_clk clock domain is 8 bits, which is different from the internal data bit width, and the two clocks are also different. Under PCle4.0, sys_clk is 2Ghz and pclk is 500Mhz. Level extension (handshake) is used to prevent leakage.

For data signals, as specified by the protocol, TxstartBlock signal will be extended by one beat and Tx_DataValid signal will be set low when the synchronization head of the transmitted data reaches the data bit width of the internal channel. If the signal Bus_Width is selected for different bit widths, the signal should be synchronized simultaneously. Table 1-1 lists the preceding signals.

Table 1-1 lists the involved input signals

Name	I/O	Description
sys_clk	I	MAC layer clock
sclk_rst_n	I	sys_clk clock reset signal, low reset
pclk	I	Internal data channel parallel clock
tx_DataValid	I	The Mac layer tells Phy that data transfer is valid and ignores data for a period when it is low
txstartBlock	I	Block start flag signal (for PCIe3.0/4.0)
BusWidth[1:0]	I	MAC layer data bit width is selected 00 : 32 01 : 16 10 : 8 11 : reserved
ss_mode_sync	O	Output data valid
data_2ififo	O	Output synchronous parallel data
TxstartBlock_ mac	O	Output the block start signal after the clock domain transition
Tx_DataValid _mac	O	Output data valid signal after clock domain conversion

4. SIMULATION ANALYSIS

Under the Gen3/Gen4 protocol, the input data with different bit widths and rates are synchronized. Figure 1-2 shows that when the data bit width selection signal BUS_WIDTH is 00, the bit width in the sys_clk clock domain is the same as the set bit width of the internal channel, and the synchronous beat output is performed.

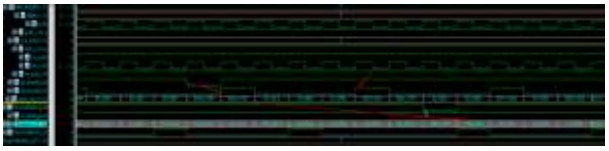

Figure 1-2 32-bit to 32-bit conversion

Figure 1-3 shows the data bit width conversion when the data bit width selection signal BUS_WIDTH is 01. At this time, it is the conversion from 16-bit to 32-bit width. At this time, the data of every two beats are combined into 32-bit data for output.

Figure 1-3 16-to 32-bit wide conversion

Figure 1-4 shows the data bit width conversion when the data bit width selection signal BUS_WIDTH is 10. At this time, the bit width of data is converted from 8 bits to 32 bits, and the data obtained every 4 beats are combined into 32-bit data for output.

Figure 1-4 8 to 32 bit width selection

5. CONCLUSION

By adjusting the bit width between data conversion modules, it can be obtained that under different PCIE versions, the running speed and bit width selection of PCIE can be judged according to the bit width selection signal. In order to facilitate the subsequent adjustment of PCIE bit width, we can increase its bit width selection. When the data bit width is 32 bits, its clock frequency is 500MHz, and the internal channel of its bit width selection is expanded to 64 bits. At this time, the clock frequency required by PCIE will not be 500MHz but 250MHz. With the design of the module bit width above, it can be explained that the desired data channel bit width can be achieved by adjusting the data bit width.

6. ACKNOWLEDGMENTS

Thank you to the teachers and classmates who helped me with this article. Thank you. Thank you for your review of the revised article.

7. REFERENCES

[1] Patterson David A.Computer organization and design : the hardware softw are interface[M].China Machine Press,2013.

[2] Lijun,WangWei.The 12th IEEE International Conference on Communication Technology[c].Nanjing: IEEE, 2010.

[3] Chen G , Shi J . An Embedded System Processor Module with PCI Busand Universal Communication Interface Based on PowerPC[J]. Iop Conference, 2019, 234.

[4] He Jia. Research on Engineering Realization of 133Mhz PCI-X Bus [J]. Journal of Public Security Marine Police College, 2013,12(02): 14-16

[5] Wu Guilin, Huang Lu. Design of PCS layer elastic buffer based on PCIe2.0 protocol [J]. Microelectronics and Computer, 2016,33(09):51-54+59.

[6] Song Pengcheng, Zhang Chun. FPGA implementation of SSD hard disk with PCIE3.0 interface [J]. Microelectronics and Computer, 2,017,34 (12): 63-66+73.

[7] Wang Qi. Introduction to PCI Express architecture [M]. Beijing: Machinery Industry Press, 2010.

[8] Wang Keyang. Research on Key Technologies of Data Receiving Based on PCIE4.0 Physical MAC [D]. Xi 'an University of Electronic Technology, 2021.

International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 03-08, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1002

Protocol Build by the Chaotic Map and Magic Square for Exchange Key Share

Dr. Abdul-Wahab Sami Ibrahim
University Mustansiriyah
College of Education, Department of Computer Science
Baghdad, Iraq

Majed Ismael Sameer
University Kufa
College of Computing and Mathematics
Department of Computer Science
Baghdad, Iraq

Abstract: In order to reach the level of security between the two parties or a group of parties in the communication channel, the inputs of the protocol algorithm must be characterized by the sensitivity of the initial parameters and conditions involved in the chaotic functions with great ability to change in any very slight manipulation of the inputs by the attacker or intruder because there will be Much of the fundamental change in the values of the shared keys of the two parties or participants in the system, as well as the prime numbers and primitive roots, is hidden rather than public. Use the magic square system algorithm to find the magic constant from the values of the Defy protocol algorithm with the chaotic values of three dimensions, and this magic constant will give us the long values of the shared keys between the parties participating in the group or the server used to distribute the shared keys to the parties, ensuring that this protocol is not attacked by a third party trying to enter the communication channel. The performance of the algorithm was analyzed by conducting and measuring the efficiency of protocol implementation, analyzing key length and sensitivity, and finding the speed of algorithm performance within the acceptable range of the number of participants in the system. A protocol algorithm in Matlab R2013b was used to implement the algorithm and perform the analyses.
Keywords: Diffie-Hellman; communication channel;magic square; chaotic map; share key .

1. INTRODUCTION

In this 1976 paper, scientists Martin Hellman and Whitfied Diffies presented the concept of asymmetric cryptography at the National Computer Conference [1, 2], before publishing it a few months later in "New Direction in Cryptography."

These shared keys can be used in a symmetric encryption algorithm, the first of its kind in terms of exchanging common keys between the two parties.

Develop and generate the first key agreement protocol algorithm, and then register it. However, their protocol failed to provide security and mutual authentication in the channel between communication parties; therefore, it was vulnerable to intermediary hacker attacks. Since then, several major protocols have been designed to prevent man-in-the-middle and related attacks [3].Kocarev and Tasev [4] proposed a public-key encryption scheme relay on chaotic maps. Bergamo et al. [5] indicated that the algorithm of the protocol presented by Kocarev-Tasev is insecure for the communication channel because, due to the redundancy of the cosine function, the adversary is able to recover the plaintext from a given ciphertext without the need for any secret key. Xiao et al. [6] designed a new key agreement protocol algorithm. Han introduced in 2008 [7] two attacks that enable a malicious adversary to prevent the user and the server from generating a shared key. Furthermore, Xiang et al. [8] It was pointed out by Xiao et al. The protocol is vulnerable to both the stolen validator attack and the offline password guessing attack. Later, Han and Zhang [9] introduced an improved protocol that works with or without clock synchronization.

In 2010, Wang and Zhao [10] proposed a modified chaos-based important protocol algorithm. Yoon and Jeon [11] have shown that this Wang-Zhao protocol algorithm requires timestamp information and is vulnerable to illegal message modification attacks. In addition, it contains redundant encryption and decryption processes to create a secure key agreement protocol.

As the idea of the appearance of the magic square is very old, dating back to BC. times, it was found in old books, such as one of the books of one of the most famous alchemists, Jabir bin Hayyan. [12]. Magic arenas also entered several different fields, such as magic, astronomy, and many other fields [13].

Mathematicians and cryptologists are other people who have used and introduced magic squares.

in the field of coding [14]. Magic squares, such as chess as the movement of the clicker in the game, sudoku, and others, are the most prominent examples of artificial intelligence in game design [13]. The following is a collection of previous work related to and based on the idea of the current paper cipher or magic square:

In 2009, Ganapathy and others developed an encryption algorithm that produces a different ciphertext using magic square as an alternative approach to dealing with stub-based ASCii code. The magic square number and the starting number are set so that the resulting result cannot be traced easily, which gives strict security measures [15]. In 2015, Duan et al. He developed an encoding algorithm based on the idea of using a strange magic square. Two specific magic squares and the complexity and speed of the proposed work were calculated [16]. In 2017, Omar proposed an encoding algorithm to get rid of the redundancy problem in ASCii. Using the command 32 magic square, he was able to easily track the command down and solve a problem, give more security, and provide a high level of security [17].

These characteristics are very important, as in this research they represent the symmetric inputs for each party for the purpose of finding the share key between them, depending on the development of an algorithm called Diffie-Hellman. This paper is structured as follows: Section 2 gives a description of the problem of research, and Section 3 gives a description of

the Henon chaotic map. In Section 4, we introduce a novel, secure key agreement protocol, analyze the efficiency of the proposed protocol, and analyze the key space. Finally, we conclude in Section 5..

2. RESEARCH PROBLEM

The problem of generating share keys between the two parties using the Diffie-Hellman algorithm is not solved in large numbers due to the time delay in implementing the protocol with a large number of iterations, which leads to a decrease in the efficiency of the implementation of the algorithm. The research problem was solved by making the protocol algorithm strong, solid, and robust against fraudulent party attacks. This is done by using chaotic functions that are related to certain properties, such as the sensitivity of parameters and initial conditions.

The research problem is solved by making the protocol algorithm robust and robust against fraudulent party attacks, and this is done by using messy functions associated with certain properties such as sensitivity parameters and initial conditions. And the results of that algorithm are from research [18]. It led to the generation of the magic constant of the magic square, and through this constant, it led to the generation of keys shared between the two parties or between the parties with a long size for the shared keys, which makes the protocol algorithm robust, robust, and robust against fraudulent party attacks

3. AN OVERVIEW ON HENON CHAOTIC MAP SYSTEM

In this section, an overview of the Henon chaotic map system is given as an important one of the 3-D chaotic map systems that are used in this work. chaotic map system is described by formula 1, which illustrates a set of the three functions of the Henon chaotic map system [19, 20,21].

x(i+1)=a-(y(i)^2)-b*(z(i)) |
y(i+1)=x(i) |…….(1)
z(i+1)=y(i) |

when initial values 1.54<|a |<2, 0<|b |<1. and -0.9<=(x or y or z)<=1

x(1)=1; y(1)=0;z(1)=0; %% Initial conditions The initial value are x=1, y=0.1, z=0,

N=5000; %% let N is the number of iterates example

a=1.6;b=0.2; %% Sets the parameters example

It has a chaotic attractor, as shown Fig..(1)

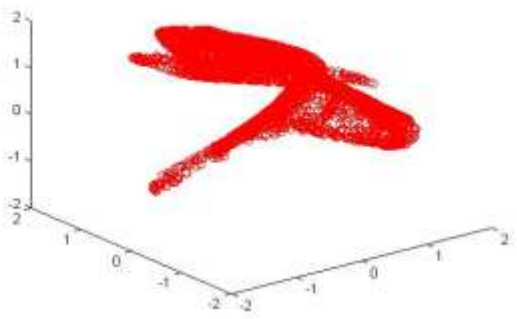

Fig.(1) three dimension henon map

3.1 Theoretical Background of the Magic Square

A magic square is a matrix with n rows and n columns. Always,lues are integers distribute so that the sum of each column, row, secondary, or main is the diagonal. Always the sum is the same number. The magic square with related classes of integer arrays was profound. A lesson in literature [22]. A magic square is a square matrix of n*n dimensions in which the sum of the digits of any row is equal to the sum of the digits of each column and the sum of the digits of each diagonal. The formula uses n (n^2 + 1)/2 to calculate the magic sum. In general, magic squares remain magical if the same positive integer is added to each number in the square or to each number in the parent square multiplied by the same number. Calculating magic squares becomes easy after knowing its algorithms, and it can be programmed in any programming language. See Figure 2 [23] of this figure; the total numbers in any row, column, or diagonal line are 34.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

34 =sum any direction

Figure2: A basic 4x4 magic square.

4. DESIGN PROTOCOL BASED ON HENON CHAOTIC MAP AND DIFFIE-HELLMAN AND MAGIC SQUARE ALGORITHM

Discusses the design of the proposed algorithm for the shared key exchange protocol between the parties or parties using chaotic functions of three dimensions with the magic square in order to generate the magic constant, from which the shared keys are generated, and all this work is done in order to create a secure channel in order to exchange information in a documented and secure way against hackers and attackers of the protocol shown in figure (3).

All symbols used in the Shared Key Finding Algorithm protocol are described in Table 1. Assume Alice and Bob are two participants in a key agreement process. The algorithm consists of the following parts:

STEP 1 :Inlet two parameter a , b and three Initial conditions Xo ,Yo, Zo to the Henon chaotic map system .

STEP 2: Extract the values of the chaotic functions Xi, Yi, and Zi, and then perform any algebraic mathematical operation such as multiplication or an operation between multiplication between them to output Henon's maps.

STEP 3:Extract primary Pi and Primitive root Qi from step 2.

STEP 4:Alice compute Ya then send to Bob.

STEP 5:Bob compute Yb then send to Alice.

STEP 6 : Find the shared key as an average of the sum of the shared keys generated by the algorithm.

STEP 7: Find the magic constant of step 6, and then find the shared key by generating the magic square of the group..

International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 03-08, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1002

Table 1: Notations used in Henon's maps protocol

Symbol	Definition
A,B	Identifiers of Alice and Bob, respectively
Xa ,Xb	Private key for A and B
P and Q	P=Primary number hidden Q=Primitive root number hidden
xxx	Magic Constant
Ya=(Q^Xa) mod P	Send to B
Yb==(Q^Xb) mod P	Send to A
K=(Q^(Xa*Xb))mo d P K=Ha=Hb	Finally established session key between Alice and Bob

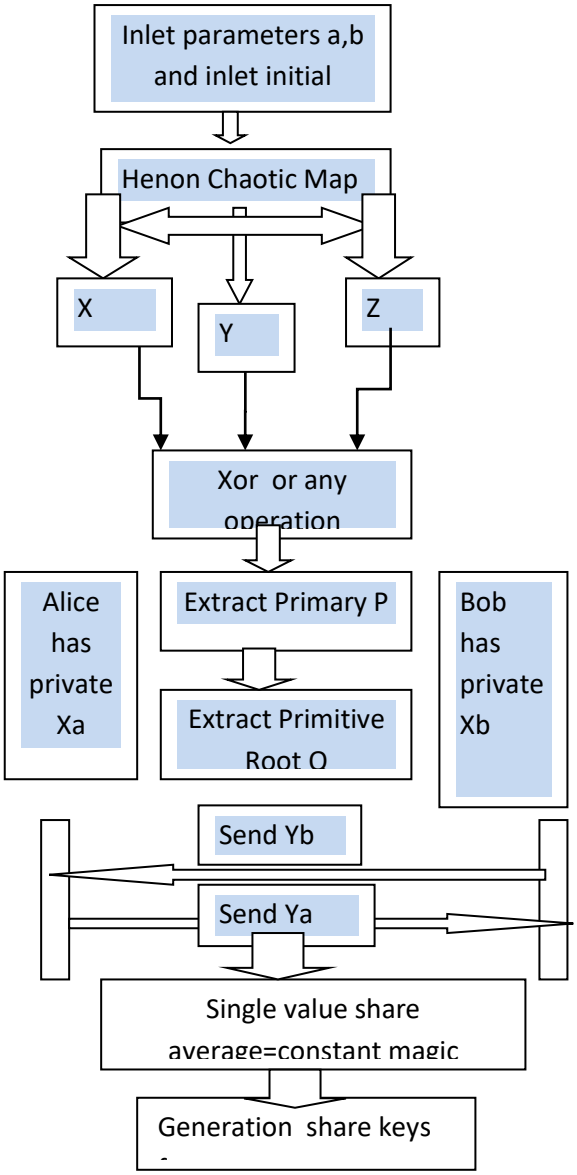

Fig. (3) General diagram of the protocol relay on chaotic and Diffie-Hellman and magic square

And depending on the algorithms from the references [18,24,25]to find the prime numbers and roots of the chaotic values of three dimensions, the prime numbers and the primitive roots are hidden and not public. It is visible only in the Matlab code because it will be among the software accounts in the Matlab code, the sender code, and the recipient code [18, 26].

It is possible to increase the number of participants in the group by increasing the number of shared keys that they exchange among themselves, and this work is inferred by increasing the length of the magic constant generated by the proposed protocol algorithm. Similarly, the number of participants can be increased depending on the size of the magic square matrix. The larger the size of the matrix used by the algorithm, the greater the number of participants, and the length of the key depends on the magic constant generated from the values of the protocol algorithm for chaotic states with

the Diffie-Hellman algorithm. Table 2 also shows the magic square algorithm.

Table (2) The function algorithm Magic Square used to find share keys

```
Algorithm function algorithm  of magic square
Process:
Input:
Share key average=magic constant
Output:
Return share keys for group
initial
xx= Share key average;
% must xx>65 if 5*5
n = 5;
xxx=xx*10;
% Create an empty matrix for the magic cube
A = zeros(n);

% Calculate the values for the elements of the magic
cube
A=magic(n);
sm = sum(diag(A));
% Display the resulting magic cube
disp(A);
B=(xxx-sm)/n;
AA=A+B;
disp('sHARE KEY BETWEEN GROUP');
disp(AA)
End.
```

5. ANALYZE AND EFFICIENCY OF THE PROPOSED PROTOCOL

In this paper, a practical program of a proposed algorithm and a practical program of all experimental and security analysis tests are designed using by using MATLAB language release R2012a for the 64-bit Windows 7 Home Premium operating system. The computer used to perform these tests is a Dell laptop with Intel (R) Core™ i3-3217u CPU@ 1.8GHz and 6 GB installed memory.

We have two parameter a=1.4 b=0.3
and three initial condition Xo=0.1 ,Yo=0.1 and Zo=0.3
Number of Iteration =50
Alice has private key Xa=3
Bob has private key Xb=7
Alice and Bob are Compute Pi and Qi
Pi=primary number =199 5 7 79 191 127 173 131 47
Qi=primitive root =197 3 5 77 189 118 171 128 45
Alice compute Ya then send to Bob
Ya=191 2 6 71 183 33 165 104 39
Bob compute Yb then send to Alice
Yb=71 2 5 30 63 105 45 40 13
Alice compute Share key
K= 109 3 6 61 28 20 127 72 35

Bob compute Share key
K=109 3 6 61 28 20 127 72 35

Then convert the set of share keys to single value

In the event that it is desired to subscribe to the shared key between two parties only and there are no participants in the group, an arithmetic operation can be carried out, such as extracting the average for that group, as shown in the table (3).

Table (3) Update share key only by average operation set

Prime numbers	199 5 7 79 191 127 173 131 47
Primitive roots	191 2 6 71 183 33 165 104 39
Ya	191 2 6 71 183 33 165 104 39
Yb	71 2 5 30 63 105 45 40 13
Share key before update	109 3 6 61 28 20 127 72 35
Share key update	Average of the Share key before update 51 xxx=Magic constant=55 after approximation Between 50,55 But I Choose the highest number=55

The magic square algorithm, which was based on the results of the chaotic functions protocol, was implemented using the Diffie-Hellman algorithm, and the results are shown in tables (4), (5), and (6).

Table (4) Results magic square which act as shared keys when use magic constant generation*10

114	121	98	105	112
120	102	104	111	113
101	103	110	117	119
107	109	116	118	100
108	115	122	99	106

Table (5) Results magic square which act as shared keys when use magic constant generation *100

1104	**1111**	1088	1095	1102
1110	**1092**	1094	1101	1103
1091	1093	1100	1107	1109
1097	1099	1106	1108	1090
1098	1105	1112	1089	1096

Table (6) Results magic square which act as shared keys when use magic constant generation *1000

11004	11011	10988	10995	11002
11010	10992	10994	11001	11003
10991	10993	11000	11007	11009
10997	10999	11006	11008	10990
10998	11005	11012	10989	10996

6. Analysis of the key space

In the proposed algorithm, Henon's chaotic function maps are generated, and each requires a control parameter value and a sequential initial condition value for the chaotic map. where they are used as input for algorithm protocol keys, if the underlying control variables and values are precisely in 10^14.

$$key(10)^{8}x(10)^{8}x(10)^{8}x(10)^{8}x(10)^{8}=(10)^{40}$$

that length $(10)^{40}$ very good for resistant brute attack.

7. CONCLUSIONS

Diffie-Hellman algorithm protocol development using chaotic functions optimized Henon-Map system for three dimensions with magic square was introduced in this algorithm with control of parameters and initial conditions. You get the results of this protocol algorithm to give different results while changing from very slight inputs to inputs. From implementing and analyzing the algorithm as presented, the following conclusions are obtained:

1. The prime numbers and primitive roots are hidden and not public. It is visible only in the Matlab code because it will be among the software accounts in the Matlab code, the sender code, and the recipient code.

2. It is possible to increase the number of participants in the group by increasing the number of shared keys that they exchange among themselves, and this work is inferred by increasing the length of the magic constant generated by the proposed protocol algorithm.

3. Any change in the value of the corresponding input values between the two parties will be due to these keys, which act as sensitive inputs to those changes in the event of manipulation or attack, such as changing any key of the values entered into the algorithm from the control parameters or initial conditions, and will be very sensitive because the values of the magic constant will change dramatically. It is very large and will return the results of the shared keys other than the previous original results between the two parties when manipulating any number of required bits, and the algorithm will be efficient and effective for all brute force attacks. Because changing the previous original equation on which the protocol algorithm depends, which is the important gem of the protocol, and relying on the same previous inputs for the control parameters, initial conditions, and iteration value.

8. REFERENCES

[1] W. Diffie and M.E. Hellman, Multiuser cryptographic technics, Proceedings of AFIPS National Computer Conference, 109-112, 1976

[2] W. Diffie and M.E. Hellman, New directions in cryptography, IEEE transactions on information theory, 22(1976), 644-654

[3] Nahid Yahyapoor, Hamed Yaghoobian, Manijeh Keshtgarib "An efficient and secure two-party key agreement protocol based on chaotic maps", Electrical Engineering, Khavaran Institute of Higher Education, Mashhad, Iran Computer Science, University of Georgia, Athens, GA 30602, 2018,USA

[4] L. Kocarev, Z. Tasev, Public-key encryption based on chebyshev maps, in: Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on, Vol. 3, IEEE, 2003, pp. III–III.

[5] P. Bergamo, P. D'Arco, A. De Santis, L. Kocarev, Security of public-key cryptosystems based on chebyshev polynomials, IEEE Transactions on Circuits and Systems I: Regular Papers 52 (7) (2005) 1382–1393.

[6] D. Xiao, X. Liao, S. Deng, A novel key agreement protocol based on chaotic maps, Information Sciences 177 (4) (2007) 1136–1142.

[7] S. Han, Security of a key agreement protocol based on chaotic maps, Chaos, Solitons & Fractals 38 (3) (2008) 764–768.

[8] T. Xiang, K.-W. Wong, X. Liao, On the security of a novel key agreement protocol based on chaotic maps, Chaos, Solitons & Fractals 40 (2) (2009) 672–675.

[9] S. Han, E. Chang, Chaotic map based key agreement with/out clock synchronization, Chaos, Solitons & Fractals 39 (3) (2009) 1283–1289.

[10] X. Wang, J. Zhao, An improved key agreement protocol based on chaos, Communications in Nonlinear Science and Numerical Simulation 15 (12) (2010) 4052–4057.

[11] E.-J. Yoon, I.-S. Jeon, An efficient and secure diffie–hellman key agreement protocol based on chebyshev chaotic map, Communications in Nonlinear Science and Numerical Simulation 16 (6) (2011) 2383–2389.

[12] S. Cichacz and T. Hincbc , " A magic rectangle set on Abelian groups and its application" , Discrete Applied Mathematics, Volume 288, Pages 201-210, 2021.

[13] A. Dharini, R. M. Devi, and I. Chandrasekar, “Data Security for Cloud Computing Using RSA with Magic Square Algorithm”, International Journal of Innovation and Scientific Research Vol. 11 No. 2 Nov. 2014, pp. 439-444 2014.

[14] Z. Duan, J. Liu, J. Li and C. Tian , " Improved even order magic square construction algorithms and their applications in multi-user shared electronic accounts" , Theoretical Computer Science – Elsevier , 2015. Carella, N. A. "Least Prime Primitive Roots". International Journal of Mathematics and Computer Science. 10 (2): 185–194,2015

[15] O. A. Dawood , A. S. Rahma and A. J. Abdul Hossen," Generalized Method for Constructing Magic Cube by Folded Magic Squares ", I.J. Intelligent Systems and Applications, 2016.

[16] D. A. Jabbar and A. S. Rahma ," Proposed Cryptography Protocol based on Magic Square, Linear Algebra System and Finite Field ", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, No. 10 , 2018.

[17] D. A. Jabbar and A. S. Rahma , " Development cryptography protocol based on Magic Square and Linear Algebra System" , Vol.11 No.1 2019

[18] Dr. Abdul-Wahab Sami Ibrahim & Majed Ismael Sameer," Protocol Build by Chaotic Map for Exchange Key Share ”, IJCSIS ,ISSN 1947 5500,July 2022 Volume 20 No. 7,

[19] Professor Ying Yang Professor Yong Li Dr. Jorge A. Ruiz-Vanoy

[20] Alia Karim Abdul Hassan," Proposed Hyper chaotic System for Image Encryption"(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016.

[21] Pianhui Wu , Weihua Zhao b, Zhengxu Zhao c," Hyper chaotic Based-on Henon Map",Journal of Information & Computational Science 11:12 (2014)

[22] Abramowitz, M. and Stegun, I. A. (Eds.). "Primitive Roots." §24.3.4 in Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables, 9th printing. New York: Dover, p. 827, 1972

[23] B. L. Kaul and R. Singh, Generalization of magic square (numerical logic) 3 × 3 and its multiples (3 × 3) × (3 × 3), Int. J. Intell. Syst. Appl. 1 (2013), 90–97.

[24] Rageed Hussein AL-Hashemy,Sadiq A. Mehdi,"A new Algorithm Based on Magic Square and a Novel Chaotic System for Image Encryption", ISSN 0334-1860,journal of Intelligent Systems , February 2019

[25] Carella, N. A. "Least Prime Primitive Roots". International Journal of Mathematics and Computer Science. 10 (2): 185–194,2015

[26] Vinogradov, I.M. "§ VI Primitive roots and indices". Elements of Number Theory. Mineola, NY: Dover Publications. pp. 105–121. ISBN 978-0-486-49530-9,2003

International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 09-16, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1003

Protocol Built by Chaotic Map and Elliptic Curve Cryptography for Key Exchange

Dr. Abdul-Wahab Sami Ibrahim
University Mustansiriyah
College of Education, Department of Computer Science
Baghdad, Iraq

Majed Ismael Sameer
University Kufa
College of Computing and Mathematics
Department of Computer Science
Baghdad, Iraq

Abstract: The elliptical curve system has received great interest in the science of security systems, and this has a great number of advantages. When linked with chaotic systems, it gave a broad comprehensiveness in the science of finding common keys between the two parties or in a system as a server that distributes the common keys among the participants in the distress.
The proposed algorithm reduces processor load, reduces power consumption, increases processing speed, enhances storage efficiency , requires smaller certificates, and is good at saving bandwidth. Where ECC gives high-level arithmetic operations ECC is an algebraic structure in wide areas for a large number of points and any point in the Cartesian coordinates, as well as for a number of prime numbers generated from the chaotic three-dimensional system using the multiplication and addition algorithm of the elliptical curved system. This paper suggested a new event in the implementation method: the inputs to the elements of the controlling parameters and the initial conditions of the symmetric chaotic functions produce an ECC by a secret shared key between two parties or a number of parties participating in the group, and all these points of the share keys lie on the points of the curve. and this key technology is available for authentication, confidentiality, and non-repudiation.
Keywords: Diffie-Hellman; communication channe l;ECC; chaotic map; share key .

1. INTRODUCTION

The main benefit of using ECC technology is that it provides the same level of protection with a smaller switch length compared to RSA. Thus, it will reduce the execution time of the algorithm processing as well as reduce the processing cost [1, 2]. Elliptic Curve Cryptography (ECC) is a popular algorithm that provides a higher level of security.

Smaller key sizes with lower resource consumption, which makes it an ideal choice for resource-constrained devices. The unpredictability introduced by the chaotic maps in the proposed algorithm is in addition to the fact that the algorithms make the model easy to implement, fast, and powerful against the attacker. The more coordinated the chaotic functions, the higher the level of safety and the better the quality. Chen et al. [3] suggest a symmetric image encoding algorithm with a 3D cat map and logistics map for mixing image data with an extra layer of confusion between them, resulting in an image with normal encoding after every two rounds of mixing. The cryptography also uses Chen's chaotic key generation system. Parrick and others [4] used as a result of two logistics maps to choose one of the eight randomly designed modes to encode every pixel in the image. Designed by Liu and Wang [5] as a one-time master-stream encoding for color image encoding on a piecewise linear chaos map (PWLCM) to calculate mainstream color image coding. The main stream is based on another sequence obtained from the Chebyshev map.

The authors, Moncef Amara and Amar Siad [6], discussed elliptical curve coding (ECC) and its performance in In terms of speed of implementation and security compared to traditional encryption algorithms like RSA, Points are generated by specifying the prime number P. The authors Ali Soleyamani, Md. Jan Nordin, and Zulkarnain Md. Ali discussed [7]. ECC The map table method is used to encode the image. ECC points are generated by choosing the largest Prime No. A mapping table is generated using points created by an elliptical curve. The points generated are set image pixels to perform encoding.

Requires good ECC technology awareness and a mathematical background compared to elliptical curves. elliptic curves In addition, elliptic curves are not ellipses [8, 9], and after all, they are It is defined as an ellipse because EC is a derivative of cubic equations (1). Sangook Moon: To perform numerical operations, develop a more efficient and novel approach to scalar point multiplication from the method of double multiplication and existing addition, then apply redundant recoding that originates from the root. 4 Booth's algorithm [10] L. Young. sign to Aydos et al protocol is not safe for humans in midfield attack by any attacker [11].

Koblitz and Miller were the first to use the elliptic curve cryptography technique [12]. Ravi Kodali and N. Sarma use Elliptic Curve Cryptography symmetric encryption with the Koblitz's encoding to encode or map the data into points locating on the Elliptic Curve, and it is one of the main basics of the Elliptic Curve Cryptography [13]. J. Nafeesa Begum and others Improved multi-level defensive messaging system ECC access control defense message system Redirects a message to parties or recipients based on message criteria for quick action [14]. Several algorithms have been developed to solve the problem. However, the effectiveness of any algorithm is determined by the type of curve and the properties of k, where k is a random number [15]. Arezou and others [16] have made effective use of the elliptic curve cipher in building a three-factor authentication.

system for satellite communications when it comes to implementing ECC cloud computing security.

Kumar & Grover's and other [17] focused on applying the ECC algorithm for encryption and decryption processes to improve cloud computing security and protect privacy. Anand and Perumal [18] introduced a method to prevent any user from gaining unwanted access to confidential data stored in the cloud. (ECC) is known to be superior to public-key cryptography approaches in wireless devices. Helps reduce

device processing time. Wang and others [19] presented a work based on the concept of ECC and introduced a new way to secure ECC output. Shenet and others [20] The Java language facilitated the usage of ECC by analyzing its capabilities and dealing with digital signatures, key exchange, and key generation.

2. RESEARCH PROBLEM

The problem of generating share keys between the two parties using the Diffie-Hellman algorithm is not solved in large numbers due to the time delay in implementing the protocol with a large number of iterations, which leads to a decrease in the efficiency of the implementation of the algorithm. The research problem was solved by making the protocol algorithm strong, solid, and robust against fraudulent party attacks. This is done by using chaotic functions that are related to certain properties, such as the sensitivity of parameters and initial conditions[21,22,23].

The research problem is solved by making the protocol algorithm robust against fraudulent party attacks, and this is done by using chaotic functions associated with certain properties such as sensitivity parameters and initial conditions. And the results of that algorithm are from research [24,25,26]. It led to the generation of common keys between the two parties or between the two parties for the common keys, and these shared keys are in the form of points with arranged pairs and are located exclusively on the points of the curve, which makes the protocol algorithm strong and strong against fraudulent attacks.

3. ELLIPTIC CURVES OVER REAL NUMBERS

Elliptic curves are not elliptical[12] .It is so named because it is described by cubic equations, similar to those used to calculate the circumference of an ellipse. In general, cubic equations for elliptical curves take the following form, known as the Weierstrass equation (1):

y^2+axy+by=x^3+cx^2+dx+e……(1)

where a,b,c,d and e are real numbers and take on values in the four real numbers.For our purpose, it is sufficient to limit ourselves to the form of equations (2).

y^2=x^3+$a\ x$ +b……..(2)

Such equations are said to be cubic, or of three degrees, because the highest exponent they contain is a three [21, 22]. The elliptic curve (E) is a non-singular algebraic plane curve defined over a finite field Fp, where x, y, a, b Fp. The clarity of this equation (2) is shown in figure 1

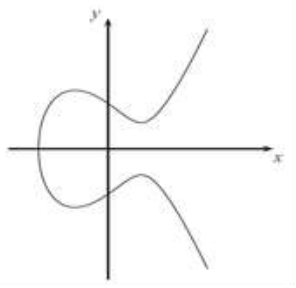

FIGURE 1. An Elliptic Curve E defined over a finite field Fp

3.1. Addition And Multiplication Of Elliptic Points

Assuming P1 ,P2 and R be three points on ellipse curve[23].Let

The addition stage first method used is R=P1+P2=(xR,yR) is determined by the following rules(3) and (4).

m=(y2-y1)/(x2-x1) mod p if P1 not equal P2 or

m=(3x1^2+a)/(2y1) mod p if P1 equal P2

xR=(m^2−x1−x2) mod P ……(3)

yR =(m(x1−xR) – y1) mod P ……(4)

Where a,b are coefficients of equation (2) and x ,y are coordinates.

The Multiplication stage second is defined as repeated addition; for example,

4P1=P1+P1+P1+P1 .

For example, let P1=(3,10) and P2=(9,7) then

m=((7-10)/(9-3))mod 23=(-3/6)mod 23=(-1/2)mod 23=11

xR=(11^2-3-9)mod23=17

yR=(11(3-17)-10)mod 23=20

P1+P2=(17,20)

To find 2P1|

m=((3(3^2)+1)/2*10)mod 23=6

xR =(6^2-3-3)mod 23=7

yR =(6(3-7)-10)mod 23=12

And then 2P1=(7,12)

Note: To generate a curve with about 2^160 points, a prime with a length of about 160 bits is required.

4. AN OVERVIEW ON HENON CHAOTIC MAP SYSTEM

In this section, an overview on Henon chaotic map system as important one of the 3-D chaotic map systems, which is used in this work. Henon chaotic map system is described by formula 5 which illustrates a set of the three function of Henon chaotic map system[24,25,26].

x(i+1)=a-(y(i)^2)-b*(z(i)) |

y(i+1)=x(i) |……(5)

z(i+1)=y(i) |

when initial values 1.54<|a |<2, 0<|b |<1. and -0.9<=(x or y or z)<=1

x(1)=1; y(1)=0;z(1)=0; %% Initial conditions The initial value are x=1, y=0.1, z=0,

N=5000; %% let N is the number of iterates example

a=1.6;b=0.2; %% Sets the parameters example

it has a chaotic attractor as shown in Fig.(2).

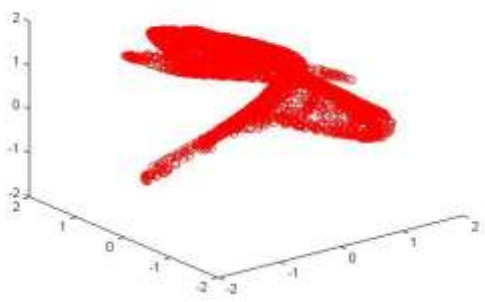

Fig.(2) Three Dimension Henon Map

International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 09-16, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1003

5. DESIGN PROTOCOL BASED ON HENON CHAOTIC MAP AND ECC

Square

Discusses the design of the proposed algorithm for the shared key exchange protocol between the parties or parties using chaotic functions of three dimensions in order to create a secure channel in order to exchange information in a reliable and secure manner against hackers and attackers of the protocol shown in the figure (3).

All the notations used in the Henon maps protocol are described in Table 1. Assume Alice and Bob are two participants in a key agreement process. The algorithm consists of the following parts:

STEP 1 :Inlet two parameter a , b and three Initial conditions Xo ,Yo, Zo to the Henon chaotic map system .

STEP 2: Operation between multiplication or any operation between them output henon maps.

STEP 3:Extract primary Pi from step 2.

STEP 4:Alice compute Ya .

In the form of ordered pairs calculated from the points through the proposed algorithm and its output, which is located within the points of the elliptic curve

then send to Bob.

STEP 5:Bob compute Yb.

In the form of ordered pairs calculated from the points through the proposed algorithm and its output, which is located within the points of the elliptic curve.

then send to Alice.

STEP 6 :Both Alice and Bob are compute K=share key.

In the form of ordered pairs calculated from the points through the proposed algorithm and its output, which is located within the points of the elliptic curve.

Table 1: Notations used in Henon's Maps Protocol

Symbol	Definition
A,B	Identifiers of Alice and Bob, respectively
Xa ,Xb	Private key for A and B
P	Primary number hidden
Ya= In the form of ordered pairs calculated from the points through the proposed algorithm and its output, which is located within the points of the elliptic curve	Send to B
Yb= In the form of ordered pairs calculated from the points through the proposed algorithm and its output, which is located within the points of the elliptic curve	Send to A
K= In the form of ordered pairs calculated from the points through the proposed algorithm and its output, which is located within the points of the elliptic curve	Finally established session key between Alice and Bob
K=Ha=Hb	note

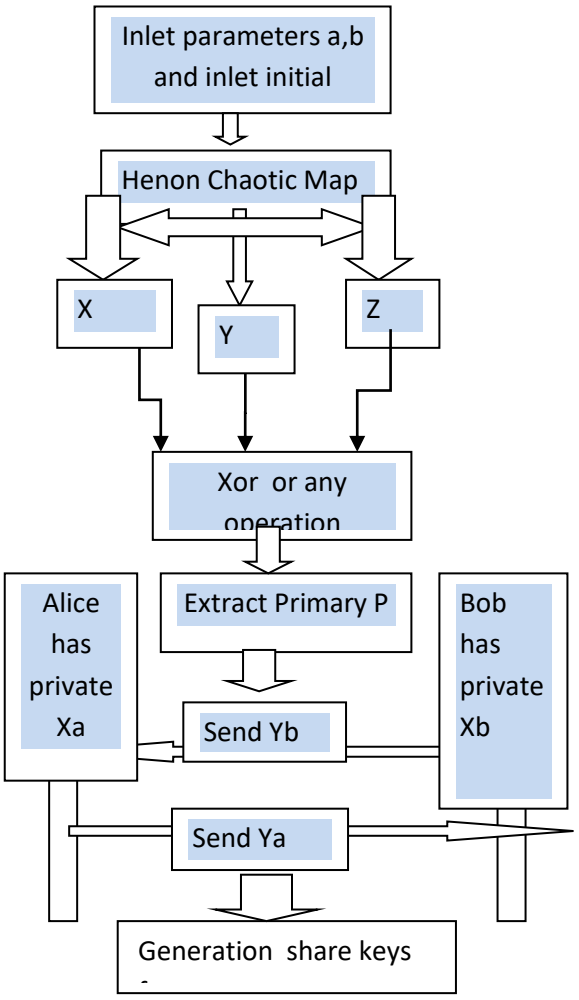

Fig. (3) General diagram of the protocol relay on chaotic and ECC

An important steps in design the proposed protocol :Extract primary Pi from step 2.

First : Let's give a more detailed definition of a prime number.

The algorithm that was used to design and extract the prime numbers is shown as in the table(2)

The algorithm that was used to design and extract the prime numbers is shown as in the table(2)

International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 09-16, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1003

Table (2 Prepare the primes numbers from chaotic sequences results

```
Algorithm Prepare the prime numbers  from step 2
Stage
Process:
Input:
P1: chaotic sequences results from step 2
N=number of iteration
Output:
Prepare the prime numbers  sequences
Initial:
m=0;
 Loop i ← 1 to N
  if(isprime(p1(i(((
      m=m+1
    hh(m)=p1(i(
  end if
End Loop i;
Loop i ←1 to m
   if hh(m)>=2
print ←prime number hh(m)
end if
End Loop m;
End.
```

Second : Alice will need the primes generated by the proposed algorithm, and then she will need the private key Xa to generate the public keys in the form of ordered pairs located within the points of the ellipse and send them to Bob. Likewise, Bob will also need the primes generated by the proposed algorithm, and he has the private key Xb to generate Public keys in the form of ordered pairs are located within the points of the ellipse and send to Alice.

Third: Here each party will generate the common key or a number of common keys and also be in the form of arranged pairs and located within the curve points of the ellipse, and these keys can be distributed to the rest of the participants in the exchange of information within the security communication channels.

6. ANALYZE AND EFFICIENCY OF THE PROPOSED PROTOCOL

In this paper , a practical programs of a proposed algorithm and a practical programs of all experimental and security analysis tests are designed by using MATLAB language release R2012a for 64bit Windows 7 Home Premium operating system. The computer used to perform these tests is a Dell Laptop with Intel (R) Core™ i3-3217u CPU@ 1.8GHz and 6 GB installed memory.

We have two parameter a=1.4 b=0.3

and three initial condition Xo=0.1 ,Yo=0.1 and Zo=0.3

Number of Iteration =50

Alice has private key Xa=3

Bob has private key Xb=9

Alice and Bob are Compute Pi as the hide from chaotic map three dimension

Pi=primary number =2441 281 293 1867 269 2113 139 331 1447 2063 307

Extract from each prime number a number of pairs that lie at the points of the curve of equation (1) for the following algorithm of generating a number of points for the arranged pairs that fall within the points of the ellipse in table(3).

Table(3) Algorithm of generate a number of points for the arranged pairs that fall within the points of the ellipse

```
Algorithm Prepare the generate a number of points for
the arranged pairs  that fall within the points of the
ellipse.
Process:
Input:
P: primary number
Output:
Prepare the generate a number of points GEN( a,b,p)
sequences
Initial:
i=1;
G=[];
for x=0:p
   for y=0:p
      if mod(y^2,p)==mod((x^3+a*x+b),p)  % This
equation must be satisfied by x and y for the given
value of a, b and p.
         G(i,:)=[x y];
         i=i+1;
      else
      end;end;end; End.
```

The results after applying the algorithm in the table (3) are shown:

GEN(a, b, p)

>> [G] =GEN(2,2, 2441)

At p=2441

G =

0	837
0	1604
1	759
1	1682
4	131
4	2310
5	523
5	1918
6	899
6	1542
11	415

And so continue from the result. But we choose one of those pairs that lie within the points of the curve of equation (2). And let the pair be in the fifth sequence, which is

4 131

At p= 281

>> [G] =GEN(2,2,281)

G =

0	132
0	149
1	75
1	206
2	24
2	257
3	63
3	218
5	74
5	207
7	42
7	239
8	116

International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 09-16, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1003

8 165
11 136

Table(4) Multiplication algorithm for the ellipse curve

```
Algorithm Prepare the generate a number of points for the arranged pairs that fall within the points of the ellipse.
Process:
Input:
P: primary number; a,b,p,n,x,y
Output:
Prepare the results of multiple private key with function GEN generate a number  pair sequences
Initial:
if n ==1
   resx = x;
   resy = y;
   return;
end
if n>=2
   [xsub,ysub]=NP(a,b,p,n-1,x,y);
   if xsub==Inf && ysub == Inf
      resx=Inf;
      resy=Inf;
   else
      [resx,resy]=Add(a,b,p,x,y,xsub,ysub);
   End;end;end;
End.
```

Table(5) The addition algorithm for the ellipse

```
Algorithm Prepare the generate a number of points for the arranged pairs that fall within the points of the ellipse.
Process:
Input:
P: primary number; a,b,p,n,x,y
Output:
Prepare the results of multiple private key with function GEN generate a number  pair sequences
Initial:
function [ resx,resy ] = Add( a,b,p,x1,y1,x2,y2 )
if x1==x2 && y1==y2
   k=modfrac(3*x1^2+a,2*y1,p);
   resx = mod(k^2-x1-x2,p);
   resy = mod(k*(x1-resx)-y1,p);
end
if x1==x2 && y1~=y2
   resx = inf;
   resy = inf;
end
if x1 ~= x2
   k=modfrac(y2-y1,x2-x1,p);
   resx = mod(k^2-x1-x2,p);
   resy = mod(k*(x1-resx)-y1,p);
end;End.
```

And so continue from the result. But we choose one of those pairs that lie within the points of the curve of equation (2) .And let the pair be in the fifth sequence, which is

2 24

The process will continue for the rest of the prime numbers generated by the chaotic three-dimensional calculation algorithm.

The next step is:

The multiplication algorithm for the ellipse curve is algorithm of NP .It is shown in Table No.(4)

Note that the private key for Alice =3. The result was the creation of a file for each party, as follows:

First:

Private key for Alice=3

And because the addition is multiplication, for example, P+P=2P because p first same as p another.

But 3P=P+P+P we need algorithm add curve ellibts because 3P=P+P+P=2P+P then 2P not similar to P.

Say to Q=2P then 3P=2P+P=Q+P

And as follows for the addition algorithm .It is shown in Table No.(5) for the ellipse.

When we use the addition and multiplication algorithm together, we will get the following results.

Note that the private key for Alice =3

Alice compute YA1 of the Elliptic curves then send to Bob

YA1=

****

470 485

11 136

254 233

241 1183

156 8

2064 140

53 106

295 291

961 551

932 471

158 58

And also ,Private key for Bob=9

Bob compute YB1 of the Elliptic curves then send to Alice

YB1=

288 579

224 118

166 263

1851 1044

251 66

878 1195

33 137

239 142

727 100

1768 1808

245 157

Alice compute Share key of the Elliptic curves

K=

1708 39

60 95

196 228

681 313

134 13

736 439

34 68

74 237

50 667

1245 1193

300 140

Bob compute Share key

K=

1708 39

60 95

196 228

681 313

134 13

736 439

34 68

74 237

50 667

1245 1193

300 140

When Alice receives the pop file, Alice will also use the multiplication and addition algorithm to find the common keys between Alice and Bob, and also does the same process for Bob's steps, and the results are as follows for the shared keys

The table of share keys obtained by Alice from the algorithm

1708 39

60 95

196 228

681 313

134 13

736 439

34 68

74 237

50 667

1245 1193

300 140

The table of share keys obtained by Bob from the algorithm

1708 39

60 95

196 228

681 313

134 13

736 439

34 68

74 237

50 667

1245 1193

300 140

And because the time taken to implement is of great importance to the protocol, it depends on the number of iterations that must be implemented for the chaotic Henon-maps three-dimensional functions. The higher the number of iterations, the longer the time for executing the protocol algorithm and the results shown as shown in the table (6), which shows the relationship between the time taken to implement the algorithm with the number of iterations to implement the protocol.

Table (6) Correlation time taken to implement the algorithm with the number of iterations

Number of iteration	taken to implement the algorithm	Number of participants in group
25	6.041915	6
50	8.808280	11
60	9.243908	12
70	13.124462	14
85	13.040652	14

7. Analysis of the key space

In the proposed algorithm, Henon's chaotic function maps are generated, and each requires a control parameters value and a sequential initial conditions value for the chaotic map. where they are used as input of algorithm protocol keys, if the

underlying control variables and values are precisely in 10^14,

the total space of the Key 10^5 x10^5 x10^5x10^5x10^5=10^25

that length 10^25 very good for resistant brute

8. CONCLUSIONS

The protocol for the ECC algorithm was developed using the chaotic functions of the three-dimensional Hennon-Map system, the symmetry of this algorithm was introduced with the control of parameters and conditions of the initials. You get the results of this protocol algorithm to give different results while changing from the very slight input, from the implementation and analysis of the algorithm as presented, the following conclusions are obtained:

1. Prime numbers are hidden and not public. It is only visible in matlab code because it will be among the software accounts in Matlab code, sender code, and recipient code.

2. It is possible to increase the number of participants in the group by increasing the number of common keys that they exchange among themselves, and this work is inferred by increasing the number of iterations that are made for the three-dimensional chaotic functions of Henon maps. Also, the results showed that there were a limited number of participants. The number can be increased by increasing the power of the computer specifications.

3. Any change in the value of the corresponding input values between the two parties will make these keys, which act as input sensitive, sensitive to those changes in case of manipulation or attack, such as changing any key of the values entered into the algorithm from the control parameters or initial conditions, and it will be very sensitive because it will display results. Shared keys other than the previous original results between the two parties when manipulating any number of required bits and the algorithm will be efficient and effective for all anti brute force attack programs.

It should include trust and security between the group participants so that keeping the corresponding entries is guaranteed by certain entities of the protocol algorithm distribution and not just known to some unspecified party .If only two parties share the common key and there are no participants in the set, an arithmetic operation can be performed, such as adding up the points for the shared keys that are within the points of the ellipse for that set.

9. REFERENCES

[1] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Trans. Inform. Theory, IT-22 :644-654, Nov 1976.

[2] A. M. Johnston, P. S. Gemmell, “Authenticated key exchange Provably Secure Against the Man-in-Middle Attack”, Journal of Cryptology, Springer , 2002, Vol. 15 Number 2 pp. 139-148.

[3] G. Chen, Y. Mao, and C. K. Chui, ‘‘A symmetric image encryption scheme based on 3D chaotic cat maps,’’ Chaos, Solitons Fractals, vol. 21, no. 3, pp. 749–761, Jul. 2004.

[4] N. K. Pareek, V. Patidar, and K. K. Sud, ‘‘Image encryption using chaotic logistic map,’’ Image Vis. Comput., vol. 24, no. 9, pp. 926–934, Sep. 2006.

[5] H. Liu and X. Wang, ‘‘Color image encryption based on one-time keys and robust chaotic maps,’’ Comput. Math. with Appl., vol. 59, no. 10, pp. 3320–3327, May 2010.

[6] Moncef Amara and Amar Siad, “Elliptic Curve Cryptography and its Applications”, IEEE 7th Int. Workshop on Systems, Signal Processing and their Applications, (2011), 247-250.

[7] Ali Soleyamani, Md Jan Nordin,Zulkarnain Md Ali, “A Novel Public Key Image Encryption based on Elliptic Curves over Prime Group Field”, Journal of image and Graphics, (2013), Vol. 1 No.1, 43-49.

[8] William Stallings, "Cryptography and Network Security Principles and Practice", Fifth Edition, 2011,300p.

[9] Darrel Hankerson, Alfred Menezes and Scott Vanstone, Guide to Elliptic Curve Cryptography", © SpringerVerlag New York, Inc. ,2004,14-30p

[10] Sangook Moon, "A Binary Redundant Scalar Point Multiplication in Secure Elliptic Curve Cryptosystems", International Journal of Network Security, Vol.3, No.2, 2006, PP.132-137.

[11] Liu Yongliang, Wen Gao, Hongxun Yao, and Xinghua Yu , "Elliptic Curve Cryptography Based Wireless Authentication Protocol", International Journal of Network Security, Vol.4, No.1, 2007, PP.99-106.

[12] V. Miller, “Uses of elliptic curves in cryptography”, in Proceedings of the Conference on the Theory and Application of Cryptographic Techniques (CRYPTO), 1985, pp. 417–426.

[13] Ravi Kishore Kodali and N.V.S Narasimha Sarma, "ECC Implementation using Koblitz’s Encoding", in Proceedings of the Conference on Communication Engineering and Network Technologies (CENT), Elsevier, 2012, pp. 411- 417.

[14] J. Nafeesa Begum, K. Kumar and Dr. V. Sumathy, "Multilevel Access Control in Defense Messaging System Using Elliptic Curve Cryptography", in Proceedings of the International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, 2010, pp. 1-9.

[15] Kumari, A., Jangirala, S., Abbasi, M. Y., Kumar, V., & Alam, M.,“ESEAP: ECC basedsecure and efficient mutual authentication protocol using smart card,”Journal of Information Security and Applications,51, 102443, 2020.

[16] Arezou Ostad-Sharif, Dariush Abbasinezhad-Mood, Morteza Nikooghadam, “Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications,”Computer Communications 147, 85–97, 2019.

[17] Kumar, D., & Grover, H. S.,“A secure authentication protocol for wearable devicesenvironment using ECC,”Journal of Information Security and Applications,47, 8-15, 2019.

[18] Anand, S., & Perumal, V.,“EECDH to prevent MITM attack in cloud computing,”Digital Communications andNetworks,5(4), 276-287, 2019.

[19] Wang H., He D., Ji Y., “Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography,”Future Generation Computer Systems, 2017.http://dx.doi.org/10.1016/j.future.2017.06.028.

[20] Shen, Y., Sun, Z., & Zhou, T.,“Survey on Asymmetric Cryptography Algorithms,”In2021 IEEE International Conference on Electronic Information Engineering

and ComputerScience (EIECS)(pp. 464-469), September, 2021.

[21] Rashmi K. Gawande, Pravin S. Kulkarni & Kamlesh A. Ganar,"Multi Level Image Encryption using Chaotic Mapping And Elliptic CurveCryptography",International Conference On Engineering Innovation and Technology, ISBN : 978-93-81693-77-3, Nagpur, pp. 69-70,1st July, 2012.

[22] PRIYANSI PARIDA , CHITTARANJAN PRADHAN , XIAO-ZHI GAO ,DIPTENDU SINHA ROY,"Image Encryption and Authentication With Elliptic Curve Cryptography and Multidimensional Chaotic Maps ",Received March 10, 2021, accepted March 31, 2021, date of publication April 9, 2021, date of current version June 1, pp.76191-76192,2021. Digital Object Identifier 10.1109/ACCESS.2021.3072075 .

[23] Revanna C R, Keshavamurthy C,"Hybrid Method of Document Image Encryption using ECC and Multiple Chaotic Maps ",International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4, pp.1615-1616,November 2019.

[24] Alia Karim Abdul Hassan," Proposed Hyper chaotic System for Image Encryption"(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, pp.37-38,2016.

[25] W. Strunk Jr., E.B. White, The Elements of Style, third ed., Macmillan, New York, 1979, 350 p.

[26] Dr. Abdul-Wahab Sami Ibrahim ,Majed Ismael Sameer, " Protocol Build by chaotic map for Exchange Key Share", IJCSIS July 2022 Volume 20 No. 7 , ISSN 1947 5500.

International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 17-20, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1004

Eye Pupil Controlled Wheelchair

Ranjeetsingh Suryawanshi
Department of Multidisciplinary Engineering, Vishwakarma Institute of Technology
Pune, Maharashtra, India

Shardul S. Bodhe
Department of Multidisciplinary Engineering, Vishwakarma Institute of Technology
Pune, Maharashtra, India

Digvijay S. Bhingare
Department of Multidisciplinary Engineering, Vishwakarma Institute of Technology
Pune, Maharashtra, India

Sarvesh V. Bongirwar
Department of Multidisciplinary Engineering, Vishwakarma Institute of Technology
Pune, Maharashtra, India

Girish Borse
Department of Multidisciplinary Engineering, Vishwakarma Institute of Technology
Pune, Maharashtra, India

Nandini Chavhan
Department of Multidisciplinary Engineering, Vishwakarma Institute of Technology
Pune, Maharashtra, India

Abstract: Elderly and disabled people find it very difficult to move freely to their desired areas at any opportune time in today's fast-paced environment. Thankfully, some people are physically fit and have good eyesight, which helps to assure their survival. This paper attempts to investigate the use of a design approach for a system that aids the disabled who are unable of operating a wheelchair in the conventional manner. This system uses information collected from the sensors and offers a system that will help replace traditional method. An intelligent vision system that analyses head movements, pupil position, the patient's angle of view, and other factors can be used to determine the necessary movements of the chair. In order to detect the pupil's position and control the wheelchair to travel in the desired direction, the suggested technology uses image processing algorithms. Project is built with the use of ultrasonic sensor to avoid the obstacles in the way.

1. INTRODUCTION

Everybody values freedom of movement highly. But it can occasionally be challenging for someone with a physical impairment. Partial or complete paralysis is possible.

Arms and legs are both affected by quadriplegia, which is a medical term for paralysis. The lain term for immobility is plegia. A spinal cord injury is the main reason for quadriplegia. The area of spinal cord that is hurt and how much damage is done determine the degree of impairment. Because the central nervous system, which carries messages throughout the body, is primarily made up of the brain and spinal cord, spinal cord injuries can be very devastating.
The human eye is additionally believed to be an intuitive means of deciphering human contact and communication that may be utilised to examine data about the surroundings and make suitable responses. Only 22% of the 132 million people who need wheelchairs actually have access to one. It should be highlighted that this is because many disorders significantly restrict a person's physiological capacity to produce regulated movement in any limb, including the head. Even the most sophisticated wheelchairs are inaccessible to them. It is vital to look at cutting edge eye tracking and recognition technologies that can enhance human-computer interaction and raise the living standards of these impaired people.

Many applications, including eye-tracking operated wheelchairs, mental health monitoring, driving tiredness warning systems, and other human-computer interaction systems, have gradually adopted eye tracking research. However, there are a number of limitations, including the need for a portable and unobtrusive system as well as consistent real-time performance, high precision, and constituent availability. Furthermore, it's critical to build a system with enhanced resistance to issues like fluctuating lighting conditions, genuine eye appearance, surrounding eye features, and eyeglass reflections. Eye-controlled wheelchair systems have been proposed in several similar publications; These, however, infrequently address the user's comfort and safety as well as the system's unique algorithms, physical issues not related to the system, and performance constraints of the system's software.

2. LITERATURE REVIEW

In recent years, the development of eye-controlled wheelchairs has been a growing research area. Eye-controlled wheelchairs allow people with physical disabilities to control the wheelchair with only their eyes [1]. This technology uses eye-tracking software and hardware to enable a person to control the wheelchair with eye movement. In this review, the current state of eye-controlled wheelchairs is discussed, along with the advantages and disadvantages of this technology. Eye-controlled wheelchairs use eye-tracking technology to allow people with physical handicaps to maneuver the wheelchair with their eyes [6]. The system works by tracking the direction of the user’s gaze and then sending the appropriate commands to the wheelchair’s motors. This

technology has been used to create a variety of wheelchair designs, from traditional manual wheelchairs to powered wheelchairs. The technology has also been used to create hybrid designs, combining elements of both manual and powered wheelchairs [2]. Eye-controlled wheelchairs offer a number of advantages. They enable people with physical disabilities to maintain their independence and autonomy. They are also easy to use and don't require the user to learn a complex set of commands [3]. Additionally, they allow the user to control the wheelchair in any direction, providing more flexibility and freedom than a manual. In their work, they have used Arduino UNO as microcontroller and raspberry pi and open-cv for image processing [4]. The Arduino controller chip for the core microcontroller system is connected to the camera and voice assistant modules. When user move his eyeballs left side then the wheelchair move left side, when ball right side then the wheelchair move right side and eyeball straight the move forward in all other case wheelchair will stop. From this research paper we get how the change the direction of wheelchair by using eyeballs. This article presents a wheelchair system using an eye movement that help differently abled people to move freely around [2]. The model uses LabVIEW for eye tracking and direction determination of glaze. This signal is then used to drive the motor desired direction. Using LABVIEW which is a graphical programming language for the processing of eye image captured by camera. For reasons of safety, they limited the robot's work area. [3]. This project supports the use of eye gaze to control assistive robotics. This paper explains about how to efficiently improve the time of completing the task of movement of wheelchair [7].

3. METHODOLOGY

Eye controlled wheelchairs are motorized wheelchairs that are operated using a person's eye movements. In order to translate the user's eye motions into orders that the wheelchair can understand, they use eye-tracking technology to detect, analyse, and interpret the user's eye movements. The user can control the wheelchair's direction and speed by simply looking in the desired direction. This technology can be beneficial for people with disabilities who have limited mobility and cannot use traditional wheelchairs. We started by using a wooden block as the car's structure. Fundamentally, this is our prototype. The wooden frame was then given four wheels.

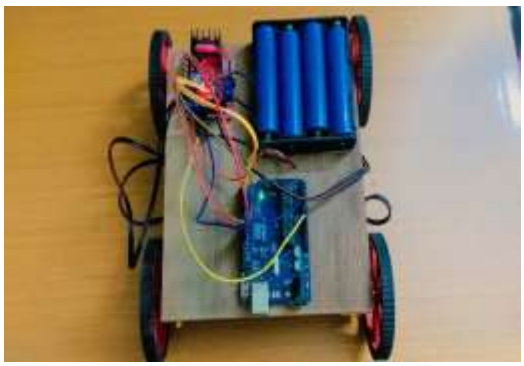

Fig.1. Prototype of system

We then used Python's OpenCV library to construct a Python module that can identify a human's eyes. We have created a module that can recognize if the eye is travelling left or right. We have created a module that can track the eye's movement, whether it is travelling left or right. Additionally, we created an Arduino programmed in the Arduino IDE that will use driver circuitry to control the movement of all 4 BO motors. The output of the Python module was then imported into the Arduino Uno using the cvzone library. Then, to connect all of the circuits, we utilized jumper wires. Last but not least, we tested our prototype and fixed the issues we encountered. Wheelchairs with eye controls employ cameras and eye tracking systems to let the user steer the chair by moving their eyes and heads. The user looks in the direction they would like the wheelchair to move, and the wheelchair responds to the user's gaze. The wheelchair can be programmed to respond to different types of eye and head movements, allowing for a range of motion. For instance, the user can look left and right to move the wheelchair forward and backward, or look up and down to move the wheelchair up and down. The wheelchair can also be programmed to respond to voice commands, allowing for even more control. The eye tracking system can be adjusted to the user's individual needs, allowing for a customized experience.

Fig. 2. Pupil Tracking

International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 17-20, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1004

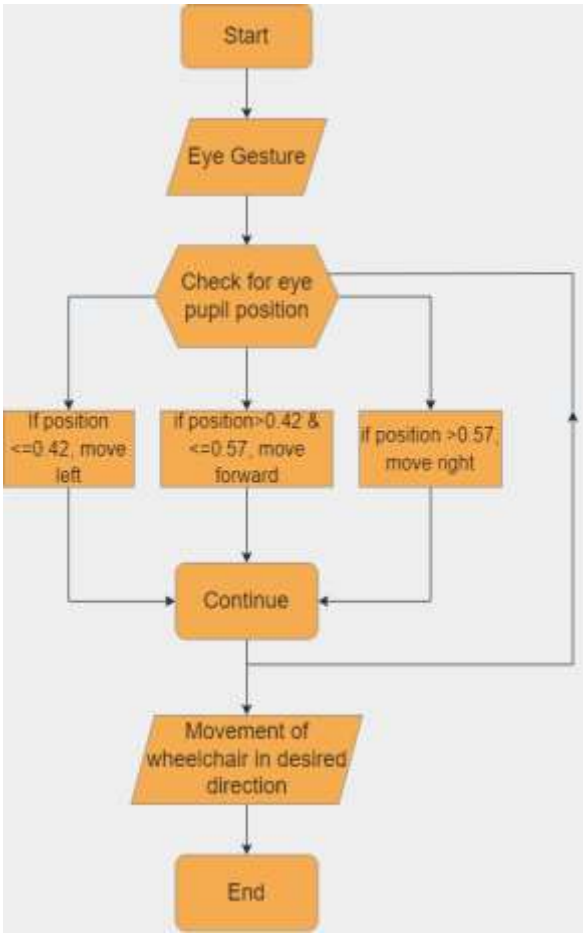

Fig. 3. Block Diagram of Proposed System

4. COMPONENTS

4.1 BO Motor : A "Bo motor" is a small, battery-powered DC geared motor that offers good torque and rpm at low voltages. Here, you could find BO motors with a range of rated speeds. This motor can rotate at a rate of about 200 rpm when fueled by a single Li-Ion battery. Excellent for battery-operated, portable robotics. The motor can work with minimal to no lubrication because of its inherent lubricity. This motor set is the ideal option for use in a mobile robot car because it is reasonably priced, small, and easy to install. They're widely used in our 2WD platforms.

4.2 Motor Driver: Linking the control circuits and the motors together are the motor drivers. While the motor demands a lot of current, the controller circuit can work on signals with minimal current. Because of this, the function of motor drivers is to transform low-current control impulses into higher-current signals that can drive motors

4.3 Arduino UNO: The Arduino Uno microcontroller board is built on the ATmega328P microcontroller chip. It has a reset button, an ICSP header, a power jack, 6 analogue inputs, a 16 MHz quartz crystal, 14 digital input/output pins, an ICSP header, and an ICSP connector. The Arduino programming environment and language are used to programme. It has a wide range of uses, including managing motors and lighting as well as gathering sensor data.

4.4 18650 Batteries: 18650 batteries are a type of lithium-ion rechargeable battery. With a nominal voltage of 3.6V, they typically range in capacity from 1800mAh to 3600mAh. The 18650's name isn't really inventive, to be honest. Power tools, spotlights, cameras, laptops, and e-cigarettes are just a few examples of the many products that include them. Even Tesla's Model S and X automobiles, which debuted in 2013, use 18650 batteries.

5. ADVANTAGES

5.1. Increased Independence: Eye-controlled wheelchairs allow users to gain greater independence by enabling them to move around without having to rely on the help of another person.

5.2. Improved Quality of Life: Eye-controlled wheelchairs can improve the quality of life of users by helping them to remain independent and active.

5.3. Increased Mobility: Eye-controlled wheelchairs allow users to move around more freely, which can lead to increased mobility.

5.4. Improved Safety: Eye-controlled wheelchairs help to keep users safe by providing more precise control of their wheelchair.

5.5. Enhanced Comfort: Eye-controlled wheelchairs can provide a more comfortable experience by allowing users to make small adjustments to their posture and pressure points.

5.6. Increased Efficiency: Eye-controlled wheelchairs can help users to move around more quickly and efficiently. This can be especially beneficial for those who are traveling long distances.

6. LIMITATIONS

6.1. Accuracy: Eye-controlled wheelchairs require a high level of accuracy for the user to effectively control the wheelchair. The user might not be able to steer the wheelchair in the appropriate direction if the system is not accurate enough.

6.2. Cost: Eye-controlled wheelchairs can be expensive. The cost of the technology, plus the time and effort required to set up the system, can be prohibitive for many individuals.

6.3. Fatigue: Eye-controlled wheelchairs require intense concentration and can be tiring to use over an extended period of time. This can be particularly challenging for individuals with limited physical strength or stamina.

6.4. Limited Mobility: Eye-controlled wheelchairs are typically limited to forward and backward motion, and may not be able to turn or move in other directions.

6.5. Environmental Factors: In some lighting situations, eye-controlled wheelchairs may be unable to precisely track a user's eye movements. Additionally, obstacles in the user's environment may block the user's vision, making it difficult or impossible to accurately control the wheelchair.

7. FUTURE SCOPE

Eye-controlled wheelchairs have a very bright future. People with impairments now enjoy greater independence and movement thanks to technological and creative advances. The following are some potential uses for eye-controlled wheelchairs: It is possible to programme an eye-controlled wheelchair to move and navigate on its own. This will make it possible for people with impairments to move around unhindered without depending on others. Eye-controlled wheelchairs can be designed to stop or slow down when they encounter impediments in their path, preventing any potential mishaps. Eye-controlled wheelchairs can be set up to understand user commands, enabling the user to interact with the outside environment. The use of eye-controlled wheelchairs makes it simpler for persons with impairments to enter public spaces by allowing them to navigate ramps, stairs, and other barriers. It is possible to programme the eye-controlled wheelchair to recognise eye motions and hand gestures, giving the user greater exact control over the wheelchair's movement. Overall, eye-controlled wheelchairs are an innovative breakthrough that, with more study, may serve to better the lives of people with impairments.

8. RESULTS

We get the conclusion that the model developed operates as planned after performing several experimental tests. Using Python's media pipe, NumPy, and math library, the model tracks the eye and establishes the direction of sight. The motor is then moved using this signal in the direction of the signal received. The motor will then turn the wheelchair in that direction. The direction of the look may result in a collision with a moving vehicle on the road (for real time application). By using a model-built robot, we were able to function as we saw fit despite the limited software and hardware.

9. CONCLUSION

People with disabilities can move around on their own thanks to the wheelchair technology detailed in this study, which makes use of eye movements. The model tracks the eye and determines the glazing direction using Python programming. This signal is then used to drive the motor in the desired direction. Thanks to this technique, persons with disabilities can now manoeuvre their wheelchair on their own, without help from anybody else

10. ACKNOWLEDGEMENT

We would like to thank our college, Vishwakarma Institute of Technology for helping and supporting us throughout the project.

11. REFERENCES

[1] Shinde, Shalini, Sandeep Kumar, and Prashant Johri. "A review: eye tracking interface with embedded system & IOT." In 2018 International Conference on Computing, Power and Communication Technologies (GUCON), pp. 791-795. IEEE, 2018.

[2] Rosch, Jonathan L., and Jennifer J. Vogel-Walcutt. "A review of eye-tracking applications as tools for training." Cognition, technology & work 15, no. 3 (2013): 313-327.

[3] Patel, Shyam Narayan, and V. Prakash. "Autonomous camera-based eye-controlled wheelchair system using raspberry-pi." In 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1-6. IEEE, 2015.

[4] Mani, Neena, Aby Sebastian, Alen Mathews Paul, Alex Chacko, and Anupa Raghunath. "Eye controlled electric wheel chair." Int. J. Adv. Res. Electr. Electron. Instrum. Eng 4, no. 4 (2015).

[5] Dragusin, Delia, and Mihaela Ioana Baritz. "Development of a System for Correlating Ocular Biosignals to Achieve the Movement of a Wheelchair." In 2020 International Conference on e-Health and Bioengineering (EHB), pp. 1-4. IEEE, 2020.

[6] Wanluk, Nutthanan, Sarinporn Visitsattapongse, Aniwat Juhong, and C. Pintavirooj. "Smart wheelchair based on eye tracking." In 2016 9th Biomedical Engineering International Conference (BMEiCON), pp. 1-4. IEEE, 2016.

[7] Akanto, Jannatul Mawa, Md Kamrul Islam, Ajijul Hakim, Md Azizul Hoque Sojun, and Kawshik Shikder. "Eye Pupil Controlled Transport Riding Wheelchair." In 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), pp. 413-417. IEEE, 2021.

[8] Poornima, G. "Information Fusion Based Wheelchair Control for Paralyzed Patient." In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 921-927. IEEE, 2020.

[9] Jagadale, Pooja Ganesh. "Role of eye tracking system to enhance life of disable people." International Research Journal of Modernization in Engineering Technology and Science 2, no. 11 (2020): 715-719.

[10] Juhong, Aniwat, T. Treebupachatsakul, and C. Pintavirooj. "Smart eye-tracking system." In 2018 International Workshop on Advanced Image Technology (IWAIT), pp. 1-4. IEEE, 2018.

International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 21-27, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1005

Next Word Prediction in Bodhi Language Using LSTM-based Approach

Ankush Kumar
Department of Computer Science and Engineering
School of Engineering and Technology
Sharda University
Greater Noida, India

Pushpendra Kumar Mishra
Department of Computer Science and Engineering
School of Engineering and Technology
Sharda University
Greater Noida, India

Tsering Namgail
Department of Computer Science and Engineering
School of Engineering and Technology
Sharda University
Greater Noida, India

Sandeep Kumar
Department of Computer Science and Engineering
School of Engineering and Technology
Sharda University
Greater Noida, India

Abstract: Bodhi language is one of the rare languages which is still spoken in the Leh neighborhood, Ladakh and many Tibetan regions. There is not much linguistic research done in this language. Even google translate does not work on this language. There are various types of other linguistic researches and model available on language like English and some other regional languages like Hindi, Bangla, Ukrainian etc. But there are almost negligible research and models available on Bodhi Language.

In this paper, we proposed a Language Modelling Technique using Long Short Term Memory network (LSTM) which is based on Recurrent Neural Network (RNN), using this machine learning technique we have made a model to predict the next word in bodhi language, when the user will input anything, the model will predict the next word according to the previous word(s). This model is already made for the English language but we are making the model or basically programing the model to predict the next word in the Ladakhi language which is also called as Bodhi language. This language is more complex than English language. We have tried to make the model as accurate as possible while predicting the next word in Ladakhi language. To prepare the model we have collected dataset as a large collection of Bodhi words. In this model, we have trained the model in 500 iterations (Epochs).

we used the TensorFlow, keras, dictionaries, pandas, NumPy packages. For the coding purpose we used the platform called Google Colab which is provided by google for machine learning enthusiasts.

Keywords: NLP, Next word prediction, RNN, LSTM, machine learning, deep learning.

1. INTRODUCTION

We are living in the word of machine learning in which we see different machine learning algorithms for different kind of automated works and services. Machines which work on themselves without any human touch and effort. And automatically improve themselves through experiences of previous and current work. Machines can easily recognize the patterns in between the words and things which humans cannot recognize. We very well know that. In traditional programming, the solution is the output, while the inputs are rules and data.

Whether we're merely sending messages or browsing the internet, we usually text on gadgets like our phones and desktops. While doing such things, we can notice that it proposes the next word based on what we are typing. This function, called next word prediction, foresees the word that could appear after one of our messages. It saves us time and enables us to write more swiftly and effectively. The next word prediction (NWP) problem is a significant one in the field of natural language processing. Another name for it is language modelling, and text mining is used in this case.

In this essay, we discuss the Bodhi language, an uncommon tongue that is only spoken in the Ladakh area. It is often written in Tibetan Script, and compared to most other Tibetan dialects, its sound is considerably more similar to the classical Tibetan language. It also goes by the name Bhoti language. Many of the prefix, suffix, and head characters that are silent in many other Tibetic languages, particularly Central Tibetan, are spoken by Ladakhis. The Ladakhi alphabets are shown in figure n. 1 below.

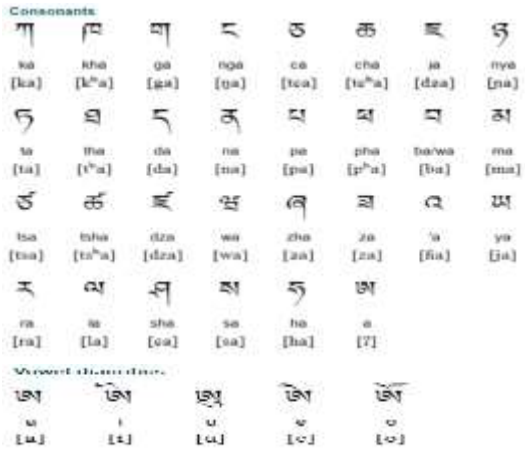

Figure 1. Alphabets in Ladakhi Script

Even Google Interpret does not have the ability to translate the Bodhi language, which is still used in Tibet and the surrounding Nepal. We are the first to attempt next word prediction in the Bodhi language, taking a step towards the strategy of preserving this extremely uncommon language. The programmers who are now working on this LSTM model are aware of how well it predicts the following word.

A variant of the recurrent neural network (RNN) architecture is long short-term memory (LSTM). However, because there is no word spacing in Bodhi, the LSTM model does not perform well when applied to this language. As a result, we must provide word space. The developers made their decision to employ LSTM because they thought it may help people remember important terms for a longer period of time. The goal of creating this model is to properly predict the next word based on input in the very language of Bodhi. In this study, we employed a variety of input changes to train the system to recognize patterns and produce correct predictions.

2. LITERATURE REVIEW

One of the current hot areas in natural language processing research is next word prediction. On this subject, numerous study papers have been published. These papers serve as the sources for our study paper.

In this paper the author suggests a method for Ukrainian language next-word prediction using a neural network-based language model.[1] To improve performance, the authors examine several model types and data pretreatment methods. They also suggest a modified version of the model that would take contextual information into account and assess the model's efficacy. The suggested method is very accurate and effective for a range of natural language processing jobs. The study advances Ukrainian, a language with limited resources, in terms of natural language processing. The quantity of the dataset utilized for assessment and the breadth of the suggested technique are two limitations of the article, though.

The use of recurrent neural networks (RNNs) for word prediction is examined in this research.[2]The authors talk on the value of next word prediction in a variety of contexts, including text completion, speech recognition, and machine translation. Following a brief introduction to RNNs and their design, they suggest a model for next word prediction that makes use of a Long Short-Term Memory (LSTM) network. On a dataset of text from diverse sources, the suggested model is assessed and contrasted with other models already in use. The findings demonstrate that, in terms of accuracy and efficiency, the suggested LSTM-based model performs better than alternative models.

The use of pre-training methods for federated text models in the context of next word prediction is explored in this work.[3]The authors provide a system to enhance next word prediction problems that blends federated learning with pre-training techniques like BERT and GPT-2. On a sizable dataset, they test their suggested framework, and they compare the outcomes to those of other cutting-edge models. In comparison to current models, the suggested framework, according to the authors, offers more accuracy and scalability.

In their study from 2020, Moghar and Hamiche [4] investigate the use of LSTM recurrent neural networks for stock market forecasting. To forecast stock values over a given time period, the authors used stock data from a significant American firm using the LSTM model. The outcomes demonstrated that the LSTM model was highly accurate in predicting stock values. The work delivers a significant addition to the field of predictive analytics and offers insights into the possible application of machine learning algorithms for financial forecasting.

The use of Long Short-Term Memory (LSTM) neural networks for the problem of next word prediction is discussed in the study. The LSTM model's design and training procedure are described by the authors, who also assess the model's performance using a dataset of text sequences.[5] In comparison to conventional language models, the experimental findings demonstrate that the LSTM model achieves excellent accuracy in predicting the following word in a given sequence. Additionally, the authors offer possible uses for the LSTM model in natural language processing tasks as speech recognition, machine translation, and text creation.

The study on COVID-19 time series forecasting in Canada using Long Short-Term Memory (LSTM) networks is presented in the publication.[6] The authors assess three LSTM models using a dataset of daily COVID-19 cases in Canada and compare their performance using various input settings. With the best model reaching a mean absolute percentage error of 5.78%, the results show that the LSTM models are successful in projecting the COVID-19 transmission. According to the study, LSTM networks can be an effective tool for forecasting COVID-19's future spread and guiding public health policy in Canada.

The study on utilizing Long Short-Term Memory (LSTM) neural networks for projecting an object's future location is presented in the publication "Next position prediction using LSTM neural networks."[7] The study focuses on using a particular dataset that contains information on the position and speed of a moving item. The LSTM neural network model is applied to this dataset by the authors, who then assess its performance using several criteria. They contrast the outcomes with those from several forecasting methods, such as Linear Regression and Random Forest. According to the study's findings, The LSTM neural network model performs better than the other models in terms of prediction accuracy, indicating its potential for usage in related applications in the future.

The exploration by Fang, Chen, and Xue [8] gives a survey of the literature on spatio-temporal sequence prediction algorithms based on recurrent neural networks (RNNs). Before discussing several RNN models and their variations that have been suggested for this job, the authors give an outline of the key ideas and difficulties in spatiotemporal data prediction. They emphasize the benefits and drawbacks of each model and shed light on the direction that this field of study is now taking. Overall, the publication is a valuable tool for scientists working on RNN-based models for spatio-temporal sequence prediction.

To predict cluster CPU consumption, Nashold and Krishnan (2020) suggested using Long Short-Term Memory (LSTM) and Seasonal Autoregressive Integrated Moving Average (SARIMA) models.[9] They tested the models using actual data and discovered that, in terms of accuracy and root mean squared error, the LSTM model performed better than the SARIMA model. The study shows how machine learning approaches might be used to enhance resource management in computer clusters. The study might benefit from further validation using more datasets as it is constrained by the use of a single dataset.

Long Short-Term Memory (LSTM) neural networks are suggested as a method in the study "Real-time driver maneuver prediction using LSTM" for the prediction of driver maneuvers in real-time.[10] The accuracy of the model that the authors developed for predicting four different driving maneuvers—changing lanes, turning left, turning right, and stopping—was 87.5% when tested on data from a driving simulator.Additionally, they evaluated the effectiveness of their model against other cutting-edge techniques. The suggested approach may be used in traffic management, driver aid systems, and driverless cars.

A paradigm for context-based text production that makes use of Long Short-Term Memory (LSTM) networks was put out by Santhanam in 2020.[11] To produce writing that is cohesive and pertinent, the model takes into account the context of the words before them. The suggested model's architecture and training procedure are described in detail, and the study assesses the

model's performance using a number of measures. The outcomes demonstrated that the suggested model performs better at producing pertinent and coherent content than conventional language models. According to the article, the suggested model may find use in a number of natural languages processing tasks, including chatbots, conversation systems, and machine translation.

The approach for forecasting product quality in the research combines time-dimensional K-means with state transition-LSTM [12] networks, multiple models, and dual sampling periods. The authors do trials using real-world datasets to show that their strategy performs better in terms of prediction accuracy than the competition. They also shed light on the significance of including both past and present data in prediction processes. In order to increase product quality and lower production costs, the study demonstrates the possibility of applying machine learning approaches for quality prediction in industrial settings.

The study describes an intelligent, autonomous street lighting system that saves energy by using weather forecast information. The Long Short-Term Memory (LSTM) algorithm [13] serves as the system's foundation for forecasting weather conditions and altering illumination settings accordingly. The results of the trials the authors ran to compare the suggested system's energy usage with a conventional street lighting system revealed a considerable reduction in energy consumption. The potential of data-driven methodologies for developing sustainable energy solutions is highlighted in the article.

A thorough analysis and assessment of text prediction and entertainment systems are provided in the work by Hamarashid, Saeed, and Rashid.[14] The authors look at several methods for text prediction, such as rule-based and machine learning-based ones, and rate their precision and efficacy. They also talk about how chatbots and video games that employ text prediction are used for fun. The study emphasizes the significance of enhancing these systems' performance through the application of cutting-edge algorithms and methodologies and offers insights into prospective future research topics.

The study suggests a unique method for employing LSTM recurrent neural networks to forecast numerous illnesses. The authors used a collection of patient medical information from a variety of conditions to conduct tests.[15] In terms of accuracy, sensitivity, and specificity, the suggested model produces encouraging results. The work emphasizes the opportunity for multi-disease prediction using deep learning models, which has the potential to greatly enhance healthcare services.

The research examines the cloud sentiment analysis accuracy of three recurrent neural network models: RNN, LSTM, and GRU. The data was pre-processed by the authors [16] using methods including tokenization, stemming, and stop-word removal from internet evaluations of cloud services. The three models were then trained, and their accuracy was assessed using measures including precision, recall, and F1-score. With an F1-score of 0.8625, the LSTM model beat the other two models. The GRU model came in second with an F1-score of 0.8573, while the RNN model came in third with an F1-score of 0.8248. For cloud sentiment analysis, the authors advise utilizing LSTM.

The Long Short-Term Memory (LSTM) algorithm and local weather predictions are combined in the paper's innovative technique for forecasting [17] hourly solar irradiance. The LSTM model is evaluated on a dataset from a solar power facility in South Korea after being trained using non-local meteorological data. Results reveal that the suggested technique performs better in terms of accuracy than other current models and can forecast the hourly solar irradiance for the following day with an average error rate of 9.73%. According to the study, energy management systems may employ the suggested technique for improved planning and management of solar power generation.

The usefulness of machine learning and deep learning approaches for forecasting stock prices is examined in the study "Stock price prediction using machine learning and LSTM-based deep learning models".[18] The study forecasts stock values using historical data utilizing LSTM-based deep learning models and a variety of machine learning methods, such as Random Forest and Support Vector Regression. The article comes to the conclusion that the LSTM-based model performed better than the conventional machine learning methods and might be a useful stock price prediction tool. The study's overall findings emphasize the promise of deep learning methods for stock market forecasting.

The EEMD-GA-LSTM approach using large scaled wind history data is the basis for the novel framework for short-term wind speed prediction proposed in this research.[19] The decomposition of the wind speed time series into intrinsic mode functions using the proposed method's ensemble empirical mode decomposition (EEMD) algorithm is followed by genetic algorithm (GA) optimization to choose the most pertinent features. Finally, wind speed prediction is performed using a long short-term memory (LSTM) model. The EEMD-GA-LSTM technique performs better than numerous other approaches in terms of prediction accuracy and resilience when the suggested method is evaluated on actual wind speed data, making it a viable method for short-term wind speed prediction.

The Long Short-Term Memory (LSTM) and bi-directional LSTM (BLSTM) models are highlighted in this paper's evaluation of the literature on the application of deep learning techniques for stock price prediction.[20] The authors describe other research that have utilized these models for stock price prediction and go through the benefits of using them over more conventional approaches.

They also list some of the drawbacks of this strategy, such as the requirement for a lot of data and the complexity of interpreting the findings. Overall, the study offers a valuable summary of the current status of LSTM and BLSTM-based deep learning-based stock price prediction.

3. METHODOLOGY

3.1 Dataset

The dataset was compiled from around 5000 Bodhi words which were from various Ladakhi articles, newspapers, and dictionaries. Sentences made up of words are then combined to serve as the input for training and testing. These sentences have a word count of five or more. Many brief sentences with sequences of less than six words can be found in the dataset. Fig. 2 shows the snap of the dataset.

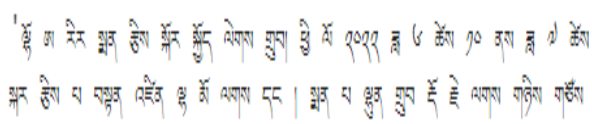

Figure 2. Snap of the dataset

3.2 Methodology

We used a LSTM based approach to build our model in which we build a sequential model with 4 layers in which two LSTM layers and two Dense layers. The input size of the model is 3 and output is 1 while the sequence length is 10. We trained our model in batch size of 64 and in 500 epochs. To maintain and update the

International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 21-27, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1005

state of memory cells, the LSTM model filters data through the gate structure. Its door structure consists of input, output, and forgotten gates.[18] Three sigmoid layers and one tanh layer make up each memory cell. The LSTM memory cells' structure is shown in Fig. 3.

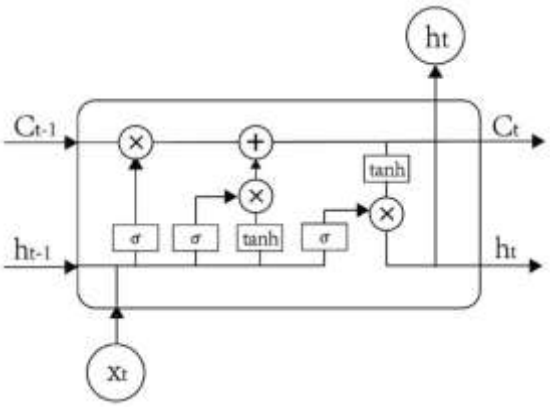

Figure 3. Basic Architecture of LSTM

Which cell state information is eliminated from the model by the forgotten gate in the LSTM unit. As seen in Fig. 1, the memory cell takes as inputs the external information xt of the present instant and the output ht-1 of the previous moment, which it then combines into a long vector [ht-1, xt] by transformation to create

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f),$$

where Wf and bf stand for the forgetting gate's weight matrix and bias, respectively, and is the sigmoid function. The primary purpose of the forgotten gate is to keep track of how much of the current cell state Ct is reserved for the prior cell state Ct-1. Based on ht-1 and xt, the gate will output a value between 0 and 1, with 1 denoting total reserve and 0 denoting complete discard.

In figure 3, By allowing only a few linear interactions, the cell state of LSTM helps the information to flow through the units without being altered. Each unit has input, output and a forget gate. Each unit with the help of input, output and forget gate can add or remove information. Forget gate decides which information is to be forgotten and which is not to be forgotten. Forget gate uses sigmoid function for it. While the input gate controls the flow of information. Input gate uses pointwise multiplication of Sigmoid and tanh function for it respectively. While the output gate decides which information to passed to next state.

Figure. 4 shows the most basic outline of our model in which 3 words as input are required while it gives the next word as output.

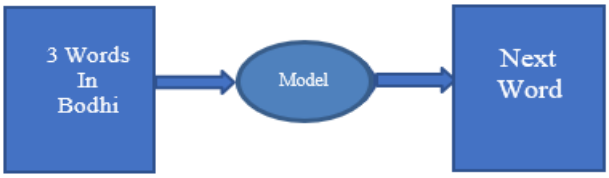

Figure 4. basic outline of the model

For the preparation of such a model, we have to work on the dataset using various operations and functions provided by various ML related packages in python such as numpy, Tensorflow, Pandas, Matplotlib, Tokenizer etc.

To prepare the model we divided the model into modules which solves the sub problems. The dataflow between these modules of sub- tasks is given in Figure. 5.

The figure describes how data flows from various sub tasks which performs some operations on data including cleaning and preprocessing of data to training the model and after that the prediction of the next word. It only shows the sub tasks for preparing the model and the data flow through it. It does not show how many layers are in the model and how and which operations are performed in the subtask.

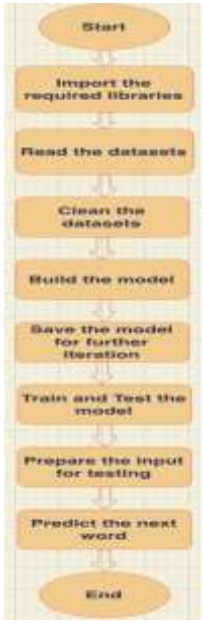

Figure 5. Applied Basic Method

All the processes or operations performed on data before feature engineering comes under the data-preprocessing in which cleaning the dataset, removing outliers and converting the data into machine understandable language or in binary digits comes. Before starting the procedure, the dataset must be cleaned. The words in the dataset are then divided into several groups.

The iterator is used to parse the input file and collect distinct words. With the help of tokenizer function in preprocessing library of tensorflow package tokens were generated for sequential text. This demonstrates that words are challenging for machine learning neural networks to process, making it essential to map them to indices, which are straightforward for neural networks to recognize.

The process starts with the sequencing of the given words after the sequencing the feature engineering is done and input and output features were created. For prediction, we used 3 words to predict the next words for which the input was the np array with 4 sequence elements and output was the last element of the np array. We used a Sequential model with 4 layers. Our model was fairly accurate. We used our model to predict in both languages in English as well as bodhi language. Model was fairly accurate in English language but its accuracy decreased in Bodhi language. Yet we tried to raise its accuracy by separating the words and then tokenization of these words. In English language, we trained our model for only 7 Epochs in last epoch loss was equal to 4.4253 and accuracy was around 70%. Which is shown in below figure.

```
Epoch 7/7
1958/1958 [==============================] - ETA: 0s - loss: 4.4253
Epoch 7: loss improved from 4.62284 to 4.42526, saving model to next_words.h5
1958/1958 [==============================] - 30s 15ms/step - loss: 4.4253
```

Figure 6. Epochs for next word prediction for English language

International Journal of Computer Applications Technology and Research
Volume 12–Issue 05, 21-27, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1205.1005

In Bodhi language we trained our model for 500 iterations and loss was around 0.00022 and accuracy was 50%. Which is show in the below figure.

Figure 7. Epochs for next word prediction model for Bodhi Language

Table 1. Comparison of accuracy between English and Bodhi language accuracy.

	Epochs	Loss	Accuracy (in %)
English	7	4.42	70
Bodhi	500	0.0003	50

As this language is very hard for preprocessing and training the model, yet we managed to train our model, and test it manually. The loss of our model kept on decreasing in our model. It was very hard to collect dataset for training our model and in future as dataset increases our model will improve in accuracy as well as performance. We prepared a separate function for preparation of user input. This function takes input from user tokenize it and preprocessing happen which converts the input text into tokens with indexing of serial numbers. Then the input is given to model. Model works on input and gives output as a word.

4. RESULT

While training our model the loss kept on decreasing. Loss to Epochs graph is given below which visualizes how the loss is behaving in each epoch. The figure given below visualizes the trend of loss during training (figure 8 shows). Which is also shown using table n. 2.

Figure 8. Training loss

Accuracy trends of our model throughout all training epochs are visualized by the figure n. 9 given below also the same is shown using the table n. 3.

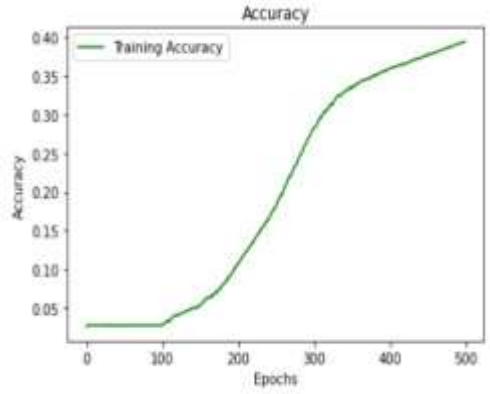

Figure 9. Accuracy

Table 2. Training loss throughout training of model

Loss	Epochs
0.00044	0-100
0.00042	100–150
0.00040	150-200
0.00036	200-250
0.00032	250-290
0.00025	290-300
0.00022	300-500

Table 3. Accuracy throughout training of model

Accuracy	Epochs
0.13	0-200
0.28	200-300
0.38	300-400
0.44	400-500

We created a function for preparing input and feeding it to our model. With the help of the tokenization our input text was sequenced. our model processes the input and gives one and the most probable word as output.
Now our model can predict the next word in Bodhi language. Which is the language of Ladakh and surrounding regions Nepal and Tibet.

We used 3 words as input and accuracy was fairly high in comparison to 1 word as input which is 50%.
A snap of the output of the model is given below in figure n. 10. including the parts of

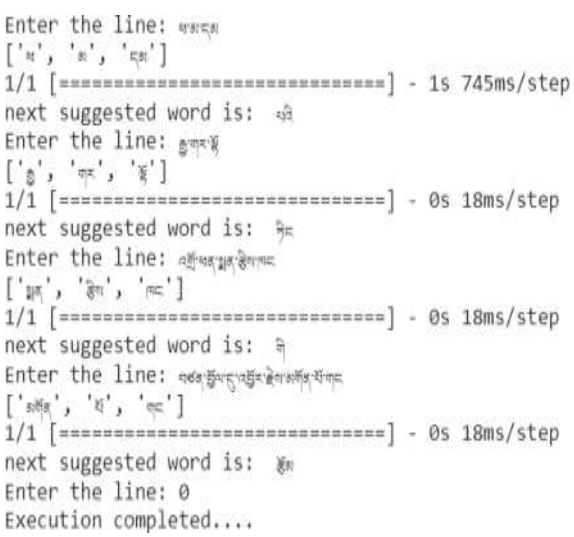

Figure n. 10: Snap of Output

5. CONCLUSION

Next word prediction is one of the most researched NLP fields because it is about finding text. We have used an LSTM model which is trained in 500 iterations. Our work is the first to be done on a rare language like Bodhi. From the result, it can be said that the accuracy is sufficiently high. This model can be used to predict the next word from the target's input. This model works on a language which even google translate does not provide a service for, which is a feat in itself. First our model takes words as input for which we have decided to take 3 words as minimum word limit so our model takes minimum 3 words as input and assign tokens to these words using tokenizer function which is already available after tokenizing model finds the next word based on these three words and gives the most probable word as input. For testing of our model, we had to make a module separately so that model can tokenize the input words and take those words as input. Because all the work is going on in numerical terms and model tries to find the underlying patterns among these numerical tokenized sequences which are given for the words while training.

6. FUTURE SCOPE

As the dataset was pretty hard to collect, hence in the future we can gather more data so that our model can be trained thoroughly. And its accuracy can be increased. There is a need to research the proper method for the preprocessing of dataset in Bodhi language so that accuracy can be increased. Future research may be done to improve next word prediction models' performance for Bodhi and other low-resource languages. The method used in this work may also be applied to other language models that call for next word prediction, which will facilitate the creation of natural language processing tools that are more precise and efficient. The results of this study demonstrate the potential of deep learning in natural language processing and its capacity to promote the growth of underdeveloped languages.

7. REFERENCES

[1] Shakhovska, K., Dumyn, I., Kryvinska, N., & Kagita, M. K. (2021). An Approach for a Next-Word Prediction for Ukrainian Language. Wireless Communications and Mobile Computing, 2021, 1-9.

[2] Ambulgekar, S., Malewadikar, S., Garande, R., & Joshi, B. (2021). Next Words Prediction Using Recurrent NeuralNetworks. In ITM Web of Conferences (Vol. 40, p. 03034). EDP Sciences.

[3] Stremmel, J., & Singh, A. (2021). Pretraining federated text models for next word prediction. In Advances in Information and Communication: Proceedings of the 2021 Future of Information and Communication Conference (FICC), Volume 2 (pp. 477-488). Springer International Publishing.

[4] Moghar, A., & Hamiche, M. (2020). Stock market prediction using LSTM recurrent neural network. Procedia Computer Science, 170, 1168-1173.

[5] Afika, R., Suprih, W., Atikah, D. A., & Fadlan, B. H. (2022). Next word prediction using LSTM. Journal of Information Technology and Its Utilization, 5(1), 10-13.

[6] Chimmula, V. K. R., & Zhang, L. (2020). Time series forecasting of COVID-19 transmission in Canada using LSTM networks. Chaos, Solitons & Fractals, 135, 109864.

[7] Violos, J., Tsanakas, S., Androutsopoulou, M., Palaiokrassas, G., & Varvarigou, T. (2020, September). Next position prediction using LSTM neural networks. In 11th Hellenic Conference on Artificial Intelligence (pp. 232-240).

[8] Fang, W., Chen, Y., & Xue, Q. (2021). Survey on research of RNN-based spatio-temporal sequence prediction algorithms. Journal on Big Data, 3(3), 97.

[9] Nashold, L., & Krishnan, R. (2020). Using LSTM and SARIMA models to forecast cluster CPU usage. arXiv preprint arXiv:2007.08092.

[10] Khairdoost, N., Shirpour, M., Bauer, M. A., & Beauchemin, S. S. (2020). Real-time driver maneuver prediction using LSTM. IEEE Transactions on Intelligent Vehicles, 5(4), 714-724.

[11] Santhanam, S. (2020). Context based text-generation using lstm networks. arXiv preprint arXiv:2005.00048.

[12] Shi, X., Li, Y., Yang, Y., Sun, B., & Qi, F. (2021). Multi-models and dual-sampling periods quality prediction with time-dimensional K-means and state transition-LSTM network. Information Sciences, 580, 917-933.

[13] Tukymbekov, D., Saymbetov, A., Nurgaliyev, M., Kuttybay, N., Dosymbetova, G., & Svanbayev, Y. (2021). Intelligent autonomous street lighting system based on weather forecast using LSTM. Energy, 231, 120902.

[14] Hamarashid, H. K., Saeed, S. A., & Rashid, T. A. (2022). A comprehensive review and evaluation on text predictive and entertainment systems. Soft Computing, 1-22.

[15] Men, L., Ilk, N., Tang, X., & Liu, Y. (2021). Multi-disease prediction using LSTM recurrent neural networks. Expert Systems with Applications, 177, 114905.

[16] Raza, M. R., Hussain, W., & Merigó, J. M. (2021, October). Cloud sentiment accuracy comparison using RNN, LSTM and GRU. In 2021 Innovations in intelligent systems and applications conference (ASYU) (pp. 1-5). IEEE.

[17] Jeon, B. K., & Kim, E. J. (2020). Next-day prediction of hourly solar irradiance using local weather forecasts and LSTM trained with non-local data. Energies, 13(20), 5258.

[18] Mehtab, S., Sen, J., & Dutta, A. (2021). Stock price prediction using machine learning and LSTM-based deep learning models. In Machine Learning and Metaheuristics Algorithms, and Applications: Second Symposium, SoMMA 2020, Chennai, India, October 14–17, 2020, Revised Selected Papers 2 (pp. 88-106). Springer Singapore.

[19] Chen, Y., Dong, Z., Wang, Y., Su, J., Han, Z., Zhou, D., ... & Bao, Y. (2021). Short-term wind speed predicting framework based on EEMD-GA-LSTM method under large scaled wind history. Energy Conversion and Management, 227, 113559.

[20] Sunny, M. A. I., Maswood, M. M. S., & Alharbi, A. G. (2020, October). Deep learning-based stock price prediction using LSTM and bi-directional LSTM model. In 2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES) (pp. 87-92). IEEE.

[21] Mei, L., Hu, R., Cao, H., Liu, Y., Han, Z., Li, F., & Li, J. (2020). Realtime mobile bandwidth prediction using LSTM neural network and Bayesian fusion. Computer Networks, 182, 107515.

[22] Zhao, J., Zeng, D., Xiao, Y., Che, L., & Wang, M. (2020). User personality prediction based on topic preference and sentiment analysis using LSTM model. Pattern Recognition Letters, 138, 397-402.

[23] Mueller, A., Nicolai, G., Petrou-Zeniou, P., Talmina, N., & Linzen, T. (2020). Cross-linguistic syntactic evaluation of word prediction models. arXiv preprint arXiv:2005.00187.

[24] Hansun, S., & Young, J. C. (2021). Predicting LQ45 financial sector indices using RNN-LSTM. Journal of Big Data, 8(1), 1-13.

[25] Rauf, H. T., Lali, M. I. U., Khan, M. A., Kadry, S., Alolaiyan, H., Razaq, A., & Irfan, R. (2021). Time series forecasting of COVID-19 transmission in Asia Pacific countries using deep neural networks. Personal and Ubiquitous Computing, 1-18.

[26] Kwon, B. S., Park, R. J., & Song, K. B. (2020). Short-term load forecasting based on deep neural networks using LSTM layer. Journal of Electrical Engineering & Technology, 15, 150