Enhancing the Hill Cipher Algorithm and Employing a One Time Pad Key Generation Technique

Mersha Derese Gietaneh[a*], Tadesse Birara Akele[a]

[a] Department of Computer Science, College of Informatics,
Kombolcha Institute of Technology, Wollo University, Ethiopia.

.

How to cite this paper: https://xxxxx*

ISSN : 2788-6239 (Print)
ISSN: 2788-6247 (online)

*Corresponding Author: mershaderese@gmail.com

ABSTRACT

Mobile money has evolved to enhance financial inclusion in many developing countries through the development of smartphones and financial technologies. The majority of mobile money schemes used in these nations implement two-factor authentication. However, these 2FA schemes are vulnerable to cryptanalysis and brute force attacks over time. This is because they only rely on a personal identification number and subscriber identity module. This study aims to develop a secure algorithm for encrypting Tele-Birr information using the enhanced Hill cipher technique with a symmetric key. The algorithm encrypts all Tele-Birr information using two keys k1, k2 in the form of a character matrix, generating a unique key for one-time encryption. Various cryptographic algorithms, such as Caesar cipher, Affine cipher, Vigenere cipher, and Hill cipher, have been created. By employing this symmetric key cryptography technique, all Tele-Birr information can be converted into unreadable messages using a combination of 131 additional characters and symbols. The enhanced encryption character set consists of 141 characters, making the ciphertext extremely difficult for intruders to decipher due to the exponentially increased key space. This algorithm not only offers secure and efficient authentication but also ensures data confidentiality, integrity, nonrepudiation, and privacy. The performance analysis indicates that the proposed algorithm achieves better overall performance compared to existing Tele-Birr security solutions. This is due to the character changes and positional arrangement of matrix possible key space. The results were obtained using the Matlab simulation tool, which demonstrated an avalanche effect in the proposed algorithm.

Keywords: Cryptography, One Time Pad Key Generation, Character positional arrangement, Avalanche effect, Tele-Birr security issue

1. INTRODUCTION

Security involves the protection of computer systems, information, and assets from attacks when data is transferred between computers and devices. Security mechanisms prevent unauthorized access, theft, harm, and disclosure of information. Online communication has become highly prevalent in today's world, making data protection crucial in network environments. Various data protection systems, such as authentication (username, password), intrusion detection systems (IDS), firewalls, biometric systems, and cryptography (encryption and decryption), exist to ensure data security. Cryptography, the science of safeguarding private information, plays a vital role in maintaining confidentiality, integrity, and authentication in cyber security. It employs encryption and decryption methods to conceal or reveal transaction information, thereby achieving security goals. Encryption transforms Tele Birr transaction messages into unreadable text for intruders, while decryption converts cipher text back into the original message. Cryptography utilizes different algorithm techniques, including Caesar substitution cipher, Vigenere cipher, columnar transposition, Hill cipher (Hc), Advanced Encryption Standard (AES), digital signature algorithm, Data Encryption Standard (DES), hash algorithms, RSA, elliptical curve, and El Gamal. These techniques fall under the categories of symmetric or asymmetric cryptography. The Hill cipher, invented by mathematician Lester Hill, is a symmetric block cipher technique. Both the sender and receiver employ the same key in the form of a matrix. The encryption and decryption keys must satisfy the condition kk-≡1 mod n=1, where n=26 [1][6][15]. The Hill cipher is commonly used to encrypt images and text messages. It assigns a number modulo 26 to each letter, where A = 0, B = 1, and Z = 25. To encrypt a document with modulus 26, each block of n letters is multiplied by an invertible nXn matrix. Similarly, to decrypt the message, each block is multiplied by the inverse of the key matrix. The cipher key represents the matrix used for encryption and should be randomly selected from a collection of invertible mxm matrices (modulo 26). This mathematical description outlines the functioning of the Hill cipher. The building block cryptography is shown in Figure 1.

RC = (PK) mod26, (For Encryption)

P = (PK-) mod26, (For Decryption)

K = $k11\ k12 - - - - k1s$

$k21\ k22 - - - - k2s$

$ks1\ ks2 - - - - kss$

C1= $P1K11$ + $P2K21 + - - -PsKs1$

C2 = $P1K12$ + $P2K22 + - - - PsKs2$

Cs = $P1K1s$ + $P2K2s + - - - PsKss$

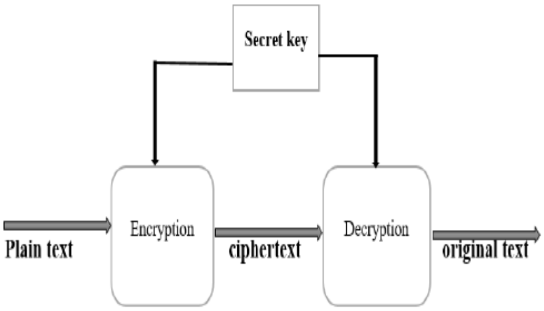


Fig. 1 The building block of cryptography [4]

The Ethiopian Telecom service was launched in 1992 and has been providing various services to its customers ever since. One of the recent additions to the telecom services is Tele Birr. Information security has emerged as a concern in Tele Birr, where money transactions and information exchanges are susceptible to cryptanalysis, social engineering, brute force attacks, and data interruption. To address these security issues, a solution called"Enhancing the Hill Cipher Algorithm and Employing a One Time Pad Key Generation Technique" (EHCAAEaOTPKGT) has been proposed.

1.1 Related cryptography literature

Cryptography involves the technique of safeguarding data from unauthorized access or modification through encryption and decryption methods. Intruders often attempt to intercept data using brute force attacks and frequency analysis. To address these issues, researchers have developed various security algorithm methods.

In one such work presented in [1], the authors propose a modified version of the Hill Cipher algorithm that utilizes ASCII values for encryption. The focus of the proposed algorithm is to address the issue of unauthorized agents gaining access to sensitive data. The algorithm is based on modular arithmetic and employs a fixed key size. It converts characters into binary using the XOR operation and increases the English alphabetical letter modulo to 256 ASCII characters. Simulation results using C++ show the effectiveness of the proposed approach. However, it should be noted that the proposed work considers ASCII characters that are known to everyone, which may pose a limitation.

In another research by authors in [3], a novel cryptosystem called the Multiplicative Substitution Cryptosystem (MSC) is proposed. This cryptosystem adds protection to characters with values ranging from 0 to 255, including extended ASCII characters. The encryption process involves multiplying the plaintext and the key, both represented as characters. The characters are converted into corresponding ASCII values. The authors aim to enhance the confidentiality issue in symmetric key cryptography by introducing a non-linear function using a combination of affine, Caesar, and playfair ciphers in the form of a multiplicative cipher. However, a drawback of this approach is that the key with ASCII characters remains printable as it is, which reduces the efficiency of symmetric encryption.

In [6], the authors propose the Generation of Key Matrix for Hill Cipher Encryption Using Classical Cipher. The modification involves using the positional value of the ciphertext as numbers in the encryption key matrix. The first ciphertext is generated using the Playfair Cipher for the given plaintext. The results show that the modified Hill Cipher enhances information communication by increasing the key size and creating robust encryption. However, the use of the Playfair cipher for key generation introduces repeated letters that can be exploited by intruders by analyzing the frequencies of English alphabets.

Authors in [7] present a hybrid cryptographic method called Text Encryption, combining the Hill Cipher and Vigenere Cipher (TEHCMUVH). The hill cipher encrypts the plaintext using a constant matrix key, which is further encrypted by the Vigenere key. The goal is to increase the confidentiality, non-repudiation, and source authentication of information. However, the statistical and brute-force attacks are still potential issues in the Hill Cipher due to the limited keyspace of 26 alphabet letters. Additionally, the encryption of the Vigenere Cipher may involve letter repetition, which weakens the overall encryption.

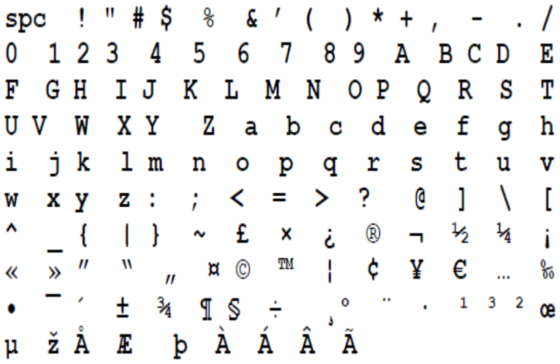
In [29], the authors propose a cryptanalysis of a modification in the Hill Cipher to overcome the defense against known-plaintext attacks. Despite the great diffusion property exhibited by the Hill Cipher, it remains vulnerable to known-plaintext attacks due to specific patterns in the plaintext. The authors suggest modifying the classical Hill Cipher to address this issue, where the plaintext is transposed into a constant matrix. However, the constant matrix structure and the limited modular arithmetic using 26 letters (A-Z) make it susceptible to decryption using cryptanalysis.

Authors in [31] present encryption and decryption of short messages using the Vigenere Cipher with matrix expression to enhance message confidentiality. To address the weaknesses of the Vigenere Cipher, they propose combining it with the Rivest-Shamir-Adleman (RSA) algorithm. The encryption process uses a public key, while decryption employs a private key. The drawback of this approach is the increased computational time required for encryption and decryption. Additionally, the use of both public and private keys in the algorithm makes it less efficient in terms of time and space.

In summary, various modifications and combinations of encryption algorithms have been proposed to address the vulnerabilities and limitations of existing cryptographic methods. Each approach offers different advantages and drawbacks, and the choice of algorithm depends on specific requirements and trade-offs.

2. MATERIALS AND METHODS

The proposed algorithm focuses on increasing the key size and using a larger modulo value of 141 to select positions in the Hill Cipher algorithm, aiming to minimize intrusion in Tele Birr transactions. This algorithm effectively reduces the likelihood of brute force and cryptanalysis attacks. The key in our algorithm consists of two matrices ('k1' and 'k2') that are multiplied with the plaintext (p). The algorithm relies on a set of private keys and parameters used to encrypt all digit characters, special characters, and other symbols to enhance the complexity of our ciphertext. The Matlab simulation tool is used in the analysis, and the key is generated based on the selected characters, taking into account the size of the message. As observed in the proposed algorithms, the number of message columns matches the size of other rows. During encryption, input characters are converted into numbers according to their positional arrangement. The positional arrangements of the characters are listed below and shown in Figure 2.



spc ! " # $ % & ' ( ) * + , - . /
0 1 2 3 4 5 6 7 8 9 A B C D E
F G H I J K L M N O P Q R S T
U V W X Y Z a b c d e f g h
i j k l m n o p q r s t u v
w x y z : ; < = > ? @] \ [
^ _ { | } ~ £ × ¿ ® ¬ ½ ¼ ¡
« » " " „ ¤ © ™ ¦ ¢ ¥ € … ‰
• ¯ ´ ± ¾ ¶ § ÷ ¸ ° ¨ · ¹ ³ ² œ
µ ž Å Æ þ À Á Â Ã

Fig. 2 The positional arrangements of the characters
Key matrix generation

The original and a new algorithm have the same square key matrix (Ksxs). The new modified algorithms have their encryption techniques, which is select key random one-time, 'E (k, P) = Ct = (K1sxs * Psxq + ((K2qxs)t + K3)) mod N' where N=141, Ct is total ciphertext, (K2qxs)t is the second key matrix transposition to increase complexity and decrease risk.

METBSIUEHCAbOTPKG encryption and decryption algorithm with key generation:

In this algorithm procedure, the first step involves the utilization of the modified Hill Cipher

- Modulus N
- Generate random key one-time pad character as input from 141 key space
- Change characters into positional integer number as a key in the form of nXn matrix
- The key which is (k1,k2)
- Encrypt original text from sender side (E(k, P) = Ct = (K1sxs*Psxq+(K2qxs)t) mod N
- Compute inverse key k1sxs = 1/| k1sxs |, where,| k1sxs | is determinant of key
- Hence, the receiver decrypts using the generated private key (p-) the same size as the sender encryption key(Ksxs).
- Our private key is k1sxs and k2qxs
- Decrypt the ciphertext from the recipient (D(C,K) = Psxq = k1sxs-(Ct - (K2qxs)t) mod N.

To prove an algorithm based on encryption and decryption, substitute the encryption formula into the decryption formula.

C = p*k1 + (K2) mod N

For decryption:

P = K1-* (C – (K2)) mod N

Substituting C into P:

P = K1-* ((p*k1 + (K2) mod N) - (K2)) mod N

Applying the minus sign using the body mass rule:

P = K1-* (p*k1 + K2) mod N – K2 mod N) mod N

Using the properties of module:

(a - b) mod n = (a mod n – b mod n)

Therefore:

P = K1-* (p*k1 + K2 – K2) mod N

The positive and negative addition cancel each other.

3. RESULTS AND DISCUSSION

For Encryption Process:

In our algorithm, Abe wants to send money to Kebe, he uses two private keys (k1, K2).

(Ct= (K1sxs*Psxq + ((K2qxs)t+) mod N'),

Where: Ct is a total cipher, (K2qxs) t is the second key Transpose

P= 50000$, K1 =? DN±, K2 = (K#, WQ the number of position characters from 141.

P (5=21, 0 =16, $ = 4 and K1 (? = 83, D = 29, N = 39, ± = 119,

k2((= 9, k = 36, # =3 , W= 48, Q= 42.

Based on the given positional number arrangement in the form of a matrix (p, k1, K2).

The plain text block arranged in the row and columns with key, then the random generated key of the column equal with the row of plaintext.

$$P = \begin{bmatrix} 21 & 16 & 16 \\ 16 & 16 & 4 \end{bmatrix}, \quad k_1 = \begin{bmatrix} 83 & 29 \\ 39 & 119 \end{bmatrix}, \quad k_2 = \begin{bmatrix} 9 & 12 \\ 36 & 48 \\ 3 & 42 \end{bmatrix}$$

In the algorithm, when Abe wants to send money to Kebe, he utilizes two private keys (k1, K2). The ciphertext (Ct) is obtained by encrypting the text using the key:

Ct = (K1sxs*Psxq + (K2qxs)t) mod N'

Where: N = 141. Here, the key matrix (k2) is transposed to match the dimensions of the rows and columns for adding the text during the first encryption step.

K2 =

$$(K\#, WQ = \begin{bmatrix} 9 & 36 & 3 \\ 12 & 48 & 42 \end{bmatrix}$$

$$Ct = (\begin{bmatrix} 83 & 29 \\ 39 & 119 \end{bmatrix} * \begin{bmatrix} 21 & 16 & 16 \\ 16 & 16 & 4 \end{bmatrix} + (\begin{bmatrix} 9 & 36 & 3 \\ 12 & 48 & 42 \end{bmatrix}) \bmod 141$$

First multiply 'P' with 'k1' and added k2t.

let A= K1sxs*Psxq =

$$\begin{bmatrix} 83*21+29*16 & 83*16+29*16 & 83*16+29*4 \\ 39*21+119*16 & 39*16+119*16 & 39*16+119*4 \end{bmatrix} = \begin{bmatrix} 2207 & 1792 & 1444 \\ 2723 & 2528 & 1100 \end{bmatrix}$$

Let B= $(K_{2qxs})^t$+= $\begin{bmatrix} 9 & 36 & 3 \\ 12 & 48 & 42 \end{bmatrix}$= then Ct=A+B mod 141

$$=(\begin{bmatrix} 2207 & 1792 & 1444 \\ 2723 & 2528 & 1100 \end{bmatrix} + \begin{bmatrix} 9 & 36 & 3 \\ 12 & 48 & 42 \end{bmatrix} =) \bmod 141 = \begin{bmatrix} 2216 & 1828 & 1447 \\ 2735 & 2576 & 1142 \end{bmatrix} \bmod 1411$$

$Ct = \begin{bmatrix} 101 & 136 & 37 \\ 56 & 38 & 14 \end{bmatrix}$ = ¡þLem. , the ciphertext is more substitute and transposition,

For decryption process

As mentioned earlier, Abe and Kebe use the same private key. Therefore, Abe encrypted the message and sent the ciphertext to Kebe. Kebe then decrypted the ciphertext using the same private key as Abe, following the formula:

P = K1sxs-(Ct- ((K2qxs)t)) mod 141).

Since

$$K1 = \begin{bmatrix} 83 & 29 \\ 39 & 119 \end{bmatrix}, \quad k2 = \begin{bmatrix} 9 & 12 \\ 36 & 48 \\ 3 & 42 \end{bmatrix}, \text{ and } Ct = \begin{bmatrix} 101 & 136 & 37 \\ 56 & 38 & 14 \end{bmatrix}$$

Find, the transpose of

k_2. $K_2 = \begin{bmatrix} 9 & 36 & 3 \\ 12 & 48 & 42 \end{bmatrix}$. Then, calculate plain text

$$P = \begin{bmatrix} 83 & 29 \\ 39 & 119 \end{bmatrix}^{-*} (\begin{bmatrix} 101 & 136 & 37 \\ 56 & 38 & 14 \end{bmatrix} - \begin{bmatrix} 9 & 36 & 3 \\ 12 & 48 & 42 \end{bmatrix}) \bmod 141$$

Using body mass rule, multiplied by a negative sign with k2t.

$$= \begin{bmatrix} 83 & 29 \\ 39 & 119 \end{bmatrix}^{-*} \begin{bmatrix} 92 & 100 & 34 \\ 44 & -10 & -28 \end{bmatrix} \bmod 141 = \begin{bmatrix} 83 & 29 \\ 39 & 119 \end{bmatrix}^{-*} \begin{bmatrix} 92 & 100 & 34 \\ 44 & 131 & 113 \end{bmatrix} \bmod 141$$

Second, we find the inverse of k1 using the determinant and adjoint.

K1- =1|𝑘1| *adj(k1)mod 141, the determinant of |k1| =83*119 – 39*29 = 9877 -1138 =8746 and adj of k1 using mathematical matrix

$adj(k1) = \begin{bmatrix} 119 & -29 \\ -39 & 83 \end{bmatrix}$. , Then, multiply with determinant.

$$K1^{-} = \frac{1}{|8746|} * \begin{bmatrix} 119 & -29 \\ -39 & 83 \end{bmatrix} \bmod 141 = \frac{1}{|8746|} * \begin{bmatrix} 119 & 112 \\ 102 & 83 \end{bmatrix} mod141.$$

The multiplicative inverse of (8746)- using Euclidean algorithm is 106 and all negative numbers change into a positive integer by modulo 141.

$$\bmod 141 = \begin{bmatrix} 65 & 28 \\ 96 & 56 \end{bmatrix}. \text{ So, } K_{1}^{-} = \begin{bmatrix} 65 & 28 \\ 96 & 56 \end{bmatrix}$$

Now, the key inverse is multiplied with the ciphertext.

$$P = \begin{bmatrix} 65 & 28 \\ 96 & 56 \end{bmatrix} * \begin{bmatrix} 101 & 136 & 37 \\ 56 & 38 & 14 \end{bmatrix} \text{mod}141 = \begin{bmatrix} 21 & 16 & 16 \\ 16 & 16 & 4 \end{bmatrix} = 50000\$$$

The encryption and decryption process involves additional substitutions and transpositions, which improve the performance metric of confusion diffusion, leading to an avalanche effect. The avalanche effect is a property in cryptography that reflects the cryptographic strength of an algorithm, characterized by diffusion and confusion [1]. If an attacker possesses knowledge about the statistical characteristics of the plaintext, such as the frequency distribution of Tele Birr transactions, cryptanalysis becomes relatively straightforward. In such cases, the known statistics can be observed in the ciphertext, allowing the cryptanalyst to deduce the secret or a portion of it. The general formula used to calculate the avalanche effect is as follows:

$$\text{Avalanche effect} = \frac{\text{Number of changed bits}}{\text{The total message of bit}} * 100, \quad ---- (1)$$

For instance, the TEHCMUVH algorithm in the EHCAAEaOTPKGT utilized a 4x4 matrix key for block messages, while the GoKMFHCEUCC algorithm employed a 5x5 matrix key for the five-block message. The message "AHMZTAOULIOU" was presented in Table 1 and analyzed in Figure 3.

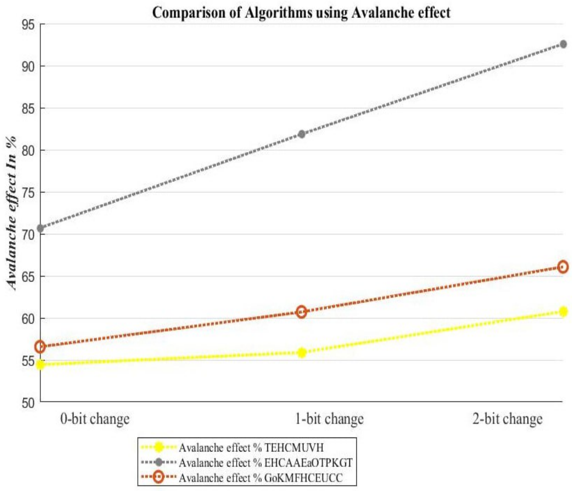


Fig. 3 Avalanche effect comparison of algorithms

Out of three algorithms presented, a new one with a large avalanche effect is proposed, and the other two algorithms "Text encryption: Hybrid cryptographic method using Vigenere and Hillciphers" (TEHCMUVH) and "Generation of key matrix for Hillcipher encryption using classical cipher",(GokMFHCEUCC) are comparable papers to the new work. The algorithm strength of new paper is better than the other two papers.

Table 1. Avalanche simply small change degree of input (plaintext or secret key) the output significantly

Plaintext (alphabet) Input TEHCMUVH EHCAAEaOTPKGT,GokMFHCEUCC	Ciphertext			Avalanche %		
	TEHCMUVH	EHCAAEaOTPKGT	okMFHCEUCC	TEHCMUVH	EHCAAEaOTPKGT	GokMFHCE UCC
HAMZATOUIU (0-bit change)	HRZZGCBQW	iHA/ ¢§,,j •⟶∼	CSQMBDWDLVZEJX	54.44	70.7	56.57
HAMZATOUILOU (1-bit change)	RFPDSOCVUI	±&'⁄p |1§\ xP/c	OHXOXNTOSTLOWER	55.9	81.85	60.71
HAMZATOUILOU (2-bit change)	XOHIQTSEARQY	Oudb ‰'}¹ ½+♦¿	OUKBKSMODQJVEMO	60.77	92.57	66.07

The measurement of the avalanche effect has been conducted using Hamming distance. In information theory, Hamming distance is utilized as a metric of dissimilarity, quantifying the number of differing characters or different bits between two strings or numbers of equal length. This metric is straightforward to implement programmatically and is indicative of a high level of diffusion and confusion [43-45].

For the TEHCMUVH algorithm, the avalanche effect is measured as 54.44% for 0-bit change, 55.9% for 1-bit change, and 60.77% for 2-bit change.

For the EHCAAEaOTPKGT algorithm, the avalanche effect is measured as 70.7% for 0-bit change, 81.85% for 1-bit change, and 92.57% for 2-bit change.

For the GoKMFHCEUCC algorithm, the avalanche effect is measured as 56.57% for 0-bit change, 60.71% for 1-bit change, and 66.07% for 2-bit change.

3.1 Time complexity of algorithm

Considering the additional aspect of computational speed in this research, time complexity becomes an important factor in cryptographic work. In the case of matrix multiplication, we consider two matrices, L and M, with dimensions s x p and p x t, respectively. Let's examine these matrices:

$$N{=}LM{=}\begin{bmatrix} a11 & a12 & a13 & \dots & a1p \\ a21 & a22 & a32 & \dots & a2p \\ a31 & a32 & a33 & \dots & a3p \\ \dots & \dots & \dots & \dots & \dots \\ as1 & as2 & as3 & \dots & asp \end{bmatrix} . \begin{bmatrix} b11 & b12 & b13 & \dots & b1t \\ b21 & b22 & b32 & \dots & b2t \\ b31 & b32 & b33 & \dots & b3t \\ \dots & \dots & \dots & \dots & \dots \\ bp1 & bp2 & bp3 & \dots & bpt \end{bmatrix}$$

$$= \begin{bmatrix} b11 & b12 & b13 & \dots & b1t \\ b21 & b22 & b32 & \dots & b2t \\ b31 & b32 & b33 & \dots & b3t \\ \dots & \dots & \dots & \dots & \dots \\ bp1 & bp2 & bp3 & \dots & bpt \end{bmatrix}$$

Each entry, Nij, in the matrix N can be calculated by performing pairwise summation of the corresponding entries in the matrices L and M.

Nij = Σ *L pk*=1 *ik*Mkj =Li1M1j + . . . +LipMpj.

Table 2. Comparison variants of algorithm in big-O notation

S.NO	Algorithm	The time complexity of encryption and decryption in big-o notation
1	TEHCMUVH	$O(3n^2)$
2	EHCAAEaOTPKGT	$O(6(n^2\text{-}n))+ O(3n^2)$
3	GokMFHCE UCC	$O(3n^2) + O(2n^2)$

When analyzing the algorithm for matrix multiplication using three nested for loops, each cycle of the eternal loop results in the same number of runs within the internal loops as the length of the matrix. In general, if the matrix length is 'n', the total time complexity would be O(nnn) = O(n^3). In the Table 2, the total time complexity of the comparison algorithm is listed and it was analyzed in Figure 4.

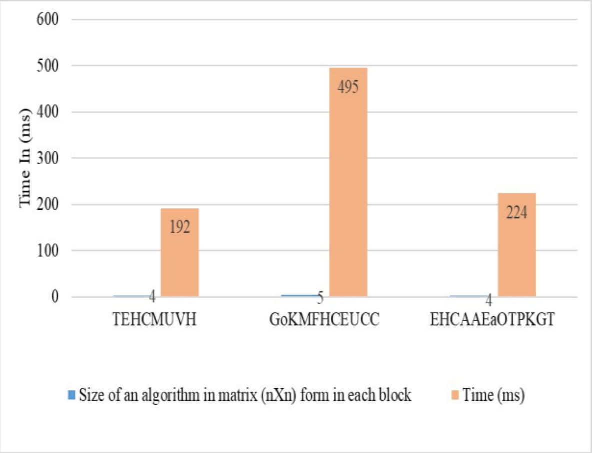


Fig. 4 Comparing the time complexity of different algo-rithms in terms of milliseconds

3.2 Memory consumption of algorithm

Table 3.Comparison of memory consumption in kilobytes for various algorithms

S.No	Algorithm	Memory consumption in kB
1	TEHCMUVH	9.242
2	EHCAAEaOTPKGT	11.478
3	GokMFHCE UCC	7.37

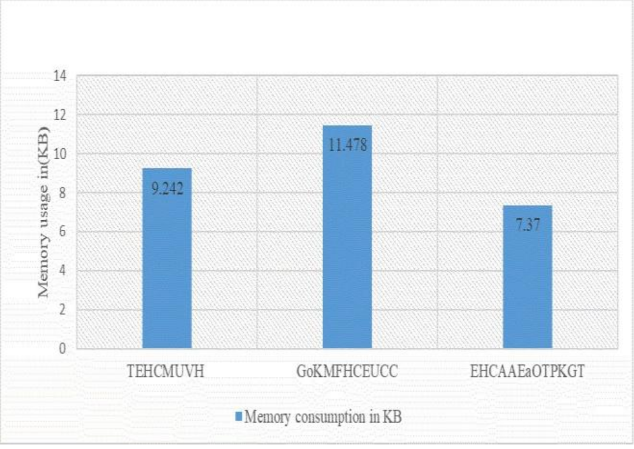


Fig. 5 Comparison of memory consumption for various algorithm

The memory consumption of an algorithm Table 3 refers to the amount of memory used during its execution. When analyzing or monitoring the memory consumption in a Matlab application, additional memory is allocated when new elements are added, and memory storage is kept contiguous by removing deleted elements. To display the utilized memory in our Matlab code, it can be utilized the "whos" command. Matlab allocates memory in bytes, with the byte class represented by double (8 bytes) and ASCII characters (1 byte) at the end of execution. It was illustrate in Figure 5. To convert the memory data consumption into kilobytes (1 KB = 1000 bytes), it can perform the conversion. To calculate the total memory usage in our code, the "memory" command can be used.

4. CONCLUSION

With the advancement of technology, there is a growing global concern regarding information security. This concern is particularly significant in developing countries like Ethiopia, which have a rich history and abundant resources. In an effort to strengthen their information security infrastructure, Ethiopia has adopted mobile money transfer systems such as Tele Birr. To enhance the protection of financial transactions and other transferred information, the EHCAAEaOTPKGT algorithm has been developed as an additional security measure.

REFERENCES

[1] R.Jessie Paragas and M.Ariel Sison,"Hill cipher modification: A simplified approach", Institute of Electrical and Electronics Engineers, 2019.

[2] Muneer Bani Yassein, Shadi Aljawarneh and Ethar Qawasmeh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms", Institute of Electrical and Electronics Engineers, 2017.

[3] Vemulapalli Rajesh and V.Panchami "A novel multiplicative substitution cryptosystem", Institute of Electrical and Electronics Engineers.2016.

[4] Umang Bhargava and Raghav Chawla, "A new algorithm combining substitution and transposition cipher techniques for secure communication", 2017, Institute of Electrical and Electronics Engineers.

[5] Akbar Serdano, Muhammad Zarlis, Erna Budhiarti Nababan , “Performance of combining hillcipher algorithm and caesar cipher algorithm in text security”, Institute of Electrical and Electronics Engineers, 2021.

[6] K.Mani1 and R.Mahendran, "Generation of key matrix for hillcipher encryption using classical cipher", Institute of Electrical and Electronics Engineers, 2017.

[7] Hamza Touil, Nabil El Akkad and Khalid Satori, "Text encryption: Hybrid cryptographic method using vigenere and hillciphers", Institute of Electrical and Electronics Engineers, Nov 2020.

[8] Deepanshu Gautam and Chandan Agrawal, "An enhanced cipher technique using vigenere and modified caesar cipher", Institute of Electrical and Electronics Engineers, Sep 2020.

[9] Shariqua Izhar, Anchal Kaushal, Ramsha Fatima, Mohammed A. Qadeer, " Enhancement in data security using cryptography and compression", Institute of Electrical and Electronics Engineers, 2017.

[10] Yuan Zhang, Chunxiang Xu, Jianbing Ni, "blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage", Institute of Electrical and Electronics Engineers, 2019.

[11] R.Ainur Zamanov, Vladimir Erokhin, S.Pavel Fedotov, "ASIC-resistant hash, functions", Institute of Electrical and Electronics Engineers, 2018.

[12] Z.Maricel Grace Fernando1, M.Ariel Sison and P.Ruji Medina1, "Securing Private Key using New Transposition Cipher Technique", 2019, Institute of Electrical and Electronics Engineers, 2019.

[13] Abid Murtaza, Syed Jahanzeb Hussain Pirzada, Liu Jianwei, "A new symmetric key encryption algorithm with higher performance", Institute of Electrical and Electronics Engineers, 2019.

[14] Muhammad Donni Lesmana Siahaan, Andysah Putera Utama Siahaan, "Application of hill cipher algorithm in securing text messages", springer, 2018.

[15] Nurhayati, Abdul Meizar, and Frinto Tambunan, 4th Erwin Ginting, "Optimizing the complexity of time in the process of multiplying matrices in the hill cipher algorithm using the strassen algorithm", Institute of Electrical and Electronics Engineers, May 2020.

[16] Sumarsono, Muhammad Anshari, Amiroh Mujahidah, "Expending technique cryptography for plaintext messages by modifying playfair cipher algorithm with matrix 5 x 19", Institute of Electrical and Electronics Engineers, 2019.

[17] R.Jessie Paragas, M.Ariel Sison, Ruji and P. Medina "An improved hill cipher algorithm using cbc and hexadecimal S-box", Institute of Electrical and Electronics Engineers,2019.

[18] Mikha Dayan Sinaga, Nita Sari Br Sembiring, Frinto Tambunan and Charles Jhony Mantho Sianturi, "Hybrid cryptography WAKE and binary caesar cipher method for data security", Institute of Electrical and Electronics Engineers, 2018.

[19] Budi Triandi, Evri Ekadiansyah, Ratih Puspasari, Lili Tanti Iwan and Fitrianto Rahmad, "Improve security algorithm cryptography vigenere cipher using chaos functions",2018, Institute of Electrical and Electronics Engineers, 2018.

[20] C.Arnold Licayan, D.Bobby Gerardo and A.Alexander Hernandez, "Enhancing playfair cipher using seed based color substitution", Institute of Electrical and Electronics Engineers, 2020.

[21] D. Rachmawati, M. A. Budiman, "New approach toward data hiding by using affine cipher and least significant bit algorithm", Institute of Electrical and Electronics Engineers, 2017.

[22] R.Rajagopal , K.Kannan , N.Nimitha, J.Gurumurthy , R. Subatra and M.Babu, “Security attacks on the improved SMS4-bsk encryption transmission system”, ,Institute of Electrical and Electronics Engineers, 2021.

[23] Tun Myat Aung and Ni Ni Hla, "A complex polyalphabetic cipher technique myanmar polyalphabetic cipher", Institute of Electrical and Electronics Engineers, 2019.

[24] Vike Maylana Putrie, Christy Atika Sari and De Rosal Ignatius Moses Setiadi, "Super encryption using transposition-hill cipher for digital color image", Institute of Electrical and Electronics Engineers, 2018.

[25] Patience Mpofu, Colin Chibaya and Taurayi Rupere, "A hybrid RSA-DH cipher for signed encrypted messages", Institute of Electrical and Electronics Engineers, 2020.

[26] S.Joseph Gladwin and Pasumarthi Lakshmi Gowthami, "Combined cryptography and steganography for enhanced security in suboptimal images", Institute of Electrical and Electronics Engineers, 2020.

[27] Vadlamudi Naveen Kumar and N. Ravi Shankar, "Cryptanalysis of a new cryptosystem of color image using a dynamic-chaos hill cipher algorithm: A chosen ciphertext attack", Springer, 2020.

[28] Sanjay Kumar, "Securing data at rest using hill cipher and XOR-based operations", Institute of Electrical and Electronics Engineers, 2018.

[29] Vishwa Nageshwar and N. Ravi Shankar, "Cryptanalysis of modification in hill cipher for cryptographic application", Springer, 2020.

[30] Adyasha Behera, Alakananda Tripathy, Alok Ranjan Tripathy, and Smita Rath, "Random invertible key matrix decomposition for classical cryptography", Springer, 2020.

[31] B.Bazeer Ahamed and Murugan Krishnamoorthy, "SMS encryption and decryption using modified vigenere cipher algorithm", Springer, 2020.

[32] S.K.Naveenkumar, H.T.Panduranga and Kiran, "Chaos and hill cipher based image encryption for mammography images", Springer, 2016.

[33] Pankaj Kumar Keserwani and Mahesh Chandra Govil, "A hybrid symmetric key cryptography method to provide secure data transmission", 2020, springer, 2020.

[34] Ritu, Niram, Ekta Narwal and Sumeet Gill, “A novel cipher technique using substitution and transposition methods”, Springer, 2022.

[35] Ni Ni Hla, Tun Myat Aung, "Computing and analysis of residue matrices over complex plane for cryptographic applications", Institute of Electrical and Electronics Engineers, 2020.

[36] Saad Almutairi, S.Manimurugan and Majed Aborokbah, "A new secure transmission scheme between senders and receivers using HVCHC without any loss", Springer, 2019.

[37] E.Froilan De Guzman and D.Bobby, "Gerardo implementation of enhanced secure hash algorithm towards a secured web portal", Institute of Electrical and Electronics Engineers, 2019.

[38] Padmapriya Praveenkumar, Rengarajan Amirtharajan, "Fusion of confusion and diffusion: A novel image encryption approach", Springer, 2017.

[39] Shahram Khazaei and SiavashAhmadi, "Ciphertext-only attack on d ×d Hill in O (d13^d), Elsevier 39, 2016.

[40] Khawaja Muhammad Ali and Majid Khan, "A new construction of confusion component of block ciphers", Springer, 2019.

[41] Manmohan Lakhera, MMS Rauthan and Amit Agarwal, "Securing biometric template using double hill cipher with self-invertible key and random permutation of pixels locations", Institute of Electrical and Electronics Engineers, 2016.

[42] Mohamed Jarjar and Said NAJAH, "Further improvement of the HILL method applied in image encryption", Institute of Electrical and Electronics Engineers, May 2020.

[43] Nguyen Thi Thu Nga and Hoang Duc Tho, "On the improving diffusion layer and performance of AES algorithm", Institute of Electrical and Electronics Engineers, 2017.

[44] Min Zhao E and Yang Geng, "Homomorphic encryption technology for cloud computing", Elsevier, 2019.

[45] A.M.Ashraf Khalaf, S.Mona Abd El-Karim, and F.A.Hesham Hamed, "A triple hill cipher algorithm proposed to increase the security of encrypted binary data and its implementation using FPGA", vol.5, issue 1, Institute of Electrical and Electronics Engineers, Jan 2016.