JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol-6, Special Issue-4, May 2018 E-ISSN: 2347-2693

Cryptosystem using Chaotic Shuffling Hill pad Encryption Scheme for Secure Data Transmission

T. Jaison Vimalraj[1*], P. Mithun[2], K. Mathiyarasu[3]

[1*, 2, 3]Information Technology, University College of Engineering -BIT Campus, Anna University, Trichy, India

*Corresponding Author: jaison.vimal@gmail.com, Tel.: +91-7373252194

Available online at: www.ijcseonline.org

***Abstract* ---** Maintaining privacy and security of any data, specifically for images that are transmitted through network is a major issue in today's world. In this paper, a new three level Chaotic Shuffling Hill Pad encryption (CSHP) scheme is proposed. In first level encryption, the input image is subdivided and shuffled using chaotic algorithm. In second level, the shuffled blocks are encrypted using subset Hill algorithm with different product keys. Third level encryption is performed with the basis of Onetime pad encryption algorithm, in order to tighten the security of the image. Finally, the encrypted image is converted to text file, which is the intended cipher format. Product keys are chosen in such a way that they are invertible. The encrypted text file transmitted through insecure channel can be decrypted at the receiver's end. The proposed method is tested with various standard images and the results are encouraging. The proposed method finds its application in Defence field.

***Keywords*---** Chaotic, Cryptosystem, Encryption, Decryption

I. INTRODUCTION

Cryptography is one of the key fields in the present technological era. It is a surreptitious writing, which is composed of principles and methodologies for transforming evident message into unintelligent and back to evident form. Recently chaos based algorithms are becoming popular due to its intrinsic features. Conversion of plain text to cipher text and cipher text to plain text is done alternatively in cryptography using various levels of substitution and transposition techniques. Encryption of image in spatial domain increases the efficiency of the proposed method and avoids additional effort. Onetime pad is an algorithm for message encryption based on randomness and variant key encryption. Usage of onetime pad is insisted since the algorithm cannot be cracked. Remaining sections of the paper are aligned as follows. Section II presents a study on the relevant literatures for the proposed scheme followed by the theoretical background for Hill cipher and Onetime pad encryption in Section III. Section IV explains the architectural framework followed by explanation of the proposed scheme in section V. Experiments and the results of the proposed system is presented in section VI. Section VII presents the conclusion and future scopes of the proposed cryptosystem.

II. LITERATURE SURVEY

In recent years, usage of chaotic algorithms is increased due to its features [2, 10]. In [8], a hyper chaotic systematic approach is suggested for image encryption and decryption. Chaotic algorithm is well implemented using shuffling of blocks or pixels [7]. Usage of classical encryption algorithms lightens the

computational work. Implementation of Hill cipher with invertible product key for encryption of images in discussed in [3]. Some other technical encryption using Hill cipher is presented in [1, 7]. Encryption using Hill cipher focuses a problem during key exchange between sender and receiver. By modifying the traditional Hill cipher by extending its complexity with other encryption algorithms is advisory for efficient encryption. Onetime pad, which is said to unbreakable, can be used as a combination for Hill cipher. Basic usage and various encryptions using Onetime pad is discussed in [5, 6]. The basic ideology for Hill cipher and one time pad is discussed in the next section.

III. BASIS OF PROPOSED METHODOLOGY

A. HILL CIPHER ALGORITHM

Hill cipher is symmetric block cipher technique proposed by mathematician Leser Hill in 1929.This encryption algorithm takes m successive plaintext letters and substitutes for them m cipher text letters.

The substitution is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1, c, z=25). For m = 2, the system can be described as

$$C1 = (K11P1 + K21P2) \bmod 26$$
$$C2 = (K12P1 + K22P2) \bmod 26$$

This can be expressed in terms of row vectors and matrices:

$$(C1C2) = \quad (P1\ P2) \quad \begin{pmatrix} K11 & K12 \\ K21 & K22 \end{pmatrix} \text{Mod } 26$$

Or

$$C = PK \bmod 26$$

Decryption requires using the inverse of the matrix K. It is easily seen that if the matrix K-1 is applied to the cipher text, then the plaintext is recovered.

In general, terms, the Hill system can be expressed as

$$\mathbf{C} = \mathrm{E}\,(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$$

$$\mathbf{P} = \mathrm{D}\,(\mathbf{K}, \mathbf{C}) = \mathbf{CK}\text{-}1 \bmod 26 = \mathbf{PKK}\text{-}1 = \mathbf{P}$$

B. *ONE TIME PAD ENCRYPTION ALGORITHM*

The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plaintext and has no statistical relationship to it. An AT&T engineer named Gilbert Vernam in 1918 introduced such a system. His system works on binary data (bits) rather than letters. The system can be expressed succinctly as follows

$$ci = pi \oplus ki$$

where,

$pi = i^{th}$ binary digit of plaintext
$ki = i^{th}$ binary digit of key
$ci = i^{th}$ binary digit of cipher text
$\oplus$ = Exclusive - OR (XOR) operation

Thus, the cipher text is generated by performing the bitwise XOR of the plaintext and the key. Because of the properties of the XOR, decryption simply involves the same bitwise operation: $pi = ci \oplus ki$. The essence of this technique is the means of construction of the key. Vernam proposed the use of a running loop of tape that eventually repeated the key, so that in fact the system worked with a very long but repeating keyword. Although such a scheme, with a long key, presents formidable cryptanalytic difficulties, it can be broken with sufficient cipher text, the use of known or probable plaintext sequences, or both.

One-Time Pad: An Army Signal Corp officer, Joseph Mauborgne, proposed an improvement to the Vernam cipher that yields the ultimate in security. Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded. Each new message requires a new key of the same length as the new message. Such a scheme, known as a one-time pad, is unbreakable. It produces random output that bears no statistical relationship to the plaintext. Because the cipher text contains no information whatsoever about the plaintext, there is simply no way to break the code.

The security of the one-time pad is entirely due to the randomness of the key. If the stream of characters that constitute the key is truly random, then the stream of characters that constitute the cipher text will be truly random. Thus, there are no patterns or regularities that a cryptanalyst can use to attack the cipher text.

IV. ARCHITECTURAL REPRESENTATION

In this section, this architecture for the proposed chaotic shuffling Hill pad encryption is presented. The image, which is to be encrypted by the cryptosystem, is fed as input. Encrypted image at each stage is provided as intermediate results. Encrypted text file format after three level encryption serves as the required output of the system.

Transmitting the image as a text file provides added advantage, which raises a confusion wall for intruders and hackers. The encrypted file can be decrypted by performing the inverse with corresponding key inverse and recombination. The scheme is elaborated in next section.

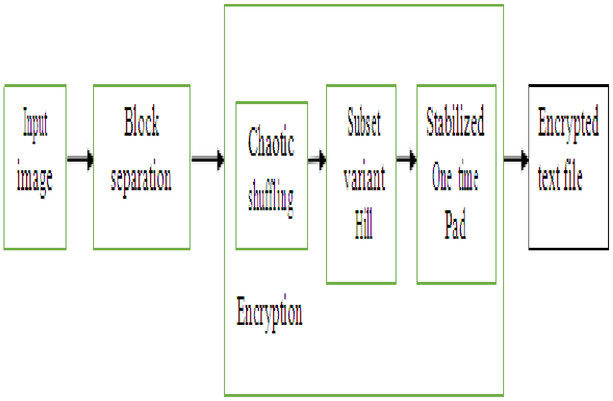

Fig. 1 CSHP Encryption scheme

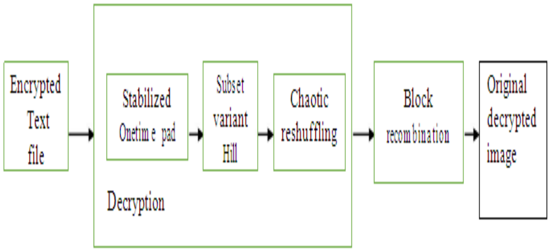

Fig. 2 CSHP Decryption scheme

V. CHAOTIC SHUFFLING HILL PAD (CSHP) ENCRYPTION SCHEME

A. Block separation

An image of size (256 x 256) is taken as input and the pixel values are extracted. Since the scheme implementation is to be carried out in spatial domain, any sort of preprocessing is not advisory. The pixel values are divided into small blocks of size (2 x 2). Block separation can be varied with size on requirement under toilsome circumstances.

B. CSHP scheme

After block separation, the blocks are shuffled randomly. A block is taken for processing and scanned based on its positionality as even or odd. The shuffling procedure is presented in *Figure 3*.A linear swapping is performed to swap the blocks between even position and odd position. Now the entire image is divided into I1 and I2 based on their positionality after shuffling. Reconstruct the image with the shuffled pattern to find the first intermediate encrypted image.

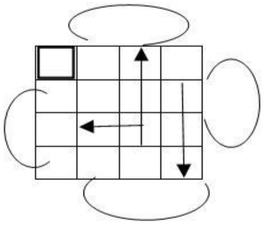

Fig. 3 Random Shuffling based on Positionality

In level two encryption, the classified blocks I1 and I2 and encrypted using Hill Cipher algorithm with different product keys, which are self-invertible.

Usage of different product keys helps in enhancing the security. Cracking of one product key may not help at any cost for decrypting the original image. The image is reconstructed with the obtained encrypted values and found with no matching patterns of the original image that is the second intermediary result of the proposed encryption scheme. For the third level of encryption, binary values of the encrypted decimal values are provided as input after the prominent decimal to binary operation. The binary values are XORed with the traditional XOR scheme's product key, which may also include the binary format of alphabets and symbols or special characters. Onetime pad algorithm does not involve with complex operations that challenge the computational speed of some relatively small processors.

$$C1 = [I1 \text{ x } I2] \bmod 256$$

$$= \begin{pmatrix} I_{11} & I_{12} \\ I_{21} & I_{22} \end{pmatrix} \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix} \bmod 256$$

$$C2= [I2 \text{ x } K2] \bmod 256$$

$$= \begin{pmatrix} I_{13} & I_{14} \\ I_{23} & I_{24} \end{pmatrix} \begin{pmatrix} K_{13} & K_{14} \\ K_{23} & K_{24} \end{pmatrix} \bmod 256$$

The final encrypted values are converted to decimal values and are converted to text file format after ASCII recombination. This conversion of image into text file adds additional advantage by reducing the assumption probability. The encrypted text file can be transmitted over unsecure channels and can be decrypted at the receiver's and Decryption is the reverse engineering of the encryption process with the inverse keys. Onetime pad decryption is carried out first at the receiver's end followed by subset variant Hill decryption and Reshuffling. Reshuffling is done by swapping between the positional values of the blocks from odd to even and even to odd respectively. Finally, the blocks are recombined and the original image is reconstructed. The proposed scheme finds its immense usage in defence field was secret messages and signals are passed as image. A simplified algorithm for the scheme can be presented as follows:

C. Encryption

```
Input - Input image
Output- Encrypted text file
Step1: Begin
Step2: Input image
Step3: Sub divides the image into blocks of size (2n)
Step4: Shuffle the blocks based on its positionality and perform a linear swap between even and odd
Step5: Perform subset variant Hill encryption as mentioned in section V
Step6: Perform Onetime pad binary encryption
Step7: Convert into text file with ASCII recombination
Step8: Transmit the file
Step9: End
```

II. Decryption

```
Input- Input Encrypted Text file
Output- Decrypted image
Step1: Begin
Step2: Reconvert text file to integer values by ASCII conversion
Step3: Perform Onetime pad decryption over the binary values
Step4: Perform subset variant Hill cipher decryption
Step5: Reshuffling the blocks based on its positionality and swaps them between even and odd
Step6: Recombining the block and construct the image
Step7: End
```

VI. EXPERIMENTAL RESULTS

The proposed cryptosystem is based over standard benchmark images and compared with existing conventional schemes. As a sample Lena image Fig. 4 (a) of size (256 x 256) is taken as input and its blocks are separated. At first, the Chaotic shuffling is carried out followed by variant Hill cipher encryption in level 2. The intermediary output of the second level is presented in Fig. 4 (b). At level three, One time pad encryption is performed and its corresponding output is shown in Fig. 4 (c). The final text file format of the encryption stage is presented in Fig. 4 (d). In the decryption phase, the exact reverse is performed using the inverse product keys and the decrypted original image is presented in Fig. 4 (e). The results of the proposed Chaotic shuffling Hill pad scheme is encouraging.

The time taken to perform the encryption and decryption using this proposed method is also calculated and compared with various existing schemes, which is tabulated in *table 1*. From the tabulation, it is evident that the proposed method is time efficient.

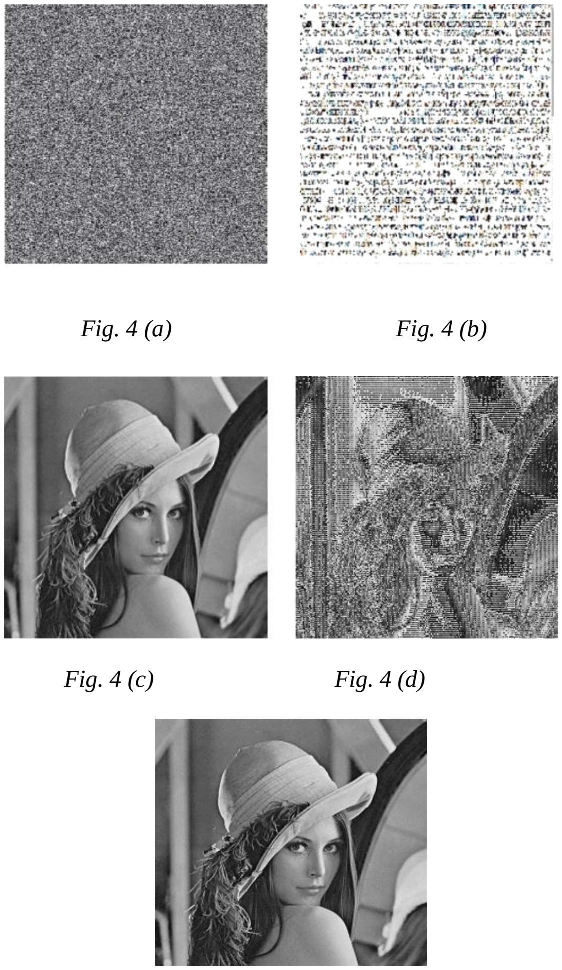

Fig. 4 (a) *Fig. 4 (b)*

Fig. 4 (c) *Fig. 4 (d)*

Fig. 4 (e)

Fig. 4 (a) input image, 4(b) level 1 encrypted image, 4 (c) level 2 encrypted image, 4 (d) expected encrypted text file as image, 4 (e) Decrypted image

Table 1. Time comparison among various schemes in terms of seconds

Image size	[4]	[9]	Proposed method
256x256	1.345	3.723	1.106
512 x 512	2.504	6.545	1.527
1024x1024	10.258	26.688	2.204

VII. CONCLUSION

In this paper, a new cryptosystem for image encryption using Chaotic shuffling Hill pad scheme is proposed. The usage of Chaotic scheme is encouraged due to its ergodicity, sensitivity, and system parameters. Onetime pad encryption, which is considered unbreakable, tightens the security further during transmission. Thus, the system saturates the need of the present technological era. The work has further scope of extension over color image and audio files.

REFERENCES

[1] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "*Image Encryption Using Advanced Hill Cipher Algorithm*", ACEEE International Journal on Signal and Image Processing Vol .1, No. 1, pp.37-41, 2010.

[2] J.S. Armand EyebeFouda, J. Yves Effa, Samrat L. Sabat, and Maaruf Ali, "A *Fast chaotic block cipher for image encryption*", Commun Nonlinear Sci Numer Simulat 19 pp. 578- 588, 2014.

[3] K. Mani, M. Viswambari "*Generation of Key Matrix for Hill Cipher using Magic Rectangle*", Advances in Computational Sciences and Technology ISSN 0973-6107 Vol. 10, No. 5 pp.1081-1090, 2017.

[4] Tang Z, Zhang X, "*Secure image encryption without size limitation using Arnold transform and Random strategies"*, Journal of Multimedia, Vol 6, No. 2, pp. 202–206, 2011.

[5] Timothy E. Lindquist, Mohamed Diarra, and Bruce R. Millard, "*A Java Cryptography Service Provider Implementing One-Time Pad*", 37th Hawaii International Conference on System Sciences, pp. 1-6, 2004.

[6] Yaqeen S. Mezaal, Dalal A. Hammood, Mohammed H. Ali, "*OTP Encryption Enhancement Based on Logical Operations*", IEEE ISBN: 978-1-4673-7504-7, pp.109-112, 2016.

[7] Prerna, Urooj, Meenakumari, Jitendra Nathshrivastava, "*Image Encryption and Decryption using Modified Hill Cipher Technique*", International Journal of Information & Computation Technology. ISSN 0974-2239 Vol. 4, No. 17 pp. 1895-1901, 2014.

[8] Zhenjun Tang &Xianquan Zhang & Weiwei Lan, "Efficient *image encryption with block shuffling and chaotic map*" Multimed Tools Appl, New York, 2014.

[9] Zhang G, Liu Q, "*A novel image encryption method based on total shuffling scheme*" Optics Communication, pp. 2775–2780, 2011.

[10] Zhang Yong, "*A Chaotic System Based Image Encryption Scheme with Identical Encryption and Decryption Algorithm*" Chinese Journal of Electronics, Vol.26, No.5, Sept. 2017.

Authors Profile

Mr. T. Jaison Vimalraj was born in Tiruchirappalli, India, in 1989. He received the B.E. degree from Karunya University, Coimbatore, India. in 2010 and the M.E degree from Dhanalakshmi Srinivasan College of Engineering, Perambalur, India, in 2012. He worked as Assistant Professor in Meenakshi Ramaswamy Engineering College, Ariyalur during 2012-2013 and in Roever Engineering College in 2014**.** Currently he is working as teaching faculty in Anna University-BIT campus, Tiruchirappalli, India since 2014. He has published a book in Computer Networks in 2013. He has published 5 research papers in International conferences and 4 papers in International Journals.

Mr. Mithun Palanimuthu was born in Madurai, Tamilnadu, India in 1996. He is persuing his B.Tech degree in the stream of Information Technology in Anna University-BIT campus, Tiruchirappalli, Tamilnadu, India.

Mr. Mathiyarasu Kulandhaisamy was born in Karur, Tamilnadu, India in 1997. He is persuing his B.Tech degree in the stream of Information Technology in Anna University-BIT campus, Tiruchirappalli, Tamilnadu, India.