4TH INTERNATIONAL CONFERENCE ON KNOWLEDGE & INNOVATION IN ENGINEERING, SCIENCE & TECHNOLOGY

21-23 December, 2018
Berlin - Germany

SECURITY ENHANCEMENT OF HILL CIPHER BY USING NON-SQUARE MATRIX APPROACH

M. Attique ur Rehman¹, Hasan Raza^{2,*} and Israr Akhter³

¹Virtual University, Lahore, Pakistan.

²Electrical Engineering Department, Hamdard University, Islamabad, Pakistan.

³Department of Computer Science, Air University, Islamabad, Pakistan.

Abstract

The conventional Hill cipher provides less information security due to fixed $N \times N$ key matrix dimensions. In this paper, a new modified Hill cipher is introduced which provides enhanced security performance than the conventional hill cipher scheme. This enhanced security of the modified Hill cipher is dependent on the non-square $N \times M$ matrix approach. The $N \times M$ Hill cipher matrix defuses N plaintext information letters into M cipher text messages. Therefore, the varying M redundant cipher text bestowed more confusion than the conventional Hill cipher. Moreover, the modified technique provides always non-singular matrix while finding its inverse which makes free from the complication of singular matrixes in the conventional Hill cipher scheme.

Keywords: Modified Hill cipher, non-square matrix, enhanced security performance.

4TH INTERNATIONAL CONFERENCE ON KNOWLEDGE & INNOVATION IN ENGINEERING, SCIENCE & TECHNOLOGY

21-23 December, 2018

Berlin - Germany

Introduction

The Hill cipher invented by Lester S. Hill in 1929 [1,2]. It is a poly-graphic substitution cipher which is based on linear algebraic technique [3]. In Hill cipher, the plain text consisted on l alphabets is composed of k blocks and each block having p elements. To compute the cipher text, the Hill cipher multiplies each block of plain text with the secret key of $N \times N$ square matrix. Therefore, the linear nature of secret key matrix, the Hill cipher is proved to be easily breakdown, i.e. the attacker can easily breakdown the secret key matrix by using one or more plaintexts messages and their consistent cipher texts [4]. In this regard, many modifications of the Hill cipher has been introduced in the literature [5,6,7,8,9,10,11] which make secure the Hill cipher from the cryptanalysis attack. Furthermore, some of these articles make the modification in Hill cipher by just combining it with the AES (advanced encryption standard) [12] which make the algorithm complex in sense of high computational complexity and as well as it provides an interlacing approach [13]. Moreover, the two most well-known versions of Hill cipher [9,10] have already been used in many real life applications such as Biometric based authentication [16], Image encryption in steganography [15], software copy protection [17] and cloud storage [14]. However, such versions may be vulnerable to cryptanalysis attacks in real situations [18, 19]. Furthermore, in [20], a detailed review on the existing modified versions of Hill cipher is introduced. In all of these techniques, the brute force over all possible secret key can easily apply which makes the algorithm insecure towards secret communication. In this paper, a modified version of Hill cipher is introduced. The modified Hill cipher uses the non-square matrix approach and makes the information more secure than the conventional methods that have been presented in the literature so far. The enhanced security of the modified Hill cipher is dependent on the non-square $N \times M$ matrix approach. The varying matrix size defuses N plaintext information letters into m cipher text messages which makes more confusion than the conventional Hill cipher technique. Moreover, the varying matrix size also provides a barrier towards brute force or known cipher text only attacks [21].

4TH INTERNATIONAL CONFERENCE ON KNOWLEDGE & INNOVATION IN ENGINEERING, SCIENCE & TECHNOLOGY

21-23 December, 2018

Berlin - Germany

Modified Hill Cipher Algorithm

The modified version of Hill cipher algorithm is dependent on the non-square matrix approach. Thus an $N \times M$ non-square key matrix K can be written as

$$K = \begin{bmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,m} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,m} \\ k_{3,1} & k_{3,2} & \cdots & k_{3,m} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n,1} & k_{n,2} & \cdots & k_{n,m} \end{bmatrix} \text{mod } 26$$

Where $k_{n,m}$ shows the matrix entity and is subscripted by $N \times M$ that shows the index number. The columns M of the non-square matrix are dependent on the block having p elements of the plain text letters while the rows N may extend as much as it can. Furthermore, the inverse of the non-square matrix K can be written as

$$K^{-1} = K(K^T K)^{-1} \text{mod } 26$$

where $K^T K$ provides the square $N \times N$ symmetric matrix which is always non-singular depending upon the condition that the elements of K are not the same.

The algorithm of modified Hill cipher is as follows:

- Select an $N \times M$ non-square as a key matrix
- Encryption:

M_i is the i^{th} plaintext block of size M

C_i is the i^{th} cipher text block of size N

$$C_i = M_i K \text{mod } 26$$

- Decryption

$$\text{Calculate } K^{-1} = K(K^T K)^{-1} \text{mod } 26$$

$$M_i = C_i K^{-1} \text{mod } 26$$

4TH INTERNATIONAL CONFERENCE ON KNOWLEDGE & INNOVATION IN ENGINEERING, SCIENCE & TECHNOLOGY

21-23 December, 2018
Berlin - Germany

Complexity Analysis

The complexity of the modified Hill cipher provides $4NM$ multiplications and $2NM$ additions which is greater than the conventional Hill cipher algorithm, e.g. for 2×2 matrix in conventional Hill cipher algorithm, the inverse of the key entails 4 multiplications and only 1 addition; however, in modified Hill cipher algorithm, it provides $4+4NM$ multiplications and $1+2NM$ additions for the manipulating of its inverse of key matrix.

Security Analysis

The modified Hill cipher algorithm provides enhanced security performance in sense of non-square matrix approach. In this technique, the size of the matrix may extend as much as it can which makes more confusion in the communication link. However, in conventional Hill cipher technique, the confusion is dependent on the fixed matrix size which is clearly envisioned in Table 1.

Table 1: Confusion in letters provided by modified and conventional Hill cipher techniques.

Name of Cipher technique	Confusion for $N=2, M=2$	Confusion for $N=2, M=4$	Confusion for $N=2, M=8$	Confusion for $N=2, M=16$	Confusion for $N=2, M=32$
Modified Hill Cipher	2 letters	4 letters	8 letters	16 letters	32 letters
Conventional Hill Cipher	2 letters	2 letters	2 letters	2 letters	2 letters

Moreover, the cipher text only attack for $N=2, M=32$ requires the brute force of 2×32 inverse matrix that can be written as

$$M = [c_1 \quad c_2 \quad c_3 \quad \cdots \quad c_{32}] [K^{-1}] \text{mod } 26$$

$$K^{-1} = \begin{bmatrix} k_{1,1}^{-1} & k_{1,2}^{-1} \\ k_{2,1}^{-1} & k_{2,2}^{-1} \\ k_{3,1}^{-1} & k_{3,2}^{-1} \\ \vdots & \vdots \\ k_{32,1}^{-1} & k_{32,2}^{-1} \end{bmatrix}$$

4TH INTERNATIONAL CONFERENCE ON KNOWLEDGE & INNOVATION IN ENGINEERING, SCIENCE & TECHNOLOGY

21-23 December, 2018

Berlin - Germany

For the brute force of 2×32 matrix size, it is difficult to find the matrix by using cipher text only attack.

Conclusion

This paper presents a new modified Hill cipher technique which has been provided enhanced security performance than the conventional hill cipher. This enhanced security of the modified Hill cipher is dependent on the non-square $N \times M$ matrix approach. Therefore, the varying m redundant cipher text has been bestowed more confusion than the conventional Hill cipher as well as of frequency analysis. Moreover, the modified Hill cipher has been provided more $4NM$ multiplications and $2NM$ addition than the conventional Hill cipher algorithm. So, there must be a tradeoff between the enhanced security performance and the computational complexity of the algorithm.

References

- [1] Hill, L.S. (1929). Cryptography in an Algebraic Alphabet. *The American Mathematical Monthly*, vol 36, 306-312.
- [2] Hill, L.S. (1931). Concerning Certain Linear Transformation Apparatus of Cryptography. *The American Mathematical Monthly*, 38, 135-154.
- [3] Eisenberg, Murray. (1999). *Hill ciphers and modular linear algebra.*" Mimeographed notes 1-19.
- [4] Stinson, D. (2002). *Cryptography: Theory and Practice*. Second edition. CRC/C&H.
- [5] Ismail, et. al. (2006). How to Repair the Hill Cipher. *Journal of Zhejiang University-Science*, vol 7, 2022-2030.
- [6] Kiele, W.A. (1990), A Tensor-Theoretic Enhancement to the Hill Cipher System. *Cryptologia*, 14(3), 225-233.
- [7] Saeednia, S. (2000). How to Make the Hill Cipher Secure. *Cryptologia*, vol 24, 353-360
- [8] Mahmoud, A.Y., Chefranov, A.G. (2009). Hill Cipher Modification Based on Eigenvalues HCM-EE. In: *Proc. of SIN'09*, 164-167.
- [9] Toorani, M., Falahati, A. (2009) A Secure Variant of the Hill Cipher. In: *Proc. of 14th IEEE Symposium on Computers and Communications (ISCC'09)*, 313-316.
- [10] Toorani, M., Falahati, A. (2011). A Secure Cryptosystem Based on Affine Transformation. *Security and Communication Networks*, vol 4, 207-215.

4TH INTERNATIONAL CONFERENCE ON KNOWLEDGE & INNOVATION IN ENGINEERING, SCIENCE & TECHNOLOGY

21-23 December, 2018

Berlin - Germany

- [11] Nofriansyah, *et. al.* (2018). A New Image Encryption Technique Combining Hill Cipher Method, Morse Code and Least Significant Bit Algorithm. *In Journal of Physics: Conference Series*, Vol 954.
- [12] Daemen, J., Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. *Information Security and Cryptography. Springer* (2002).
- [13] Sastry, V., Shankar, N.R. (2007). Modified Hill Cipher with Interlacing and Iteration (2007).
- [14] Chen, *et. al.* (2014). A Hill Cipher-Based Remote Data Possession Checking in Cloud Storage. *Security and Communication Networks*, vol 7, 511-518.
- [15] Karthikeyan, *et. al.* (2013) An Enhanced Hill Cipher Approach for Image Encryption in Steganography. *International Journal of Electronic Security and Digital Forensics*, vol 5, 178-187.
- [16] Acharya, *et. al.* (2010), Privacy Protection of Biometric Traits Using Modified Hill Cipher with Involutory Key and Robust Cryptosystem. *In: Proc. of BIOTEC'10*. 242-247.
- [17] Huang, N. (2014). An Enhanced Hill Cipher and Its Application in Software Copy Protection. *JNW*, vol 9, 2582-2590.
- [18] Keliher, L., Thibodeau, S. (2013). Slide Attacks Against Iterated Hill Ciphers. *In Proc. of SSCC'13, Springer*, 179-190.
- [19] Keliher, L., Delaney, A.Z. (2013). Cryptanalysis of the Toorani-Falahati Hill Ciphers. *In: Proc. of ISCC'13*. 436-440.
- [20] Parmar, N.B., Bhatt, K. (2015). Hill Cipher Modifications: A Detailed Review. *International Journal of Innovative Research in Computer and Communication Engineering*, vol 3, 1467-1474.
- [20] Bauer, C.P., Millward, K. (2007). Cracking Matrix Encryption Row by Row. *Cryptologia*, vol 31, 76-83.

Appendix A: Example

4TH INTERNATIONAL CONFERENCE ON KNOWLEDGE & INNOVATION IN ENGINEERING, SCIENCE & TECHNOLOGY

21-23 December, 2018

Berlin - Germany

The key is consider to be taken as

$$K = \begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 1 & 0 \end{bmatrix} \text{mod } 26$$

and the plain text message is $M = [B \ E] = [1 \ 4]$. The cipher text corresponding to plain text message M is calculated as

$$C = MK^T$$

$$C = [1 \ 4] \begin{bmatrix} 0 & 2 & 1 \\ 1 & 2 & 0 \end{bmatrix} = [4 \ 10 \ 1] = [E \ H \ B]$$

The cipher text C is EHB corresponding to text message BE

The plaintext corresponding to cipher text is calculated as

$$M = CK^{-1} = CK(K'K)^{-1}$$

$$M = [4 \ 10 \ 1] \begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 1 & 0 \end{bmatrix} \left\{ \begin{bmatrix} 0 & 2 & 1 \\ 1 & 2 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 1 & 0 \end{bmatrix} \right\}^{-1} \text{mod } 26$$

$$M = [4 \ 10 \ 1] \begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 1 & 0 \end{bmatrix} \frac{1}{9} \begin{bmatrix} 5 & -4 \\ -4 & 5 \end{bmatrix} \text{mod } 26$$

$$M = [4 \ 10 \ 1] \begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 1 & 0 \end{bmatrix} 3 \begin{bmatrix} 5 & 22 \\ 22 & 5 \end{bmatrix} \text{mod } 26$$

$$M = [4 \ 10 \ 1] \begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 15 & 14 \\ 14 & 15 \end{bmatrix} \text{mod } 26$$

$$M = [4 \ 10 \ 1] \begin{bmatrix} 14 & 15 \\ 6 & 6 \\ 15 & 14 \end{bmatrix} \text{mod } 26$$

$$M = [131 \ 134] \text{mod } 26$$

$$M = [1 \ 4] = [B \ E]$$

After decryption the plain text is BE