The CSI Journal on
Computer Science and Engineering
Vol. 12, No. 2 & 4 (b), 2014
Pages 11-15
Regular Paper

Modified Bitwise Hill Crypto System

Jaber Karimpour Masoud Aghdasifam Ali A. Noroozi

Department of Computer Sciences, University of Tabriz, Tabriz, Iran

Abstract

Hill Cipher (HC) is a matrix-based polygraph symmetric data encryption method. In 2011, Desoky *et al.* proposed the Bitwise Hill Crypto System (BHC) which is based on bit arithmetic. In this paper, we analyze BHC and show that it is insecure. Then, we propose a new modification using chaotic maps which provides better security.

Keywords: Cryptography, Bitwise Cipher, Chaotic Maps, Hill Cipher.

1. Introduction

The Hill Cipher, proposed by Lester S. Hill in 1929 [1], is a famous method based on matrix computations. HC is a block cipher algorithm where plain text is divided into equal size blocks. In this method, the key is a non-singular invertible square matrix. The plain text P is encrypted as:

$$\mathrm{C} = \mathrm{P} \times \mathrm{K} \bmod \mathrm{m} \qquad (1)$$

in which m is a positive integer number greater than 1, C is the cipher text block, K is the key matrix, and × is the matrices multiplication operator. Decryption of the cipher text block C produces the plain text block as:

$$\mathrm{P} = \mathrm{C} \times \mathrm{K}^{-1} \bmod \mathrm{m} \qquad (2)$$

Such that

$$\gcd(\det(\mathrm{K}) \bmod \mathrm{m}, \mathrm{m}) = 1 \qquad (3)$$

where det(K) is determinant of K, and K^{-1} refers to inverse of the matrix K.

Bitwise Hill Crypto System (BHC) is an extended HC, which uses data in a binary form. This method splits one byte-data matrix into 8 binary-data matrices and calculates the corresponding binary-data matrices by Hill Cipher with m = 2. Then it combines back these matrices to generate one byte-data cipher matrix. Our proposed algorithm (MBHC) improves BHC's performance using inverse of the key matrix and another auxiliary chaotic-based matrix. In MBHC, the vulnerability of BHC against KPA is solved. This new algorithm is also suitable for encrypting images as a probabilistic encryption algorithm.

Rest of the paper is as follows. In section 2, we review some recent researches on improvements of HC. Then, in section 3, we introduce Bitwise Hill Crypto System. Cryptanalysis of BHC is presented in section 4. Finally, a new algorithm is proposed in section 5 and it's analysis in section 6. The paper is concluded in section 7.

2. Previous Work

In recent years, various researches have been done to improve the security of HC. Saeednia in [2] proposed a modification of HC, called Secure Hill Cipher (SHC), which uses a dynamic key matrix and random permutation of rows and columns from a master key. SHC uses a new key for each block that prevents known plain text attacks. But transferring permutations in this method is insecure. Lin et al. [3] proposed a modified algorithm for SHC, which uses one way hash functions in its process.

Sastry et al. [4] proposed a new iterative cipher (MHC). In this method, the plain text is multiplied by the key matrix in both sides. Keliher [5] proved that MHC is vulnerable against known plain text attacks.

In 2010, Sastry et al. [6] introduced a variant of the HC, named SVK, which uses a pair of key matrices and a permutation scheme. This method is secure against common attacks, specially known plain text attacks. Sastry and Shirisha [7] proposed another algorithm which includes a key matrix and a key bunch matrix. This algorithm is supplemented with a function for creating confusion. Rahman et al. [8] proposed Hill++, which is an extension of Affin Hill Cipher. The Affine Hill Cipher is expressed in the form of $\mathrm{C = P \times K + V \,(mod\, m)}$, where V represents a constant in the form of matrix [9].

Recently year some novel algorithms related to HC are proposed to improve its performance (e.g. [10]), or its secrecy (e.g. [11]). All these researches are based on decimal numbers.

3. Bitwise Hill Crypto System

Bitwise Hill Crypto System (BHC) is proposed by Desoky and Madhusoodhanan [10]. In this system the plain text is available in binary format. The input file is converted to a $\mathrm{(n/b) \times b}$ matrix where n is the total length of the plaintext and b is the block size. Then, it is divided into 8 planes with $\mathrm{i^{th}}$ plane containing the $\mathrm{i^{th}}$ bit of the data bytes. The keys $[\mathrm{K_i}]$, with $\mathrm{i = 1, 2, \cdots, 8}$ are $\mathrm{b \times b}$ invertible matrices which are generated randomly.

Multiplication of the binary matrices is carried out using bitwise AND and bitwise XOR. Thus, encryption is bit wise multiplication (modulo 2) of the planes by the key matrices. This generates 8 cipher planes. These planes are then reshaped to form a matrix C such that the contents of cipher plane i becomes the $\mathrm{i^{th}}$ column:

$$C_i = P_i \times K_i \; mod\; 2\,, i = 1, 2, 3, \cdots, 8 \tag{4}$$

4. Cryptanalysis of BHC

Although BHC is secure against brute force attacks, but in this section we list three defects for it.

The first defect is vulnerability against the known plain text attacks (KPA). Multiplication of i^{th} plain matrix by i^{th} key matrix is a simple binary matrix multiplication. In multiplication of matrices, there is a linear dependency between the operands and the result. For example, if plain text is “Hello Masoud”, then $\mathrm{P_1}$ in ASCII code for $\mathrm{b = 3}$ would be as follows:

$$P_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

If we know the cipher text, we could build the matrix $\mathrm{C_1}$:

$$C_1 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

The problem is to find matrix $\mathrm{K_1}$ such that:

$$\mathrm{P_1 \times K_1 = C_1} \tag{5}$$

or:

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

This is a system of 12 linear equations in the 9 variables $\mathrm{k_{11}, k_{12}, \dots, k_{33}}$ and $\mathrm{K_1}$ could be calculated:

$$K_1 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

As a result, BHC is vulnerable against KPA.

The second defect is that BHC is not suitable for all zeroes block encryption. All zeros block may happen when it is used to encrypt an image which has a large black area. Multiplication of an all zeros matrix by another matrix always results an all zeros matrix. So, BHC maps an all zeros plain text to itself.

Key:
96F50B8995CEFD55EF5453EE978884F7

Plain message:
3C32303134303231313232333030303E
3C32303134303231323030303030303E

Cipher message using BHC:
35262809372422033123230036282406
35262809372422033220220036282406

Cipher message using MBHC:
9DAF035F5B089D053447C030D35F02E4
191790016D1035DFA990320285D5EB39

Figure 1. Encryption of a message by BHC and MBHC algorithms with a same invertible random key. All data are represented in hexadecimal form of ASCII codes

Finally, the third defect is that BHC is not suitable for encrypting an image containing large same-colored areas. This happens because all the same-colored blocks would map to a unique matrix.

5. The Proposed Algorithm

To improve BHC, we propose to use the inverse of key matrix and another auxiliary matrix, as follows:

$$\mathrm{C_i = K_i^{-1} \times P_i \times K_i + K_C \; mod\; 2\,, i = 1{,}2{,}\cdots, 8} \tag{6}$$

and to decrypt:

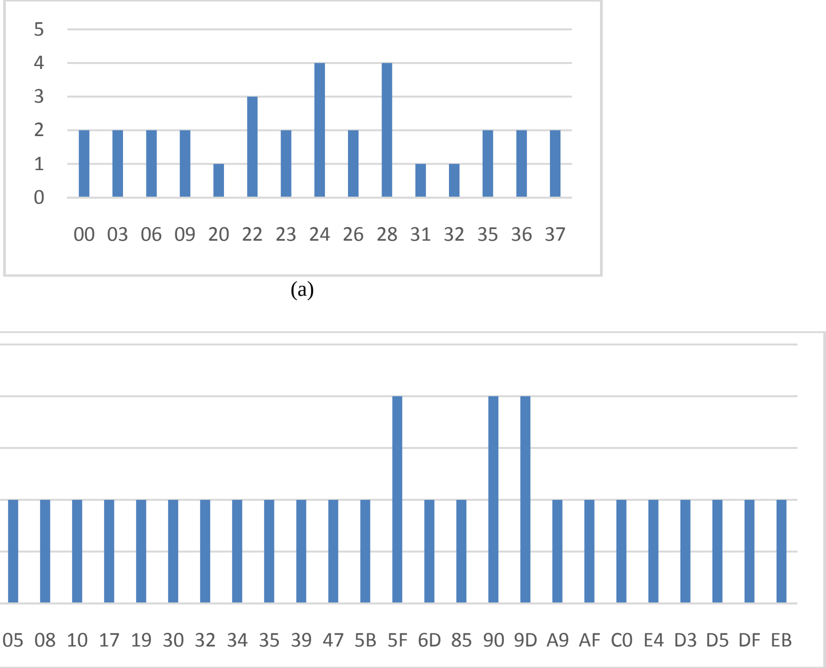
$$\mathrm{P_i = K_i \times (C_i - K_C) \times K_i^{-1} \; mod\; 2\,, i = 1, 2, \cdots, 8} \tag{7}$$

where $\mathrm{K_C}$ is an auxiliary chaotic-based matrix, calculated as:

(1) For every row r of the key matrix calculate $\mathrm{e_r}$, equivalent real value of row r. This value belongs to the range [0, 1]. For example:
$\mathrm{10111010 = \; 2^{-1} + 2^{-3} + 2^{-4} + 2^{-5} + 2^{-7} = 0.7265625}$

(2) Set $\mathrm{x_0 = \prod_{r=1}^{b} K_r}$, as the initial value of Logistic Map:

$$\mathrm{x_n = 4x_{n-1}(1 - x_{n-1})} \tag{8}$$



(a)

(b)

Figure 2. Frequency of the characters in cipher text of (a) BHC and (b) MBHC. The horizontal axis indicates hexadecimal numbers of ASCII codes and the vertical axis indicates frequency of repetition

Key:
86F50B8995CEFD55EF5453EE978884F7

Plain message:
3C32303134303231313232333030303E
3C32303134303231323030303030303E

Cipher message using BHC:
25262809272422032122220126282406
25262809272422032220220026282406

Cipher message using MBHC:
8CAE024E5A088C043546C031C24E12F4
190690117D0024DFA980221395C4EA29

Figure 3. Effect of one-bit-change of the key on encryption of a message by BHC and MBHC algorithms. All data are represented in hexadecimal form of ASCII codes

(3) Calculate elements of K_c by Logistic Map sequence

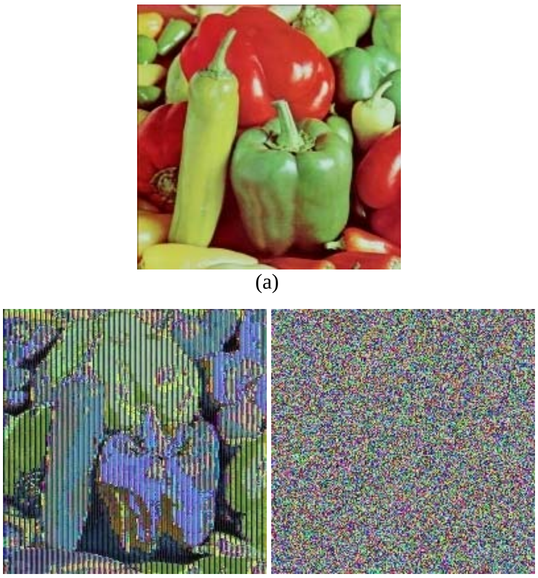
$$(K_C)_{ij} = \begin{cases} 0 & x_n \leq 0.5 \\ 1 & x_n > 0.5 \end{cases} \qquad (9)$$

where n increases by one after calculating every element.

In this algorithm, there is no linear dependency between the cipher matrix and the plain matrix. It is clear that P should be rearranged in size b × b.

6. Experiments and Security Analysis of the Proposed Algorithm

Security of the proposed algorithm is based on two different concepts. By using inverse of key matrix, a simple linear equation sets problem is converted to a nonlinear equation sets problem. The latter problem is NP-hard, and hard to solve. Correspondingly, this method is secure against the known plain text attack. It also incorporates more confusion and diffusion effects into cipher text.



(a)

(b) (c)

Figure 4. Encrypting (a) Pepper image by (b) BHC and (c) MBHC with a same random key

According to the way auxiliary chaotic-based matrix is generated in the algorithm, each block is encrypted by a different K_c, and if two blocks are the same, their corresponding cipher blocks would be different. As a result, the proposed method can easily deal with the problem of large same-colored area images. This matrix is also a pseudorandom matrix which causes more confusion and diffusion effects.

BHC multiplies the key matrix and the plain matrix. So if the plain matrix is zero, the cipher matrix would be zero too. The proposed algorithm adds K_c to the multiplication of the key matrix and the cipher matrix. Therefore, the so called all zero blocks problem is solved, and as described above, two same all-zero matrices generate different non-zero cipher matrices.

In order to evaluate efficiency of the proposed algorithm, three experiments were done. In the first experiment, the message

“<20140211223000><20140212000000>”

(start and stop date-time of a network attack) was encrypted by both BHC and our proposed algorithm (MBHC) with a same 128-bits random invertible key.

As shown in figure 1, BHC encrypts two similar text message blocks to two similar cipher blocks, but MBHC encrypts them to two different non-related blocks. Repetition frequency of the characters is shown in figure 2.

To check avalanche effect of changing the key on the cipher text, the first experiment is repeated by a new key which is different from the old one in just one bit. The results are shown in figure 3 Changing one bit of the key, in this example, changes just 11 bits (almost 4.3% of the total bits) of the cipher message in BHC, but in MBHC, this one-bit-change of the key affects 35 bits (almost 13.7% of the total bits) of the cipher message.

In the third experiment, the Pepper image (Figure 4 a) is encrypted by BHC and MBHC with a random 128-bits invertible key. As shown in figure 4 b, the objects are distinguishable in the image encrypted by BHC, but the image encrypted by MBHC (Figure 4 c) is completely garbled and the objects are indistinguishable.

According to the results of these experiments, MBHC is more secure than BHC, because of using inverse of the key matrix and K_c.

7. Conclusion

Bitwise Hill Cipher Crypto System is a new binary-data-based crypto system. We show that it is not secure against known plain text attacks. It is also not secure enough for encrypting a plain text consisting of many zeros or if an image has large same colored areas.

In this paper, a new algorithm (Modified BHC) is proposed to improve the security of BHC. This modification involves both the key and its inverse and a pseudorandom matrix, based on key matrix and logistic chaotic map. It disarranges any direct dependency between the plain text and the cipher text. It also increases confusion effect and diffusion effect in the encryption process.

Further research can be done on calculating the auxiliary matrix K_c. The Logistic Map can be replaced by other chaotic maps too. 2D chaotic maps can be used to achieve better performance.

References

[1] L. S. Hill, "Cryptography in an Algebraic Alphabet," *The American Mathematical Monthly*, vol. 36, no. 3, pp. 306-312, 1929.

[2] S. Saeednia, "How to Make Hill Cipher Secure," *Journal of Cryptologia*, vol. 4, no. 24, pp. 353-360, 2000.

[3] C. H. Lin, C. Y. Lee, and C. Y. Lee, "Comments on Saeednia’s Improved Scheme for The Hill Cipher," *Journal of the Chinese Institute of Engineers*, vol. 5, no. 27, pp. 743-746, 2004.

[4] V. U. K. Sastry, D. S. R. Murthy, and S. D. Bhavani, "A Block Cipher Involving a Key Applied on Both Sides of the Plain Text," *Journal of Computer and Network Security*, vol. 1, no. 1, pp. 27-30, 2009.

[5] L. Keliher, "Cryptanalysis of a Modified Hill Cipher," *Journal of Computer and Network Security*, vol. 2, no. 7, pp. 122-126, 2010.

[6] V. U. K. Sastry, A. Varanasi, and S. U. Kumar, "A Modified Hill Cipher Involving a Pair of Keys and a Permutation," *Journal of Computer and Network Security*, vol. 2, no. 9, pp. 105-108, 2010.

[7] V. U. K. Sastry, and K. Shirisha, "A Block Cipher Involving a Key Matrix and a Key Bunch Matrix, Supplemented with Mix," *Journal of Engineering and Science*, vol. 2, no. 9, pp. 37-43, 2013.

[8] M. Rahman, A. Nordin, A. F. A. Abidin, N. K. Yusof, and N. S. M. Usop, "Cryptography: A New Approach of Classical Hill Cipher," *Journal of Security and Its Applications*, vol. 7, no. 2, pp. 179-190, 2013.

[9] D. R. Stinson, *Cryptography Theory and Practice*, New Jersey: Chapman-Hall, 2006.

[10] W. Xinyu, and Z. Mi, "Parallel Algorithm for Hill Cipher on Map Reduce," *Proc. IEEE Intl Conf. Informatics and Computing*, pp. 251-257, 2014.

[11] M. Ahmed, and A. Chefranov, "Hill Cipher Modification Based on Pseudo-Random Eigen Values," *Journal of Electrical Engineering and Computer Science on Application and Mathematics*, vol. 8, no. 2, pp. 505-516, 2014.

[12] A. Desoky, and A. P. Madhusoodhanan, "Bitwise Hill Crypto System," *Proc. IEEE Intl Symp. Signal Processing and Information Technology*, pp. 80-85, 2011.

Jaber Karimpour received the B.Sc. Degree in Computer Science and Applied Mathematics from University of Tabriz (Iran) in 1998, the M.Sc. Degree specializing in the computer systems area of Applied Mathematics from University of Tabriz in 2000, and the Ph.D. degree in Computer Systems form University of Tabriz. Dr. Karimpour is currently an Assistant Professor in the Department of Computer Sciences at University of Tabriz and has been manager of Information Technology of the university since 2011. His current research interests include cryptography, network security, formal specification, and verification

E-mail: karimpour@tabrizu.ac.ir

Masoud Aghdasifam received the Associate Degree in Applied Mathematics from University of Tabriz (Iran) in 2008, the B.Sc. Degree in Software Engineering from University Collage of Daneshvaran (Tabriz – Iran), and the M.Sc. Degree in Computer science from University of Tabriz. His current research interests include data security (cryptography) and network security (IDS).

E-mail: m_aghdasifam91@ms.tabrizu.ac.ir

Ali A. Noroozi received B.Sc. in information technology engineering from Amirkabir University of Technology, Iran in 2009, and M.Sc. in Management of Information Systems from K. N. Toosi University of Technology, Iran in 2011. Now, he is a Ph.D. student of Computer Science in University of Tabriz, Iran. His research interests include secure information flow and formal verification.

E-mail: noroozi@tabrizu.ac.ir

Paper Handling Data:

Submitted: 20.04.2014
Received in revised form: 11.03.2015
Accepted: 04.04.2015
Corresponding author: Masoud Aghdasifam, Department of Computer Sciences, University of Tabriz, Tabriz, Iran.