The 2013 CSI International symposium on
Computer Science and Software Engineering (CSSE)

Modified Bitwise Hill Crypto System

Jaber Karimpour[1], Masoud Aghdasifam[2], Ali Asghar Noroozi[1]

[1]Department of Computer Sciences, University of Tabriz, Tabriz, Iran
{karimpour, noroozi}@tabrizu.ac.ir

[2]Department of Computer Sciences, University of Tabriz, Tabriz, Iran
m_aghdasifam91@ms.tabrizu.ac.ir

Abstract. Hill Cipher (HC) is a polygraph symmetric data encryption method which is based on matrices. 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 map which provides better security.

Keywords: Bitwise Cipher, Chaotic Maps, Cryptography, 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 square matrix. The plain text *P* is encrypted as:

$$C = P \times K \bmod m \tag{1}$$

in which *C* is the cipher block and *K* is the key matrix. Decryption of the cipher text block *C* produces the plain text block as:

$$P = C \times K^{-1} \bmod m \tag{2}$$

such that

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

Bitwise Hill Crypto System is an extended HC, which uses data in a binary form. 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, several researches have been done to improve the security of HC. Saeednia in [6] 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.* [7] 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 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.* [2] introduced a variant of the HC (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 [8] 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.* [9] proposed Hill++, which is an extension of Affin Hill Cipher. The Affine Hill Cipher is expressed in the form of $C = P \times K + V \ (mod\ m)$, where *V* represents a constant in the form of matrix [10].

3 Bitwise Hill Crypto System

Bitwise Hill Crypto System (BHC) is proposed by Desoky and Madhusoodhanan [3]. In this system the plain text is available in the form of binary. The input file is converted to a $(n/b) \times b$ matrix where b is the block size. Then, it divided into 8 planes with i^{th} plane containing the i^{th} bit of data bytes. The keys $[K_i]\ \ i = 1, 2, \cdots, 8$ are invertible matrices generated randomly in size $b \times b$.

Multiplication of the binary matrices is carried out using bitwise AND and bitwise XOR. Thus, encryption is bitwise 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 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 we show that it is vulnerable against known plain text attacks.

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 P_1 in ASCII code for $b = 3$ 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 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 K_1 such that:

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

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 variable k_{11}, k_{12}, … , k_{33} and K_1 could be calculated:

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

As a result, The BHC is vulnerable against known plain text attacks.

On the other hand, 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.

The BHC also is not suitable for encrypting an image containing *large same-colored area*. This happens because all the same-colored blocks would map to a unique matrix.

5 The Proposed Algorithm

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

$$C_i = K_i^{-1} \times P_i \times K_i + K_C \; mod \; 2 \; , i = 1, 2, 3, \cdots, 8 \tag{6}$$

and to decrypt:

$$P_i = K_i \times (C_i - K_C) \times K_i^{-1} \; mod \; 2 \; , i = 1, 2, 3, \cdots, 8 \tag{7}$$

where K_C is an auxiliary chaotic-based matrix, calculated as:

(i) For every row r of the key matrix calculate e_r, equivalent real value of row r. This value in range [0,1]. For example:

$$10111010 = 2^{-1} + 2^{-3} + 2^{-4} + 2^{-5} + 2^{-7} = 0.7265625$$

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

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

(iii) Calculate elements of K_c:

$$(K_C)_{ij} = \begin{cases} 0 & x_{s+bi+j} \leq 0.5 \\ 1 & x_{s+bi+j} > 0.5 \end{cases} \tag{9}$$

where s is an arbitrary static integer greater than 20.

(iv) After encoding each block, multiply K_c by itself, to obtain different auxiliary matrix for next block.

Subject to calculation steps of K_c, it is a pseudorandom matrix which causes more confusion and diffusion effects. In this algorithm, the cipher matrix and the plain matrix don't have any linear dependency. It is clear that P should be rearranged in size $b \times b$.

6 Security analysis of the proposed algorithm

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

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 encryption*.

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. As a result, the so called *all zero blocks encryption* problem is solved, and as described above, two same *all-zero matrices* generate different *non-zero cipher matrices*.

7 Conclusion

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

In this paper, a new algorithm (Modified BHC) 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 and diffusion effects in encryption process.

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

References

1. Hill, L.S.: Cryptography in An Algebraic Alphabet. In: The American Mathematical Monthly, vol. 36, pp. 306-312 (1929).
2. Sastry, V.U.K., Varanasi, A., and Kumar, S.U.: A Modified Hill Cipher Involving a Pair of Keys and a Permutation. In: International Journal of Computer and Network Security, Vol. 2, No. 9, pp. 105-108 (2010).
3. Desoky, A., Madhusoodhanan, A.P.: Bitwise Hill Crypto System. In: Signal Processing and Information Technology (ISSPIT), Vol. , No., pp.80-85, (2011 IEEE International Symposium).
4. Sastry, V.U.K., Murthy, D.S.R., Durga Bhavani, S.: A Block Cipher Involving a Key Applied on Both Sides of the Plain Text. In: International Journal of Computer and Network Security, Vol. 1, No. 1, pp. 27-30 (2009).
5. Keliher, L.: Cryptanalysis of a Modified Hill Cipher. In: International Journal of Computer and Network Security, Vol. 2, No. 7, pp. 122{126, (2010).
6. Saeednia, S.: How to Make Hill Cipher Secure. In: Journal of Cryptologia, Vol. 4, No. 24, pp. 353-360 (2000).
7. Lin, C. H., Lee, C. Y., Lee, Cu. Yu.: Comments on Saeednia's Improved Sheme for The Hill Cipher. In: Hournal of the Chinese Institute of Engineers, Vol. 5, No. 27: pp. 743-746 (2004).
8. Sastry, V.U.K., Shirisha, K.: A Block Cipher Involving a Key Matrix and a Key bunch Matrix, Supplemented with Mix. In: International Journal of Engineering and Science, Vol. 2, No. 9, pp. 37-43 (2013).
9. Rahman, M. Nordin A., Abidin, A. F. A., Yusof, M. K., Usop, N.S.M.: Cryptography: A New Approach of Classical Hill Cipher. In: International Journal of Security and Its Applications, Vol. 7, No. 2, pp. 179-190 (2013).
10. Stinson, D. R.: Cryptography Theory and Practice 3td edition, Chapman & Hall/CRC, pp. 13-37 (2006).