Image Encryption by Novel Cryptosystem Using Matrix Transformation

Bibhudendra Acharya, Sarat Kumar Patra, and Ganapati Panda
Department of Electronics and Communication Engineering
National Institute of Technology Rourkela, Orissa-769008, India
bibhudendra@gmail.com, {skpatra, gpanda}@nitrkl.ac.in

Abstract

The Hill cipher is a famous symmetric cryptosystem that have several advantages in data encryption. However, the Hill cipher algorithm cannot encrypt images that contain large areas of a single color. Thus, it does not hide all features of the image which reveals patterns in the plaintext. Moreover, it can be easily broken with a known plaintext attack revealing weak security. In this paper, novel cryptosystem is used to encrypt image that overcomes these disadvantages. The novel cryptosystem uses randomly generated self-invertible matrix as an encryption key for each block encryption and also this method eliminates the computational complexity involved in finding inverse of the matrix while decryption. The proposed variant yields higher security and significantly superior encryption quality compared to the original one.

Keywords- *Cryptosystem, Hill cipher, Image encryption, Self-invertible matrix, Quality of encryption.*

1. Introduction

Information is an asset that has a value like any other asset. As an asset, information needs to be secured from attacks. To be secured, information needs to be hidden from unauthorized access. Popular application of multimedia technology and increasingly transmission ability of network gradually leads us to acquire information directly and clearly through images. Hence, data security has become a critical and imperative issue. Cryptography, the science of encryption, plays a central role in mobile phone communications, pay-TV, e-commerce, sending private emails, transmitting financial information, security of ATM cards, computer passwords, and touches on many aspects of our daily lives. Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message (plaintext) into one that is unintelligible (ciphertext) and then retransforming that message back to its original form. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering [1].

Substitution cipher is one of the basic components of classical ciphers. A substitution cipher is a method of encryption by which units of plaintext are substituted with ciphertext according to a regular system; the units may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution [2]. The units of the plaintext are retained in the same sequence as in the ciphertext, but the units themselves are altered. There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different times in the message— such as with homophones, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext. Hill cipher is a type of monoalphabetic polygraphic substitution cipher. Hill cipher has several advantages such as disguising letter frequencies of the plaintext, its simplicity because of using matrix multiplication and inversion for enciphering and deciphering, its high speed, and high throughput [3, 4].

The Hill cipher algorithm cannot encrypt images that contain large areas of a single color. Thus, it does not hide all features of the image which reveals patterns in the plaintext and also it can be easily broken with a known plaintext attack revealing weak security. In this paper, novel cryptosystem [5] is used

978-0-7695-3267-7/08 $25.00 © 2008 IEEE
DOI 10.1109/ICETET.2008.110

to encrypt image that overcomes these disadvantages. The novel cryptosystem uses randomly generated self-invertible matrix as an encryption key for each block encryption. The resulting image from the algorithm is scrambled using a random matrix which is used as another secret key. This increases the secrecy of data. This method encompasses less computational complexity during decryption, as self-invertible matrix [6] is used as key.

The organization of the paper is as follows. Following the introduction, the basic concept of Hill Cipher is outlined in section 2. Section 3 discusses about the modular arithmetic. In section 4, Cryptosystem is presented. Image encryption and results are discussed in section 5. Finally, section 6 describes the concluding remarks.

2. Hill Cipher

Hill ciphers are an application of linear algebra to cryptology. It was developed by the mathematician Lester Hill. The Hill cipher algorithm takes m successive plaintext letters and substitutes m ciphertext letters for them. The substitution is determined by m linear equations in which each character is assigned a numerical value $(a = 0, b = 1, \ldots, z = 25)$. Let m be a positive integer, the idea is to take m linear combinations of the m alphabetic characters in one plaintext element and produce m alphabetic characters in one ciphertext element. Then, an $m \times m$ matrix A is used as a key of the system such that A is invertible modulo 26 [7]. Let a_{ij} be the entry of A. For the plaintext block $x = (x_1, x_2, \ldots, x_m)$ (the numerical equivalents of m letters) and a key matrix A, the corresponding ciphertext block $y = (y_1, y_2, \ldots, y_m)$ can be computed as follows.

Encryption:

$$(y_1, y_2, \ldots, y_m) = (x_1, x_2, \ldots, x_m) A \pmod{26} \quad \ldots (1)$$

Where

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{bmatrix}$$

The ciphertext is obtained from the plaintext by means of a linear transformation.

Decryption:

The reverse process, deciphering, is computed by

$$(x_1, x_2, \ldots, x_m) = (y_1, y_2, \ldots, y_m)\ A^{-1} \pmod{26}, \qquad \ldots (2)$$

Where

$$A^{-1} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{bmatrix}^{-1} \pmod{26}$$

Since the block length is m, there are 26^m different m letters blocks possible, each of them can be regarded as a letter in a 26^m -letter alphabet. Hill's method amounts to a monoalphabetic substitution on this alphabet [8].

3. Modular Arithmetic

The arithmetic operation presented here are addition, subtraction, unary operation, multiplication and division. Based on this the self invertible matrix for Hill cipher algorithm is generated. The congruence modulo operator has the following properties [9]:

1. $a \equiv b \mod p$ if $p \mid (a - b)$
2. $(a \bmod p) = (b \bmod p) \Rightarrow a \equiv b \mod p$
3. $a \equiv b \mod p \Rightarrow b \equiv a \mod p$
4. $a \equiv b \mod p$ and $b \equiv c \mod p$

   $\Rightarrow a \equiv c \mod p$

Let $Z_p = [0, 1, \ldots, p - a]$ the set residues modulo p. If modular arithmetic is performed within this set Z_p, the following equations present the arithmetic operations:

1. Addition:

   $(a + b) \bmod p = [(a \bmod p) + (b \bmod p)] \bmod p$

2. Negation:

   $-a \bmod p = p - (a \bmod p)$

3. Subtraction:

   $(a - b) \bmod p = [(a \bmod p) - (b \bmod p)] \bmod p$

4. Multiplication:

   $(a * b) \bmod p = [(a \bmod p) * (b \bmod p)] \bmod p$

5. Division:

$(a/b) \bmod p = c$ when $a = (b * c) \bmod p$

The Table 1 exhibits the properties of modular arithmetic.

4. Cryptosystem

As Hill cipher decryption requires inverse of the matrix, we suggest the use of self-invertible matrix generation method while encryption with the Hill Cipher. In the self-invertible matrix generation method, the matrix used for the encryption is itself self-invertible. So, in the proposed cryptosystem at the time of decryption, we need not to find inverse of the matrix. Moreover in this cryptosystem, algorithm generates the different key matrix for each block encryption instead of keeping the key matrix constant. This increases the secrecy of data. In order to generate different key matrix each time, the encryption algorithm randomly generates the seed number and from this key matrix is generated. Method of generating random self-invertible even matrix is described as follows.

Table 1. Properties of Modular Arithmetic

Commutative Law: $(\omega + x) \bmod p = (x + \omega) \bmod p$ $(\omega * x) \bmod p = (x * \omega) \bmod p$
Associative Law: $[(\omega + x) + y] \bmod p = [\omega + (x + y)] \bmod p$
Distribution Law: $[\omega * (x + y)] \bmod p$ $= [\{(\omega * x) \bmod p\} + \{(\omega * y) \bmod p\}] \bmod p$
Identities: $(0 + a) \bmod p = a \bmod p$ $(1 * a) \bmod p = a \bmod p$
Inverses: For each $x \in Z_p$, there exists y such that $(x + y) \bmod p = 0$ then $y = -x$ For each $x \in Z_p$ there exists y such that $(x * y) \bmod p = 1$

The algorithm generates $n \times n$ matrix where n is even and utilized for generating a self-invertible matrix.

Let s be the seed for generating the random number,

t be the multiplier generating the random number,

p the modulus (necessarily to be a prime number), and

k a scalar constant.

Form a random matrix of $\frac{n}{2} \times \frac{n}{2}$, A_{11} with elements as

$a_{11} = s$

$a_{12} = st$

.

•

•

$a_{21} = st^{\frac{n}{2}}$

•

•

•

$a_{2n/2} = st^{n-1}$

Thus $a_{ij} = st^m$

where $m = (i-1)\frac{n}{2} + j - 1$, $1 \le i \le \frac{n}{2}$ and $1 \le j \le \frac{n}{2}$

Then form $A_{22} = -A_{11}$

Set $a_{i+n/2,\, j+n/2} = -a_{ij}$ for $i, j = 1$ to $n/2$

Then form A_{12} as $A_{12} = k(I - A_{11})$

One can also take $k(I + A_{11})$ that means

$a_{i,j+\frac{n}{2}} = k(1 - a_{ij})$ *for* $i = j = -ka_{ij}$ for

$i \ne j$ with $i,\ j = 1$ *to* $n/2$

Form A_{21} as $A_{21} = \frac{1}{k}(I + A_{11})$

Thus $a_{i+n/2}, j = \frac{1}{k}(1 + a_{ij})$ for $i = j = \frac{a_{ij}}{k}$ *for* $i \ne j$

$i \ne j$ with $i,\ j = 1$ *to* $n/2$

Finally formulate A.

Example: For 6×6 random matrix (modulo 13)
s = seed value = 5, t = multiplier 7, k =3, then

$$A_{11} = \begin{bmatrix} 5 & 9 & 11 \\ 12 & 6 & 3 \\ 8 & 4 & 2 \end{bmatrix},\ A_{22} = \begin{bmatrix} 8 & 4 & 2 \\ 1 & 7 & 10 \\ 5 & 9 & 11 \end{bmatrix},$$

$$A_{12} = 3(I - A_{11}) = \begin{bmatrix} 1 & 12 & 6 \\ 3 & 11 & 4 \\ 2 & 1 & 10 \end{bmatrix}$$

$$A_{21} = \frac{1}{3}\left[I + A_{11}\right] = \begin{bmatrix} 2 & 3 & 8 \\ 4 & 11 & 1 \\ 7 & 10 & 1 \end{bmatrix}$$

So $A = \begin{bmatrix} 5 & 9 & 11 & 1 & 12 & 6 \\ 12 & 6 & 3 & 3 & 11 & 4 \\ 8 & 4 & 2 & 2 & 1 & 10 \\ 2 & 3 & 8 & 8 & 4 & 2 \\ 4 & 11 & 1 & 1 & 7 & 10 \\ 7 & 10 & 1 & 5 & 9 & 11 \end{bmatrix}$.

5. Image Encryption by the Cryptosystem

We note that Hill cipher can be adopted to encrypt grayscale and color images. For grayscale images, the modulus will be 256 (the number of levels is considered as the number of alphabets). In the case of color images, first decompose the color image into (R-G-B) components. Second, encrypt each component (R-G-B) separately by the algorithm. Finally, concatenate the encrypted components together to get the encrypted color image [10]. We have taken different images and encrypted them using the Hill cipher algorithm and the results are shown in Figure 1. It is clearly noticeable from the Figure 1 (b, d, and f), that algorithm works for different gray scale as well as colour images in which the pixels are uniformly distributed. But in Figure 2 (b, e) it is found that the image is not properly encrypted because of the background of the image of same colour or gray level. This drawback removed by scrambling the resulting image from the algorithm using a random matrix which is used as another secret key. It is clearly noticeable from the Figure 2 (c, f).

6. Conclusion

This paper suggests efficient method for encryption of image by self-invertible matrix with Hill Cipher algorithm. These methods encompass less computational complexity as inverse of the matrix is not required while decrypting in Hill Cipher. This proposed method for generating self-invertible matrix can also be used in other algorithms where matrix inversion is required. Although the algorithm presented in this paper aims at image encryption, it is not just limited to this area and can be widely applied in other information security fields such as video encryption.

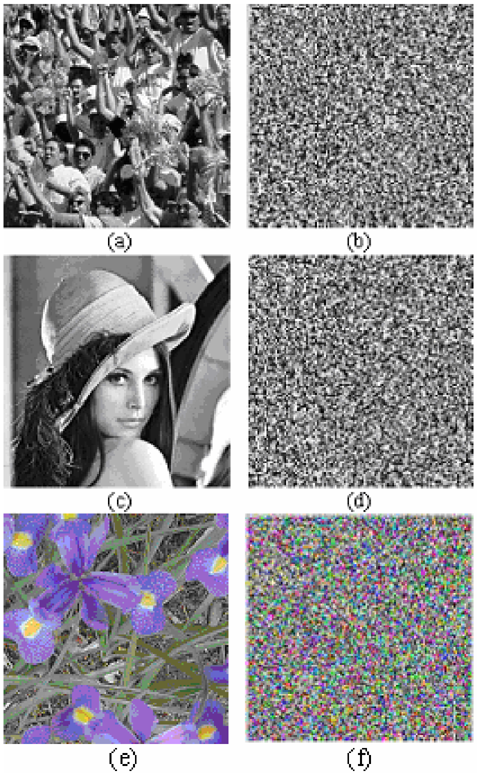

Figure 1. Original images (a, c, e) and corresponding encrypted images (b, d, f)

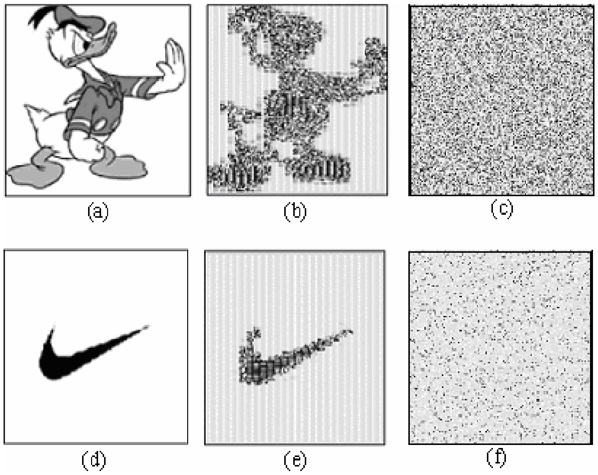

Figure 2. Original images (a, d) and corresponding encrypted images (c, f)

7. References

[1] Imai H., Hanaoka G., Shikata J., Otsuka A., Nascimento A. C., "Cryptography with Information Theoretic Security", Information Theory Workshop, 2002, Proceedings of the IEEE, 20-25 Oct 2002.

[2] Stallings, W. Cryptography and Network Security. 2005. 4th edition, Prentice Hall.

[3] Overbey, J., Traves, W., Wojdylo, J., 2005. "On the keyspace of the Hill cipher", *Cryptologia*, 29(l):59-72.

[4] Saeednia, S., 2000. "How to make the Hill cipher secure", *Cryptologia*, 24(4),:353-360.

[5] Bibhudendra Acharya, Sarat Kumar Patra, and Ganapati Panda. "A Novel Cryptosystem Using Matrix Transformation". Proceedings of SPIT-IEEE Colloquium & International Conference. Vol. 4, pp. 92-95, 2008.

[6] Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, and Saroj Kumar Panigrahy. "Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm". *International Journal of Security* (CSS Journals). Vol. 1, Issue. (1), pp. 14-21, 2007.

[7] Petersen, K., 2000. Notes on Number Theory and Cryptography.
http://www.math.unc.edu/Faculty/petersen/Coding/cr2.pdf

[8] Barr T.H., *Invitation to cryptography*, Prentice Hall, 2002.

[9] Lerma, M.A., 2005. Modular Arithmetic.
http://www.math.northwestern.edu/~mlerma/problem_solving/results/modular_arith.pdf.

[10] Li, S., Zheng, X., 2002. "On the Security of an Image Encryption Method", ICIP2002.
http://www.hooklee.com/Papers/ICIP2002.pdf.