Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm

Saroj Kumar Panigrahy
Department of CSE
National Institute of Technology
Rourkela, 769 008, Orissa, India
Ph: +91-9438003014
skp.nitrkl@gmail.com

Bibhudendra Acharya
Department of ECE
National Institute of Technology
Rourkela, 769 008, Orissa, India
Ph: +91-9937376028
bibhudendra@gmail.com

Debasish Jena
Department of MCA
Centre for IT Education
Bhubaneswar, India-751 010
Ph: +91-9437230284
debasishjena@hotmail.com

ABSTRACT
The Hill cipher algorithm is one of the symmetric key algorithms that have several advantages in data encryption. But, the inverse of the key matrix used for encrypting the plaintext does not always exist. Then if the key matrix is not invertible, then encrypted text cannot be decrypted. In the Self-invertible matrix generation method the key matrix used for the encryption is self-invertible. So, at the time of decryption we need not to find the inverse of the key matrix. This paper presents image encryption technique using the Hill cipher. Here we presented a proposed method of generating self-invertible matrix for Hill Cipher algorithm. Moreover this method eliminates the computational complexity involved in finding inverse of the matrix while decryption. However, a main drawback of this algorithm is that it encrypts identical plaintext blocks to identical ciphertext blocks and 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. But it works well for all other types of gray scale images as well as colour images.

Categories and Subject Descriptors
E.3 **[DATA ENCRYPTION]**: Code Breaking – *Algorithms, Reliability, Security.*

General Terms
Algorithms, Reliability, Security.

Keywords
Cryptography, Hill Cipher, Image Encryption, Security.

1. INTRODUCTION
Owing to the advance in network technology, information security is an increasingly important problem. 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, electronic commerce 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 [2].

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 [9]. 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 is a block cipher that 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 [6, 8].

In this paper, we proposed a method of generating self-invertible key matrix which can be used in Hill cipher algorithm. The objective of this paper is to overcome the drawback of using a random key matrix in Hill cipher algorithm for encryption, where we may not be able to decrypt the encrypted message, if the key matrix is not invertible. Also the computational complexity can be reduced by avoiding the process of finding inverse of the matrix at the time of decryption, as we use self-invertible key matrix for encryption. Using this key matrix we encrypted gray scale as well as colour images. Our algorithm works well for all types of gray scale as well as colour images except for the images with background of same gray level or same colour,

ICAC Conference'08, February 21–22, 2008, Chikhli, M.S.INDIA.

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, proposed method for generating self-invertible matrices is presented. Image encryption and results are discussed in section 5. Finally, section 6 describes the concluding remarks.

2. HILL CIPHER

It is developed by the mathematician Lester Hill in 1929. The core of Hill cipher is matrix manipulations. For encryption, algorithm takes m successive plaintext letters and instead of that substitutes m cipher letters. In Hill cipher, each character is assigned a numerical value like $a = 0, b = 1, \ldots, z = 25$ [5, 9]. The substitution of ciphertext letters in the place of plaintext letters leads to m linear equation. For $m = 3$, the system can be described as follows:

$$\begin{aligned} C_1 &= (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26 \\ C_2 &= (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26 \\ C_1 &= (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 26 \end{aligned} \quad \ldots (1)$$

This case can be expressed in terms of column vectors and matrices:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \quad \ldots (2)$$

or simply we can write as $C = KP$, where C and P are column vectors of length 3, representing the plaintext and ciphertext respectively, and K is a 3×3 matrix, which is the encryption key. All operations are performed $\bmod 26$ here. Decryption requires using the inverse of the matrix K. The inverse matrix K^{-1} of a matrix K is defined by the equation $KK^{-1} = K^{-1}K = I$, where I is the Identity matrix. But the inverse of the matrix does not always exist, and when it does, it satisfies the preceding equation. K^{-1} is applied to the ciphertext, and then the plaintext is recovered [2, 6]. In general term we can write as follows:

For encryption:

$$C = E_k(P) = K_p \quad \ldots (3)$$

For decryption:

$$P = D_k(C) = K^{-1}C = K^{-1}K_p = P \quad \ldots (4)$$

If 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 [5].

3. MODULAR ARITHMETIC

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

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

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

Addition:

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

Negation:

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

Subtraction:

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

Multiplication:

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

Division:

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

The following exhibits the 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:

$$(0 + a) \bmod p = a \bmod p$$
and $$(1 * a) \bmod p = a \bmod p$$

Inverses:

For each $x \in Z_p$, $\exists y$ such that

$$(x + y) \bmod p = 0 \text{ then } y = -x$$

For each $x \in Z_p$ $\exists y$ such that $(x * y) \bmod p = 1$

4. PROPOSED METHOD FOR GENERATING SELF-INVERTIBLE KEY MATRIX

A is called a self-invertible matrix if $A = A^{-1}$. The analysis presented here for generation of self-invertible key matrix is valid for matrix of +ve integers, that are the residues of modulo arithmetic of a number [1].

4.1 Method of Generating Self-Invertible Key Matrix

Let $A = \left[\begin{array}{c|ccc} a_{11} & a_{12} & \dots & a_{1n} \\ \hline a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{array}\right]$

be an $n \times n$ self-invertible matrix partitioned into $A = \left[\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array}\right]$

A_{11} is a 1×1 matrix = $[a_{11}]$,

A_{12} is a $1 \times (n-1)$ matrix = $[a_{12} \quad a_{13} \dots \quad a_{1n}]$,

A_{21} is a $(n-1) \times 1$ matrix = $\begin{bmatrix} a_{21} \\ a_{31} \\ \dots \\ a_{n1} \end{bmatrix}$, and

A_{22} is a $(n-1) \times (n-1)$ matrix = $\begin{bmatrix} a_{22} & a_{23} & \dots & a_{2n} \\ a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots \\ a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix}$.

So, $A_{12} A_{21} = I - A_{11}^2 = 1 - a_{11}^2$ … (5)

and $A_{12}(a_{11} I + A_{22}) = 0$ … (6)

Also, $a_{11} =$ – (one of the Eigen values of A_{22} other than 1)

Since $A_{21} A_{12}$ is a singular matrix having the rank 1,

and $A_{21} A_{12} = I - A_{22}^2$ … (7)

So, A_{22}^2 must have rank of $(n-2)$ with Eigen values +1 of $(n-2)$ multiplicity.

Therefore, A_{22} must have Eigen values ± 1.

It can also be proved that the consistent solution obtained for elements A_{21} & A_{12} by solving the equation (7) term by term, will also satisfy the equation (5).

Algorithm:

1. Select A_{22}, a non-singular $(n-1) \times (n-1)$ matrix which has $(n-2)$ number of Eigen values of either +1 or −1 or both.
2. Determine the other Eigen value λ of A_{22}.
3. Set $a_{11} = -\lambda$.
4. Obtain the consistent solution of all elements of A_{21} and A_{12} by using the equation (7).
5. Formulate the matrix.

Example: (For modulo 13)

Let $A_{22} = \begin{bmatrix} 9 & 6 & 10 \\ 12 & 10 & 2 \\ 5 & 3 & 4 \end{bmatrix}$ which has Eigen values $\lambda = \pm 1,\ 10$.

So, $A_{11} = [3]$, and one of the consistent solutions is $A_{12} = [11 \quad 9 \quad 4]$,

and $A_{21} = \begin{bmatrix} 10 \\ 2 \\ 5 \end{bmatrix}$.

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

Another consistent solution is

$A_{12} = [1 \quad 2 \quad 11]$, and $A_{21} = \begin{bmatrix} 6 \\ 9 \\ 3 \end{bmatrix}$.

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

5. IMAGE ENCRYPTION USING HILL CIPHER AND RESULTS

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 [4].

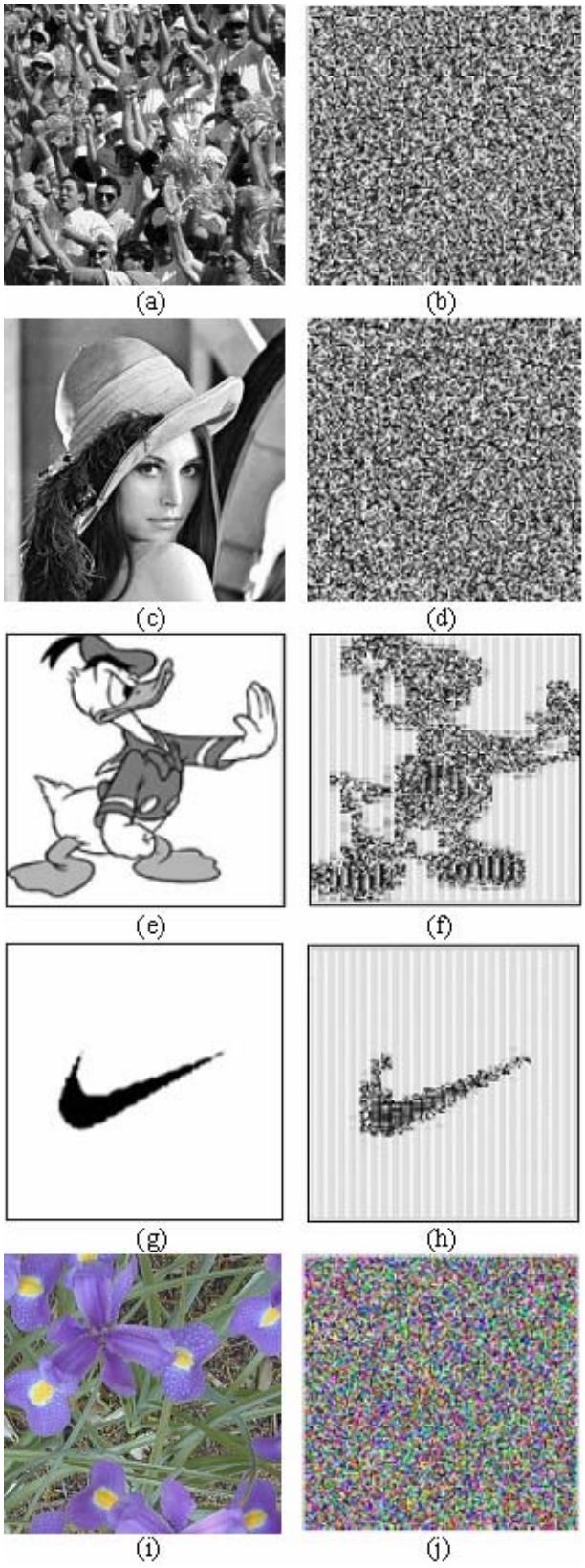

Figure. 1. Original images (a, c, e, g, i) and corresponding encrypted images (b, d, f, h, j)

We have taken different images and encrypted them using the Hill cipher algorithm and the results are shown below in Figure 1. It is clearly noticeable from the Figure 1(a, c, i), that our proposed algorithm works for different gray scale as well as colour images in which the pixels are uniformly distributed. But in Figure 1(e, g) it is found that our algorithm could not able to decrypt the image properly because of the background of the image of same colour or gray level. This drawback can also be removed by adjusting the key matrix [8].

6. CONCLUSION

Hill cipher is a block cipher that 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 [6, 8]. However, Hill cipher succumbs to a known plaintext attack and can be easily broken with such attacks. This paper suggests efficient methods for generating self-invertible matrix for 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.

7. REFERENCES

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

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

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

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

[5] Menezes, A. J., P.C. Van Oorschot, S.A. Van Stone. 1996. Handbook of Applied Cryptography. CRC press.

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

[7] Petersen, K., 2000. Notes on Number Theory and Cryptography.

http://www.math.unc.edu/Faculty/petersen/Coding/cr2.pdf.

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

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