2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies

H-S-X Cryptosystem and Its Application to Image Encryption

Bibhudendra Acharya[1,3], Sambit Kumar Shukla[2], Saroj Kumar Panigrahy[2],Sarat Kumar Patra[3],and Ganapati Panda[3]

[1]Department of E & TC, NIT Raipur, Chhattisgarh-492010, India
[2]Department of CSE, NIT Rourkela, Orissa-769008, India
[3]Department of ECE, NIT Rourkela, Orissa-769008, India
bibhudendra@gmail.com, sambit_shukla@yahoo.com, skp.nitrkl@gmail.com,{skpatra, gpanda}@nitrkl.ac.in

***Abstract*—Information security is an important issue. Today's encryption technologies can be traced back to the earliest ciphers, and have grown as a result of evolution. The first ciphers were cracked, so new, stronger ciphers emerged. Code breakers set to work on these and eventually found flaws, forcing cryptographers to invent better ciphers and so on. Hill Cipher is one of the most famous symmetric cryptosystem that can be used to protect information from unauthorized access. Hill cipher is a polygraph substitution cipher based on linear algebra. it was the first polygraph cipher which was practical to operate on more than three symbols at once, Hill Cipher has many advantages in data encryption. First, it is resistant to the frequency letter analysis. It's also very simple since it uses matrix multiplication. Finally, it has high speed and high throughput. However, noninvertible key matrix over Z_m is the main disadvantage of Hill Cipher, because few of the matrices have inverses over Z_m. This means that the encrypted text can't be decrypted. Moreover, 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. The objective of this paper is to encrypt an image using a technique different from the conventional one. In this paper, a novel encryption technique has been proposed which we name H-S-X (Hill-Shift-XOR) encryption. The scheme is relatively slow but quite reliable technique where cryptanalysis is quite difficult. It also injects more diffusion and confusion which are the two important attributes of a powerful encryption technique. A comparative study of the proposed encryption scheme and the existing Hill cipher scheme is made. The output encrypted images reveal that the proposed technique is quite reliable and robust.**

Keywords- cryptosystem, encryption, decryption, Hill Cipher.

I. INTRODUCTION

In the current world that we live in, of rapid growing technology, and especially reliance on the Internet for our daily lively hood (Banking, shopping, entertainment, news), and also with current crimes (Identity-theft, hacking, spyware), computer security is becoming more and more important. By "computer security", we often refer to addressing three important aspects of a computer-related system: Confidentiality, integrity and availability. Encryption clearly addresses the need for confidentiality of data, both in storage and transmission. Popular application of multimedia technology and increasingly transmission ability of network gradually leads us to acquire information directly and clearly through images [1, 2, 3].

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. 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 cipher. 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 [4]. 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 [5, 6, 7].

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, noninvertible key matrix over Z_m is the main disadvantage of Hill Cipher, because few of the matrices have inverses over Z_m. This means that the encrypted text can't be decrypted. And also it can be easily broken with a known plaintext attack revealing weak security. In this paper, we have proposed a novel technique which is a modified version of Hill cipher algorithm for image encryption named H-S-X (Hill-Shift-XOR) which can be applied to any type of images whether they are colour or gray. It overcomes the problems raised by the original Hill cipher while encrypting

978-0-7695-3915-7/09 $26.00 © 2009 IEEE
DOI 10.1109/ACT.2009.183

blocks of same gray level pixels. It is also more resistant to brute-force, known plaintext as well as chosen plain text attack.

The organization of the paper is as follows. Following the introduction, the basic concept of Hill Cipher is outlined in section II. Section III presents the proposed method of image encryption using H-S-X algorithm. In Section IV Invertible random key matrix generation methods outlined. Simulation results are discussed in section V. Finally, section VI provides the concluding remarks.

II. HILL CIPHER

Hill cipher was developed by the mathematician Lester Hill in 1929. The core of Hill cipher is matrix manipulations. For encryption, the algorithm takes m successive plaintext letters and substitutes with m cipher letters. In Hill cipher, each character is assigned a numerical value like $a = 0$, $b = 1$, ... , $z = 25$. 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:

$$\begin{aligned} C_1 &= (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26 \\ C_2 &= (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26 \\ C_3 &= (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 26 \end{aligned} \quad (1)$$

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

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

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 mod 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. In general term we can write as follows:

For encryption:

$$C = E_k(P) = KP \quad (3)$$

For decryption:

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

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 [8, 9].

III. IMAGE ENCRYPTION USING H-S-X TECHNIQUE

As we note that Hill cipher can be adopted to encrypt grayscale and color images, our H-S-X algorithm can also be used for 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 color image is decomposed 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, 11].

In this technique, Encryption is done in 3 sub-steps. These steps if repeated sufficiently leads to quite a strong encryption at the cost of encryption time. Our proposed algorithm is resistant to brute-force attacks, known plaintext attacks as well as chosen plaintext attacks. The algorithm is given below and the block diagram for the encryption process is presented in Figure 1.

Algorithm H-S-X:

Step1: 2-level Hill Cipher is applied to original Image using a preferably random matrix (having odd determinant).

Step2: Appropriate P_1 and P_2 values are selected for the row and column shifting function where, P_1 and P_2 are generators for the elements co-prime to congruence modulo n and m respectively. These values can be extracted from a predetermined table for different n values.

2a: i[th] row pixel values circularly right shifted according to the formula

$$\left\lfloor P_1^{i+1} + ceil(i/k) * K_{r_{i(\bmod k)}} \right\rfloor (\bmod \ n) \quad (5)$$

where,

i – Corresponding row number,

k – Size of key matrix used for shifting,

$K_{r_{i(\bmod k)}}$ – Sum of the values of the i[th] row of the key matrix,

n – No. of columns in the original image,

P_1 – Generator for co-prime numbers congruence modulo n,

$ceil()$ – The Ceiling function.

2b: j[th] row pixel values circularly down shifted according to the formula

$$\left\lfloor P_2^{j+1} + ceil\,(j/k) * K_{c_{j(\bmod k)}} \right\rfloor (\bmod \ m) \quad (6)$$

where,

j – Corresponding column number,

k – Size of key matrix used for shifting,

$K_{c_{j(\bmod k)}}$ – Sum of the values of the j[th] column of the key matrix,

m – No. of rows in the original image,

P_2 – Generator for co-prime numbers congruence modulo m,

$ceil()$ – The Ceiling function.

Step3: Block wise XOR operation is performed onto resultant image using the key matrix or one of its permutations or a masked version of the key.

All the above operations are performed modulo 256 and

on 8-bit gray (or 24-bit color) images.

IV. INVERTIBLE RANDOM KEY MATRIX GENERATION

In this section, we present algorithms to generate modular non-singular key-matrix for Hill cipher. The matrix generated in invertible matrix formulation scheme is always invertible. So these matrices can be used as a key matrix in Hill cipher scheme. Here we have described two invertible matrix formulation methods. [12-16]

1st Method:

1. Select a random matrix A of size $m \times m$
2. If it is singular and of rank $m-1$, then select principal-minor of matrix A of $(m-1)\times(m-1)$ size which is non-singular.
3. Then add 1 to the diagonal element which is not included in non-singular.

$$A = \begin{bmatrix} a_{11} & . & . & a_{1n} \\ . & . & . & . \\ . & . & . & . \\ a_{m1} & . & . & a_{mn} \end{bmatrix} \quad (7)$$

If rank of A is $m-1$ then select A_{ii} = Principal minor eliminating i^{th} row and i^{th} column of A, such that ΔA_{ii} = is non-zero then $a_{ii} \leftarrow a_{ii} + 1$

To generate the above method: If the rank of A is l,

- Select non-singular principal-minor $(l \times l)$.
- Then add 1 all the principal diagonal elements which are not included in the principal-minor.

Above method has one limitation as one has to determine the rank of the matrix.

2nd method:

$$\text{Matrix } A = \begin{bmatrix} a_{11} & . & . & a_{1n} \\ . & . & . & . \\ . & . & . & . \\ a_{m1} & . & . & a_{mn} \end{bmatrix}$$

where,

a_{11} = seed number (generation of random number)

$a_{12} = (a_{11} \times t) \bmod n$, where t is any number prime to n

$a_{13} = (a_{12} \times t) \bmod n$

...

$a_{21} = (a_{1m} \times t) \bmod n$

Such matrix A has rank one, if Trace $A \bmod n \neq 0$ then $K = A + I$ provided that the eigen value of A is not equal to $(n-1)$.

K can be found by adding 1 to any $(m-1)$ diagonal elements.

And if Trace of $A \bmod n = 0$

Then $K = A + aI$, where a = any scalar.

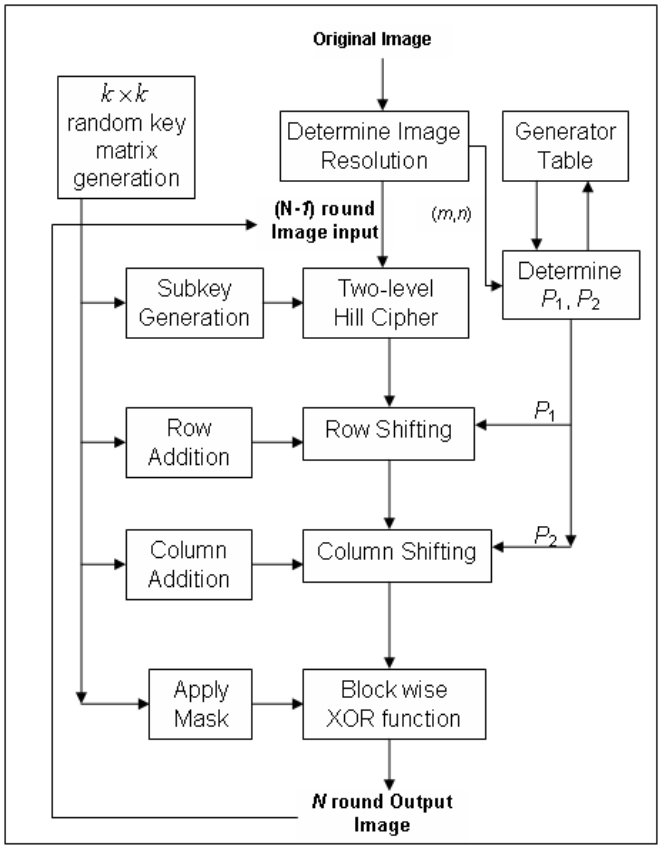

Figure 1. The block diagram for proposed H-S-X algorithm.

V. EXPERIMENTAL RESULTS

We have taken different images and encrypted them using original Hill and our proposed H-S-X algorithm and the results are shown in Figure 2 and 3. It is clearly noticeable from the Figure 2 (f, h), that original Hill Cipher can't encrypt the images properly if the image consists of large area covered with same color or gray level. But our proposed H-S-X algorithm works fine for all types of images including gray scale, color and also binary images. In Figure 3, it is found that proposed H-S-X algorithm can able to encrypt the image properly as compared to original Hill Cipher algorithm.

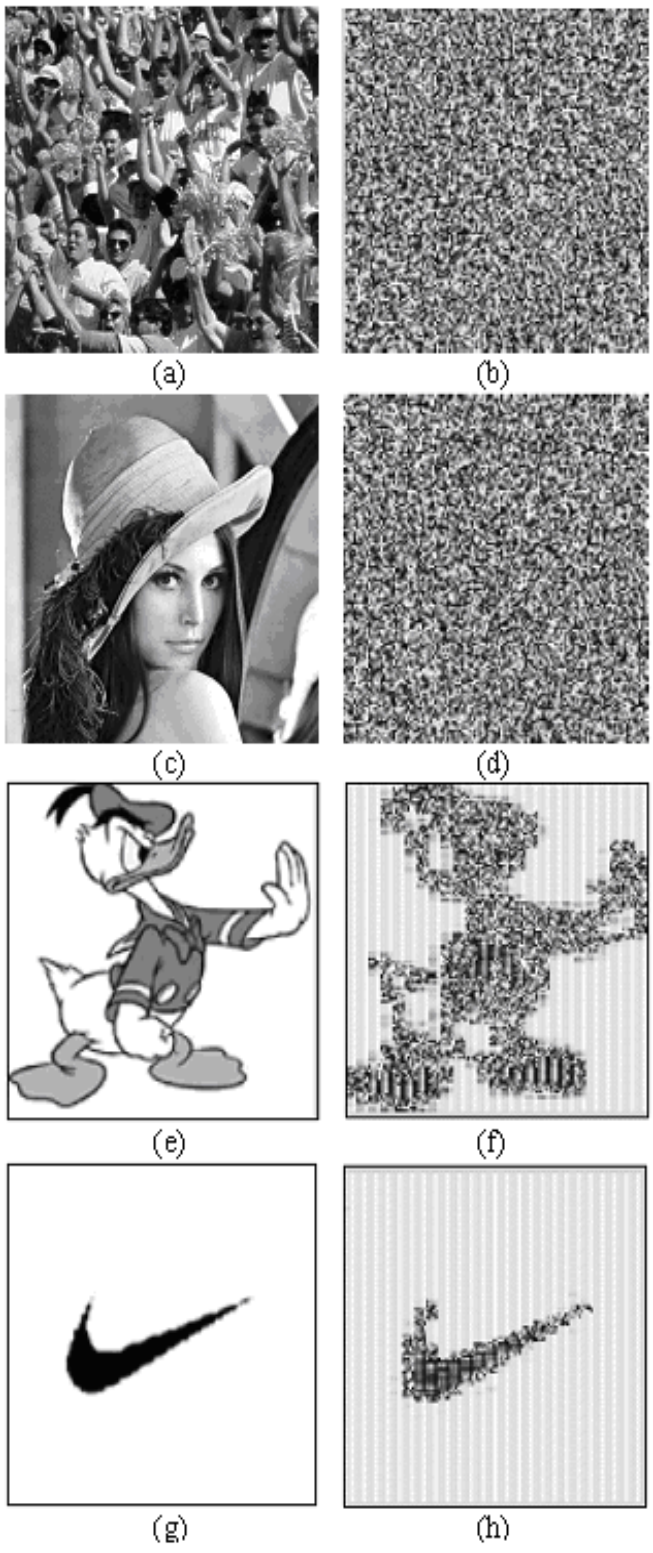

Figure 2. Original images (a, c, e, g) and corresponding encrypted images by original Hill Cipher Algorithm (b, d, f, h).

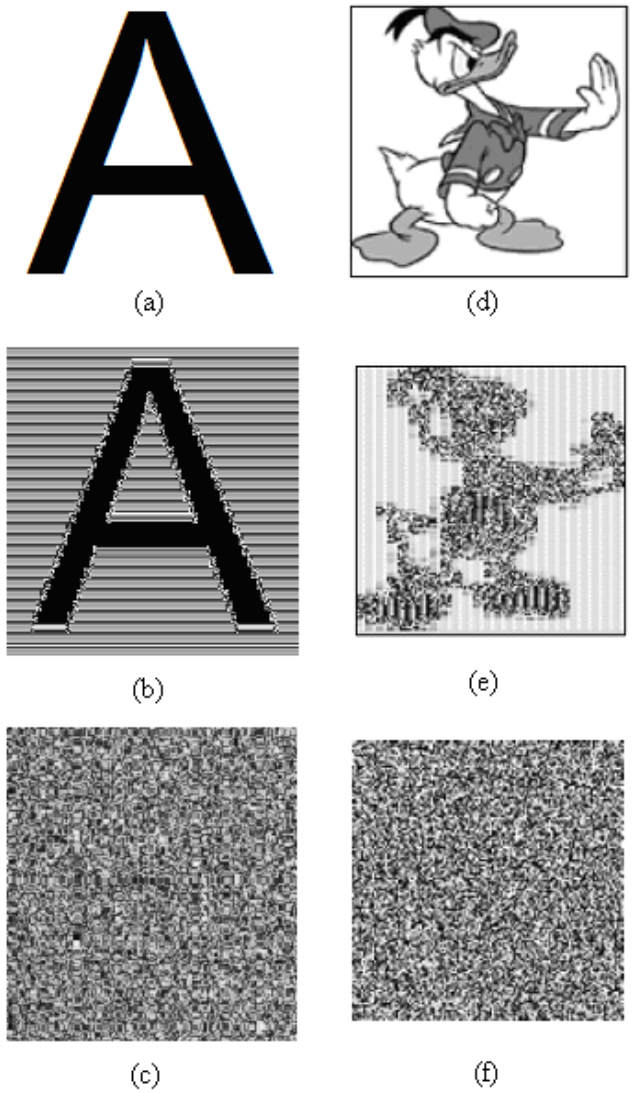

Figure 3. (a,d) Original images, (b,e) corresponding encrypted images by original Hill Cipher algorithm and (c,f) by our proposed H-S-X algorithm

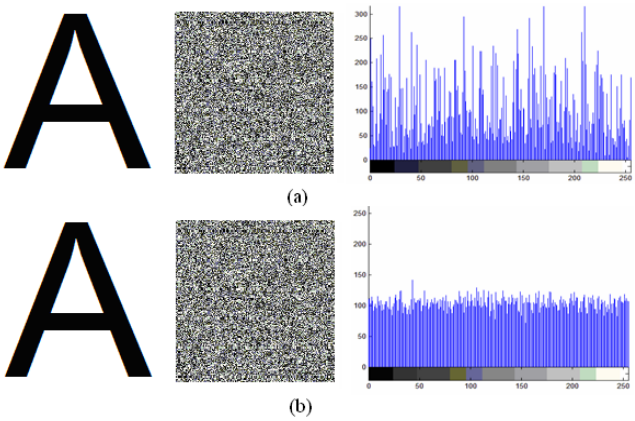

Figure 4. Comparison of 1-round and 4-rounds of H-S-X technique (4-round destructs the image more)

VI. CONCLUSION

H-S-X algorithm is more secure to brute force attacks as compared to original Hill cipher algorithm. A Brute Force Attack requires 2^{8n^2} number of key generations; where n is the order of key matrix. H-S-X is a slow but strong encryption technique which can provide satisfactory results against the normal Hill cipher technique. The proposed scheme is resistant against known plaintext attacks due to the shifting steps involved in Step2. It is also resistant to Chosen Plaintext attacks, if the H-S-X steps are repeated which is shown in Figure. 4. From the histograms it is clear that, the iteration leads to a gradual avalanche effect and hence thwarts the attacks. It incorporates increased diffusion and confusion. Here, key size itself can be used as a secret key as chosen Plaintext techniques cannot reveal key size.

REFERENCES

[1] G.R. Blakley, Twenty years of cryptography in the open literature, Security and Privacy 1999, Proceedings of the IEEE Symposium, 9-12 May 1999.

[2] W.-K. Chen, Scott Sutherland, "An Introduction of Cryptography", MSTP MATH WORKSHOP, 2005.

[3] Forouzan - Behrouz .A "Cryptography And Network Security", McGraw Hill. 2008.

[4] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall. 2006.

[5] Ismail, I.A., Amin, M., Diab, H., 2006. How to repair the Hill Cipher. J. Zhejiang Univ. Sci. A, 7(12):2022-2030.

[6] Jeffrey Overbey, William Traves, and Jerzy Wojdylo, "On the Keyspace of the Hill Cipher", Cryptologia, 29(1), January 2005, pp59-72.

[7] Adam J. Elbirt, Christof Paar "An Instruction-Level Distributed Processor for Symmetric-Key Cryptography", IEEE Transactions on Parallel and Distributed Systems, May 2005.

[8] Lester S. Hill, "Cryptography in an Algebraic Alphabet", The American Mathematical Monthly 36, June-July 1929, pp306–312.

[9] Lester S. Hill, "Concerning Certain Linear Transformation Apparatus of Cryptography", The American Mathematical Monthly 38, 1931, pp135–154.

[10] Chengqing Li, Dan Zhang, and Guanrong Chen, "Cryptanalysis of an image encryption scheme based on the Hill cipher", J. of Zhejiang University SCIENCE, 2008.

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

[12] 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, CSC Journals, Vol. 1, Issue 1, pp. 14-21, 2007.

[13] Bibhudendra Acharya, Debasish Jena, Sarat Kumar Patra and Ganapati Panda, "Invertible, Involutory and Permutation Matrix Generation Methods for Hill Cipher System", International Conference on Advanced Computer Control (ICACC 2009), Singapore, pp.410-414, 2009.

[14] Autar K. Kaw. "Introduction to Matrix Algebra", University of South Florida, 2002.

[15] Lerma, M.A., 2005. Modular Arithmetic. http://www mathnorth western .edu/~mlerma/problem_solving/results/modular_arith.pdf.

[16] V.U.K. Sastry, S. Udaya Kumar, and A. Vinaya babu, "A Large Block Cipher Using Modular Arithmetic Inverse of a Key Matrix and Mixing of the Key Matrix and the Plaintext", Journal of Computer Science vol. 2 (9), 2006, pp. 698-703, New York, 2006