International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 17 (2014), pp. 1895-1901
© International Research Publications House
http://www. irphouse.com

Image Encryption and Decryption using Modified Hill Cipher Technique

Prerna[#1], Urooj[#2], Meena kumari[#3], Jitendra Nath shrivastava[#4]

*[#1]M.Tech students of Computer Science and Engineering,
Invertis University Bareilly, Uttar Pradesh, India*

Abstract

Today's world is a digital world in which paper and ink have been replaced by much more versatile and practical covers for hiding messages video, audio digital documents, and images. Cryptography is the study of encoding and decoding secret messages videos and images. In the language of cryptography, codes are known as ciphers, encoded messages are known as plaintext, and coded messages are known as cipher text. The main objective of proposed algorithm is to encrypt an image using a technique different from the traditional Hill Cipher. In this paper a Modified Hill encryption and decryption technique has been proposed which uses an involuntary key matrix. The scheme is a fast encryption scheme which provides a solution of problems of encrypting the images with homogeneous background. Proposed algorithm for encrypting and decrypting images is quite reliable and robust. In proposed algorithm we generate a function which select a random key matrix and then encrypt the image using the key matrix. For the decryption we again use this key matrix to get the original image.

Keywords: Image Encryption, Image Decryption, Hill Cipher, Image Encryption, Modified Hill Cipher.

INTRODUCTION

Today, Cryptography is crucial technology that is used in applications present in technologically advanced societies; examples include the security of ATM cards, E-Commerce, and computer passwords, which all depend on cryptography. It is used in Secure Image transmission on internet these days.Until modern times, cryptography referred almost exclusively to encryption, the process of converting ordinary information into encoded format (i.e., cipher text). Decryption is the reverse process of converting unintelligible cipher text into plaintext. A cipher is a pair of algorithms which creates the encryption and the reversing decryption. Hill cipher is a type of monoalphabetic polygraphic substitution cipher [1]. 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 [1].We proposed a technique of generating self-invertible key matrix which can be used in Modified Hill cipher algorithm. The objective of our work is to overcome the drawback of using a random key matrix in Hill cipher algorithm for encryption, where encrypted message cannot be decrypted until the key matrix is not invertible. Computational complexity can also 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. Our algorithm encrypt gray scale as well as color images using this key matrix. This algorithm works well for all types of gray scale as well as color images except for same gray level images or same color images.

Hill Cipher

Hill cipher is a substitution technique in symmetric encryption developed by **Lester Hill** in **1929**. The algorithm takes m successive plaintext letters and substitutes for them m cipher text letters. In Hill cipher, each character is assigned a numerical value like $a = 0$, $b = 1$, $z = 25$ [5, 9]. The substitution of cipher text letters in the place of plaintext letters leads to m linear equation. For $m = 3$, the system can be described as follows**:**

$$c_1 = (k_{1\,1}p_1 + k_{1\,2}p_2 + k_{1\,3}p_3) \bmod 26$$
$$c_1 = (k_{1\,1}p_1 + k_{1\,3}p_2 + k_{1\,3}p_3) \bmod 26$$
$$c_1 = (k_{1\,1}p_1 + k_{1\,3}p_2 + k_{1\,3}p_3) \bmod 26$$

This can be expressed in term of column vectors and matrices:

c1 = k11 k12 k13 p1
c2= k21 k22 k23 p2 mod 26
c3= k31 k32 k33 p3

by the operation of Column matrix we can find it out that $C = KP$, where C and P are column vectors of length 3, representing the plaintext and cipher text 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 cipher text, and then the plaintext is recovered. The term for encryption as follows.

For encryption:

C = Ek (P) = K p

For decryption*:*

P = D_k(C) = K^{-1} (C) = P

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.

PROPOSED SCHEME

Implemented Hill Cipher technique one is cover image which act as key image which is shared by both sender and receiver and other is Informative image. As first step, we add cover image and informative image to obtained resultant image. The gray scale image is passed to the Hill Cipher algorithm to form encrypted image. The encrypted image is communicated over unsecured channel. The encrypted image after receiving by receiver passed to Hill Cipher technique. Receiver first obtained inverse of Key image, K-1. The resulted image which is encrypted is passed to the Hill Cipher to obtain Informative Image. The cover image is subtracted from merged image to obtained informative image. The detail process is summarized in figure 1.In proposed technique author has used hill cipher technique for encrypting image by breaking the image into blocks of length rather than whole image. In this paper image is divided into blocks of length and use hill cipher technique for encrypting blocks of image rather than whole image.

Fig 1: Original image

ALGORITHM FOR PROPOSED SCHEME:

1. A pixel matrix of original image of dimensions $n\times n$ is constructed.
2. The plain image is divided into $n\times n$ symmetric blocks.
3. Generate a random key matrix of $n\times n$
4. For grayscale images, the number of levels is equal the number of alphabets.
5. For color images-

- decompose the color image into (R-G-B) components.
- encrypt each component (R-G-B) separately.
- obtain the cipher image.

6. Find the image matrix of cipher image.
7. Decrypt the image with using the inverse square matrix of the same key.
8. Obtain the original image.

Image Encryption:

Find the pixel matrix of original image.

Randomly generate a key matrix equal to the dimensions of image matrix to be encrypted.

Apply the concept of hill cipher i.e.

$C = E_k (P)$

But in the concept of image we have 256 gray(For example)intensity levels so our approach will work as

$C = E_k (P) \bmod 256$

Where "C" is the matrix of cipher image, "P" is the matrix of original image and "k" is the randomly generated matrix value (key). After applying the concept each and every pixel of original image will substitute by the each and every pixel of cipher image.

Image Decryption:

1. For the decryption we find out the pixel matrix of cipher image.
2. Consider the same value of k (key). As in the hill cipher for the text we had the equation.

$P = D_k (C) = K^{-1} (C) = P$

Same concept work for the image the difference will be only here again we considered the gray scale lave of image i.e. 256 now the equation will look like

$P = D_k (C) = K^{-1} (C) \bmod 256 = P$

EXPERIMENTAL RESULTS:

For evaluation of our proposed technique, we used Matlab tool. We have created 200 by 200 informative image as shown in figure 3. The informative image is used to store some information which is passed through unsecured channel. We apply Hill Cipher technique to perform encryption of informative image. For using Hill Cipher algorithm, we have created key image as shown in figure 2. We used traditional Hill Cipher Technique to perform encryption of informative image using key image. This newly obtained encrypted image is sent on unsecured channel. The intruder, even if received this encrypted image, could not able to get the informative image, because the key image is not available to the intruder. In this way the informative image is encrypted and securely transferred on unsecured channel. After receiving this encrypted image by receiver, receiver has the key image. The first task is to find the inverse of this key image. This inverse key image is used in the decryption process of hill cipher technique to obtain the original informative image. This decrypted image is same as the image originally sent by the sender. Thus the task of hiding informative image and passing through unsecured channel is achieved.

We have taken different images and encrypted them using original Hill and our proposed Advance Hill algorithm and the results are shown below in Figure 2 and 3. It is clearly noticeable from the Figure 2(e, g), that original Hill Cipher can't encrypt the images properly if the image consists of large area covered with same colour orgray level [8]. But our proposed algorithm works for any images with different gray scale as well as colour images.

In Figure 3, it is found that proposed Advance Hill algorithm can able to encrypt the image properly as compared to original Hill Cipher algorithm.

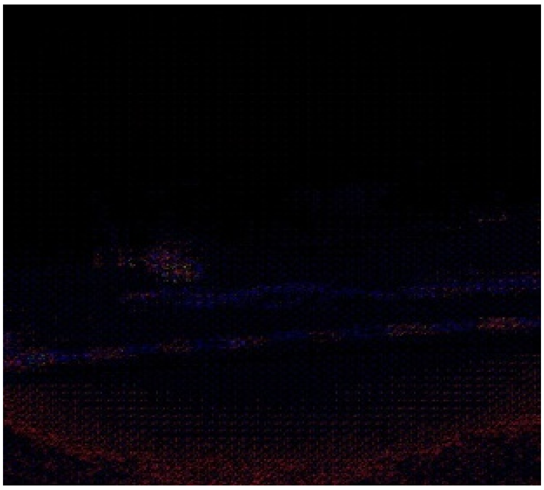


Fig2: encrypted image

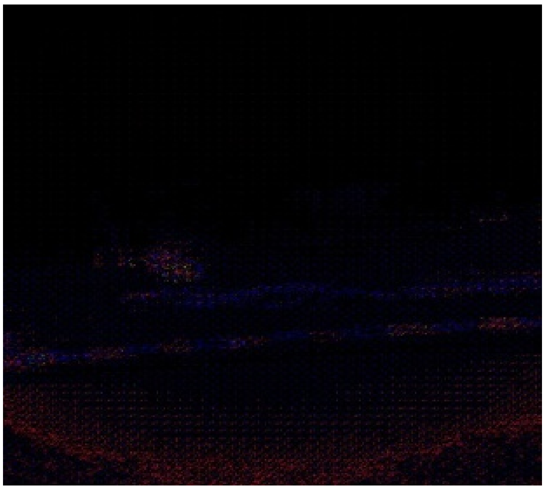


Fig 3:

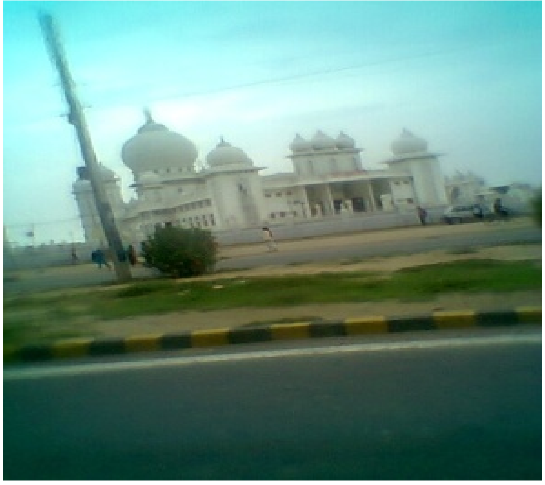
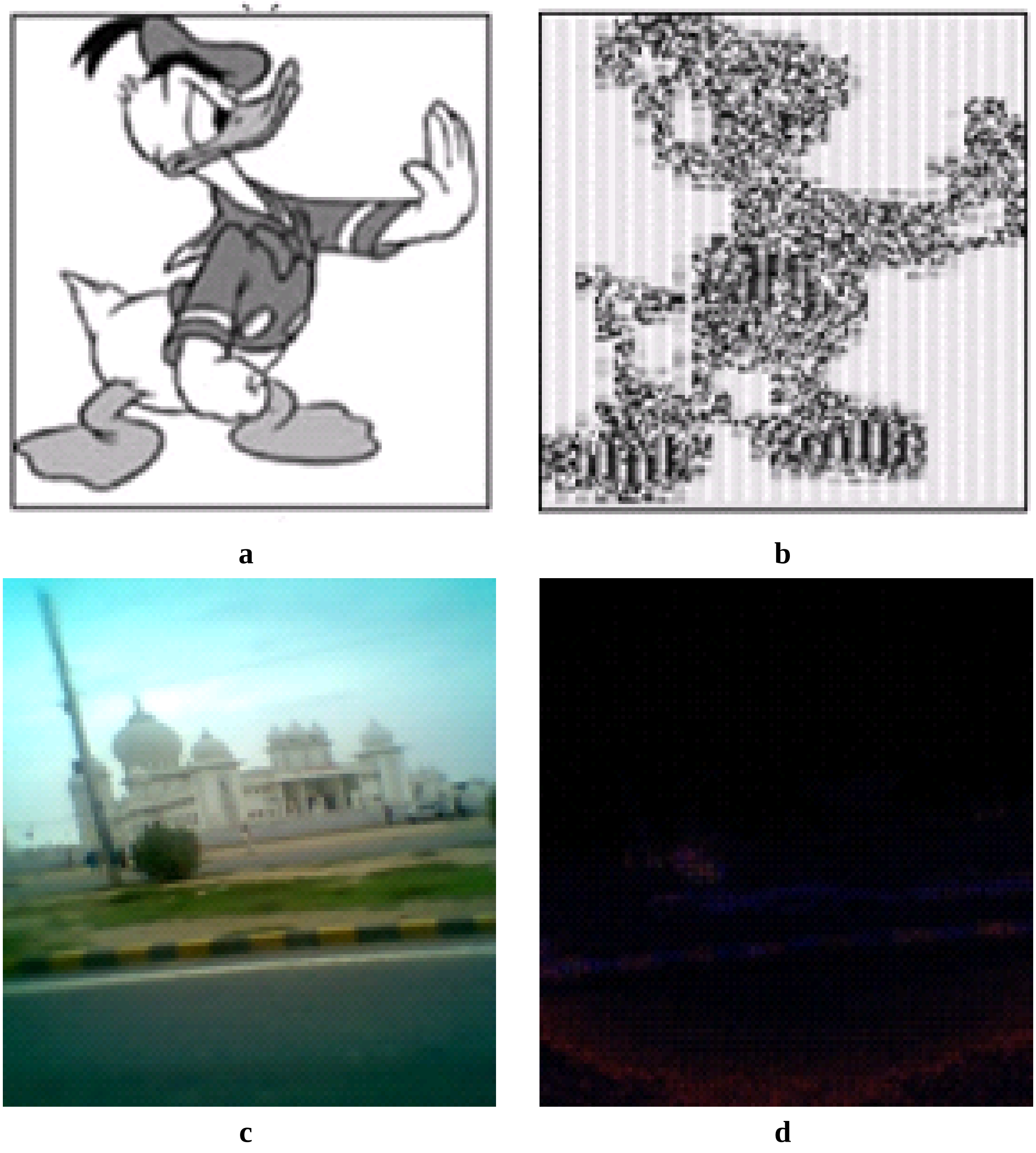


Fig4: decrypted image

Example

Lets compare Images by the original cipher Algorithm and images by our proposed scheme Modified Hill Cipher images (c,d) by original Hill Cipher Algo.



a

b

c

d

Figure.5:. Original images (a) and corresponding encrypted images (b) by original Hill Cipher Algorithm and (c,d) by proposed modify Hill cipher algorithm.

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 project aims at image encryption and decryption, it is not just limited to this area and can be widely applied in other information security fields such as video encryption. This provides the security against the different attacks like brute-force attacks. Proposed Advance Hill algorithm is more secure to brute force attacks as compared to original Hill cipher algorithm. A Brute Force Attack requires 27+8*(*n* / 2)2 number of key generations; where n is the order of key matrix. Advance Hill is a fast encryption technique which can provide satisfactory results against the normal hill cipher technique. The proposed scheme is resistant against known plaintext attacks. So the image encryption with Advance Hill cipher is quick response encryption scheme.

References:

[1] ACEEE International Journal on Signal and Image Processing Vol 1, No. 1, Jan 2010" Image Encryption Using Advanced Hill Cipher Algorithm".

[2] *International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013"*Advance Cryptography Scheme for Data Hiding using Advance Hill cipher & DES".

[3] IEEE paper ofNeil Johnson, Sushil Jajodia, "Exploring Cryptography Research paper of Petersen, K.,on Cryptography.

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

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