ISSN No. 0976-5697

Volume 1, No. 4, Nov-Dec 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Image Encryption using the Standard Hill Cipher

Gaurav Agarwal*
Invertis University
Bareilly, India
gauravagarwal95@gmail.com

Saurabh Singh
Invertis University
Bareilly, India
saurabh.iiet@gmail.com

Meeta Chaudhary
Invertis University
Bareilly, India
meeta.c@invertis.org

Abstract: In the recent decade of cryptography the concept of image played a big role. Hiding image into another image may be a good idea for image encryption. Considerable work is done in this field. There are many ways to encrypt the image but in this paper we are presenting a new technique of image encryption by the standard hill cipher. Hill cipher algorithm is a technique for symmetric key algorithm in which we use the matrix form key for the encrypting the text data. Images are also a matrix of pixels and each pixel has its intensity value. Using this concept 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: Hill Cipher, Image Encryption, Image Processing, cryptography

I. INTRODUCTION

Secure Image transmission on internet has become an important requirement these days. For secure transmission we use the cryptography which plays a important role in the security for communication among various channels. By the techniques involved in cryptography we can transform readable form of message (plaintext) into an unreadable form (cipher text) and vice-versa. In these days cryptography is a part of network security which can be used for encryption of text, audio, video, graphics and other multimedia files. Here we are talking about the image encryption which provides an original image into the encrypted image.

A. *INTRODUCTION TO 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**: [1]**

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

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.

$$C = E_k\,(P)$$

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

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 [10].

II. PRAPOSED WORK

In proposed technique we have used hill cipher technique for encrypting image rather then image.

A. *ENCRYPTION:*

(a) Find the pixel matrix of original image. Randomly generate a key matrix equal to the dimensions of image matrix to be encrypted.

(b) 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.

B. *DECRYPTION*

(a) For the decryption we find out the pixel matrix of cipher image.

(b) 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

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

III. EXPERIMENTAL RESULTS

We have implemented our approach in matlab and following images were used in implementation.

The pixel matrix which we found from this image is

$$\begin{pmatrix} 12 & 65 & 65 & \ldots\ldots\ldots.. \\ 23 & 45 & 45 & \ldots\ldots\ldots.. \\ 23 & 56 & 87 & \ldots\ldots\ldots.. \\ \ldots & \ldots. & \ldots. & \ldots\ldots\ldots.. \end{pmatrix}$$

The randomly generated key matrix by the mat lab [4] similar to the pixel matrix of image is

$$\begin{pmatrix} 407 & 425 & 251 & \ldots\ldots\ldots \\ 452 & 280 & 244 & \ldots\ldots\ldots \\ 63 & 464 & 438 & \ldots\ldots.. \\ \ldots\ . & \ldots. & \ldots. & \ldots\ldots\ldots \end{pmatrix}$$

After getting these two matrixes we applied the encryption scheme according to the hill cipher i.e.

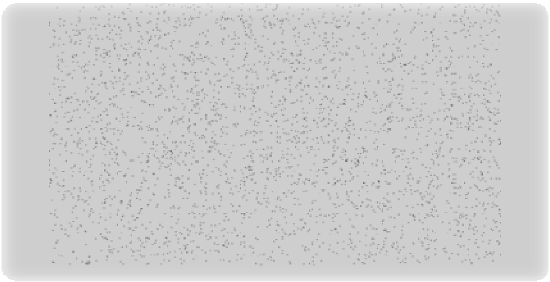
$$C = E_k\ (P) \bmod 256$$

Multiplying these matrix value the final matrix value look like

$$\begin{pmatrix} 212 & 74 & 217 & \ldots\ldots\ldots \\ 0 & 128 & 156 & \ldots\ldots\ldots \\ 66 & 96 & 106 & \ldots\ldots.. \\ \ldots\ . & \ldots. & \ldots. & \end{pmatrix}$$

This is the final matrix value of cipher image the every value of pixel matrix of original image will now substitute by this matrix and the final encrypted image will be.

Original image



Encrypted image

To decrypt the image we again consider the same concept i.e. the pixel matrix of cipher image and the

K^{-1} (inverse of key matrix) which is

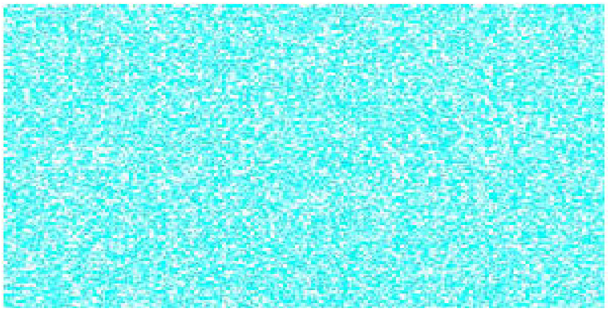
$$\begin{pmatrix} -0.0004 & -0.0029 & -0.0013 \\ 0.0071 & -0.0064 & -0.0006 \\ -0.0075 & 0.0063 & 0.0031 \\ \ldots\ldots\ldots. & \ldots\ldots\ldots\ldots & \end{pmatrix}$$

Now using the algorithm of decryption we have

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

The result shows that from the cipher matrix again we can generate the original matrix same process done on different images result shows as follows.

(A)



(B)

The image (A) shows the original image and the image and finally the image (B) shows the cipher image after the mod 256.

IV. CONCLUSION

This paper gives the efficient way to encrypt an image. This provides the security against the different attacks like brute-force attacks. So the image encryption with stdHill cipher is quick response encryption scheme.

V. REFERENCES

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

[2] Use of image to secure the message with the help of LSB ISSN-0976-4259 Gaurav Agarwal, Saurabh Singh (IJAER).

[3] Y. Rangel-Romero, R. Vega-García, A. Menchaca-Méndez, D. Acoltzi-Cervantes, L. Martínez-Ramos, M.Mecate-Zambrano, F. Montalvo-Lezama, J. Barrón-Vidales, N. Cortez-Duarte, F. Rodríguez-Henríquez, Comments on How to repair the Hill cipher, Journal of JZhejiang Univ SCIENCE A, pp. 1-4, 2007

[4] http://www.mathworks.com/support/books/index.jsp

[5] MATLAB R° / R Reference May 25, 2010 David Hiebeler Dept. of Mathematics and Statistics University of Maine Orono, ME 04469-5752 http://www.math.umaine.edu/~hiebeler

[6] Shuqun Zhang and Mohammed A. Karim, “Color image encryption using double random phase encoding”, Microwave And Optical Technology Letters / Vol. 21, No. 5, June 5 1999, 318-322

[7] I. Ozturk, I.Sogukpinar, "Analysis and comparison of image encryption algorithm," Journal of transactions on engineering, computing and technology December, vol. 3, 2004, p.38. http: //www.enformatika.org/

[8] Hill Ciphers and Modular Linear Algebra Murray Eisenberg November 3, 1999 [9] P. Lin, W. L. Wu, C. K. Wu, \Security analysis of double length compression function based on block cipher," International Journal of Network Security, vol. 4, no. 2, pp. 121-127, 2007.

[9] V. U. K. Sastry, and V. Janaki, \On the modular arithmetic inverse in the cryptology of hill vipher,"Proceedings of North American Technology and Busi- ness Conference, pp. 105, Montreal, Canada, Sep.2005.