International Journal of Pure and Applied Mathematics
Volume 119 No. 15 2018, 485-492
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue
http://www.acadpubl.eu/hub/

A NEW HILL CIPHER ALGORITHM FOR IMAGE ENCRYPTION WITH SELF INVERTIBLE MATRIX

RAJESH KUMAR S[1], PERIYASAMY K[2], MANOJKUMAR S[3], POOMANI S[4], KARUPPIAH S[5]
[1]Assistant Professor, Department of Electronics and Communication Engineering,
V.S.B Engineering College
Karur, India.
e-mail: rajeshkumar26june@gmail.com
[2,3,4,5]Departmentof Electronics and Communication Engineering,
V.S.B Engineering College
Karur, India.
e-mail: kpsammy96@gmail.com, manojece197@yahoo.in, manipoo1991@gmail.com, karuppiahsenthil20@gmail.com

ABSTRACT
This work proposes a new scheme to implement a cryptosystem for image security. In this system, the encryption is done using Hill cipherwith self-invertible matrix as key. Hill cipher technique performs image encryption based on matrix multiplicationin both encryption and decryption processes. For decryption process, Hill cipher requires an inverse of key matrix. Since it is not possible to generate inverse matrix for all the cases, there is a possibility for occurrence of errors in the cryptosystem. In order overcome inverse of a matrix problem, this system uses a self-invertible matrix as key at both sender and receiver side.

AMS Subject Classification: 94A60
Keywords: Cryptography, Image, Key, Encryption, Decryption, Hill Cipher

1. Introduction

At present we are in the digital era in which internet plays a vital role in the field of communication. We are depending on internet for most of the needs like from shopping, banking, etc. While using the internet we are supposed to share our personal and confidential data in some of the applications. Those data can be easily hacked by the hackers if there is no proper mechanism is used for transmission of data. In order to overcome this issue we are using cryptography. Cryptography is a technique that uses encryption and decryption to maintain the confidentiality of the data transferred between the sender and the receiver. Encryption is the process of converting data from original format to another format. Decryption is the process of retrieving original format of data from some other format. The encryption process is applied on the sender side and decryption process is carried out on the receiver side. Since the data is transmitted in some other format by the sender it is very difficult for the hacker to get the original data. Hill cipher and Affine cipher are the two different techniques used in cryptography. In this work a new cryptosystem is developed by using both of the above mentioned techniques. To overcome the inverse matrix problem in Hill Cipher, this system uses a self-invertible key.

2. Hill Cipher

Hill cipher is one of the cryptographic technique based on matrix multiplication. The mathematical model for image encryption in Hill cipher technique is given as

$$E = O * K$$

Where,
E is Encrypted image block of size $n \times n$
O is Original imageblockofsize $n \times n$
K is Keyof size $n \times n$
The decryption process is given as

$$D = E * K^{-1}$$

Where,
E is Encrypted imageblock of size $n \times n$
D is Decrypted imageblock of size $n \times n$
K^{-1} is Inverse of keyof size $n \times n$

Self-Invertible Matrix
A self-invertible matrix is a matrix whose inverse is its original value and is given by

$$A = A^{-1}$$

Where A is Matrix of size $n \times n$

3. Proposed Scheme

Our proposed scheme consists of four modules such as self-invertible key, encryption using generated key, decryption using self-invertible key, and performance analysis.

3.1 Key Generation

In this system we generate key on both sender and receiver side. The generators g_1, g_2,g_3, $g_4$are shared between sender and receiver. Sender selects a private key a and the receiver selects another private key$b$. Then the key can be generated as following as per our algorithm.

3.1.1 Key Generation at Sender

The algorithm for key generation on sender side is as follows

1. Selects a private key a
2. Generated public keys W_s, X_s,Y_s and Z_s as given below and shares with the receiver

$$W_s = g_1^a$$
$$X_s = g_2^a$$
$$Y_s = g_3^a$$
$$Z_s = g_4^a$$

3. Compute the values of W, X, Y and Z as follows

$$W = {W_r}^a = (g_1^b)^a = g_1^{ab}$$
$$X = {X_r}^a = (g_2^b)^a = g_2^{ab}$$
$$Y = {Y_r}^a = (g_3^b)^a = g_3^{ab}$$
$$Z = {Z_r}^a = (g_4^b)^a = g_4^{ab}$$

4. Generates the key matrix K_{11} of size 2×2 as given below

$$K_{11} = \begin{bmatrix} W & X \\ Y & Z \end{bmatrix}$$

5. Generates self-invertible matrix K_S of size 4×4 as given below

$$K_S = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix}$$

Where,

$$K_{12} = I - K_{11}$$
$$K_{21} = I + K_{11}$$
$$K_{22} = -K_{11}$$

Where K_S is the key generated by sender.

3.1.2 Key Generation at Receiver

The algorithm for key generation on receiver side is as follows

1. Selects a private key b
2. Compute the values of W_r, X_r,Y_r and Z_r as given below

$$W_r = g_1^b$$

$$X_r = g_2^b$$
$$Y_r = g_3^b$$
$$Z_r = g_4^b$$

3. Compute the values of $W,\ X,\ Y$ and Z as follows

$$W = W_s{}^b = (g_1^a)^b = g_1^{ab}$$
$$X = X_s{}^b = (g_2^a)^b = g_2^{ab}$$
$$Y = Y_s{}^b = (g_3^a)^b = g_3^{ab}$$
$$Z = Z_s{}^b = (g_4^a)^b = g_4^{ab}$$

4. Generates the key matrix K_{11} of size 2×2 as given below

$$K_{11} = \begin{bmatrix} W & X \\ Y & Z \end{bmatrix}$$

5. Generates self-invertible matrix K_R of size 4×4 as given below

$$K_R = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix}$$

Where,

$$K_{12} = I - K_{11}$$
$$K_{21} = I + K_{11}$$
$$K_{22} = -K_{11}$$

Where K_R is the key generated by receiver.

Since the values of $W,\ X,\ Y$ and Z are same on sender and receiver side the key values K_S and K_R are equal i.e.,

$$K_S = K_R = K$$

Where K is the symmetric key used for both encryption and decryption processes.

3.2 Encryption Process

The encryption process is carried out using the key K on the sender side. First, the original image is divided into blocks of equal size of 4×4. Each block is encrypted using the following encryption model and finally all blocks are combined to produce the cipher image.

$$C = KM + NI$$

Where,
C is Cipher image block of size 4×4
K is Self-invertible key matrix of size 4×4
M is Original image block of size 4×4
N is Scalar multiplicative value
I is Identity matrix of size 4×4

3.3 Decryption Process

The decryption process is carried out using the key K on the receiver side. First, the ciphered image is divided into blocks of equal size of 4×4. Each block of cipher image is decrypted using the following decryption model and all blocks are combined to produce the decrypted image.

$$D = K^{-1}(C - NI)$$

Since K is a self-invertible matrix, the value of $K = K^{-1}$. So, the above equation can be written as

$$D = K(C - NI)$$

Where,
C is Ciphered image block of size 4×4
K is Self-invertible key matrix of size 4×4
D is Decrypted image block of size 4×4
N is Scalar multiplicative value

I is Identity matrix of size 4× 4

4. Performance Analysis

This system is implemented in MATLAB 2015b and the results were analyzed and compared with various schemes to demonstrate the efficiency of our scheme. Our results show that the proposed scheme is more efficient than other schemes.

Fig.1(a). Lena Image before Encryption

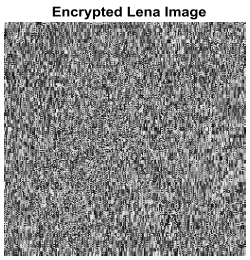

Fig.1(b). Lena Image after Encryption

Fig.1(c). Lena Image afterDecryption

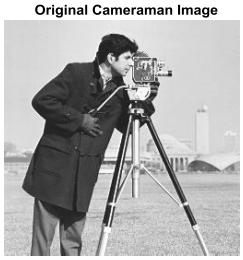

Fig.1(d). Cameraman Image before Encryption

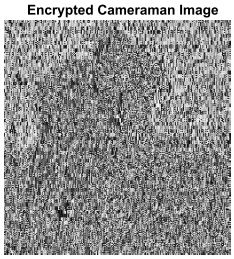

Fig.1(e). Cameraman Image after Encryption

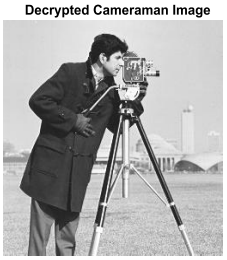

Fig.1(f). Cameraman Image after Decryption

4.1 Histogram Analysis

In image encryption environment, the histogram of an image generally states to a histogram of the pixel intensity values. This histogram is a graph display the quantity of pixels in an image at each dissimilar intensity value found in that image. For an 8-bit gray scale image there are 256 different possible intensities, and so the histogram will graphically display 256 numbers showing the distribution of pixels amongst those gray scale values. Thus, by relating the histograms of original and encrypted images, we can say that the encrypted images are uncertainty identical.

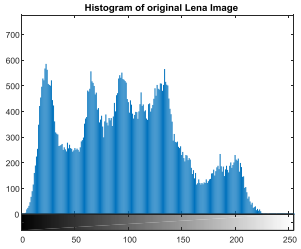

Fig.2(a). Histogram of Lena image before Encryption

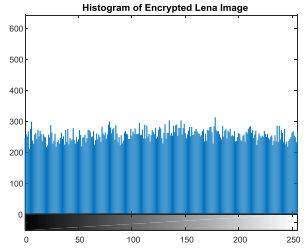

Fig.2(b). Histogram of Lena image after Encryption

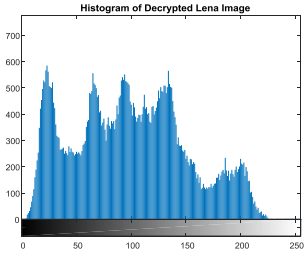

Fig.2(c). Histogram of Lena image afterDecryption

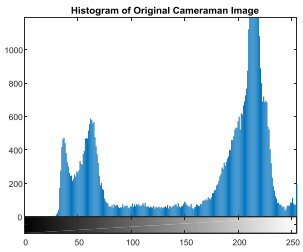

Fig.2(d). Histogram of Cameraman image before Encryption

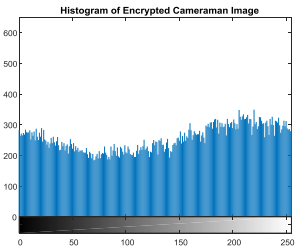

Fig.2(e). Histogram of Cameraman image after Encryption

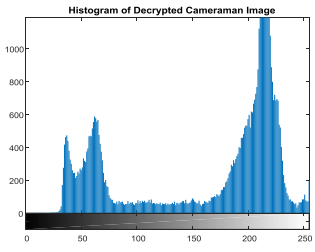

Fig.2(f). Histogram of Cameraman image after Decryption

4.2 Entropy Analysis

Information entropy is the quantity used for uncertainty of an image. It can serve a measure of disorder. In place of the level of disorder increases, the entropy growths and system become less predictable. The entropy is given as,

$$H(X) = \sum_{i=1}^{n} \Pr(x_i) log_2 \Pr(x_i)$$

$$\Pr(X = x_i) = {}^{1}/_{G}$$

Where, X represent the test image, x_i symbolize the i_{th} possible value in X.

Entropy of encrypted images using our algorithm and other references are shown in Table 1.

Image Name	Our approach	Ref.1	Ref.2	Ref.4	Ref.5	Expected Value
Lena	7.9963	7.9970	7.9973	7.9891	7.7626	8

Table.1: Entropy values for Lena image

Theoretical entropy value for a gray scale image is 8 and it is expected to be near to 8. Table.1 shows the entropy value calculated for our algorithm and the comparision with other schemes.

4.3 NPCR and UACI

The number of pixel change ratio and unified average changing intensity (UACI) are the most important parameters used to evaluate the strength of image cryptosystems. A high NPCR/UACI valuemeans, the cryptosystem has high resistance to differential attacks.

Theoretically, NPCR and UACI values are calculated using the following formulas.

$$NPCR = \sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times \frac{100\%}{M \times N} \begin{cases} 0 & if\ C_1(i,j) = C_2(i,j) \\ 1 & if\ C_1(i,j) \neq C_2(i,j) \end{cases}$$

$$UACI = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|\ C_1(i,j) - C_2(i,j)|}{255} \times \frac{100\%}{M \times N}$$

Where $C_1(i,j)$ is the original image pixel value at the position i,j

$C_2(i,j)$ is the cipher image pixel value at the position i,j

$M \times N$ is the image dimension

In the proposed scheme, we approach a new scheme by establishing a mathematical model for image encryptionand calculated NPCR and UACI values for this model with Lena image. Further, these values are used to analyze the strength of the cryptosystem. Experimental results for NPCR and UACI tests from Table.2 and Table.3 show that the proposed cryptosystem is efficient and more secure with

some other existing systems.

Image name	Our approach	Ref.4	Ref.6	Expected Value
Lena	99.06	99.59	88.99	High

Table.2: NPCR of proposed scheme and references

Image name	Our approach	Ref.1	Ref.4	Ref.6	Expected Value
Lena	29.71	30.38	33.42	30.21	High

Table.3: UACI of proposed scheme and references

4.4 Mean Square Error

Mean Square Error (MSE) is a parameter used to measure difference between original and encrypted image in which pixels are expressed between 0 and 255. To check the quality of encryption the original image and cipher image is usually compared. MSE for original and cipher image can be calculated as

$$\sum_{i=1}^{M}\sum_{j=1}^{N}[C(i,j) - C^{'}(i,j)]$$

Where,

$C(i,j)$ = pixel value of original image at the position i, j

$C^{'}(i,j)$= pixel value of cipher image at the position i, j

M, N = size of the original or encrypted image

Image name	Our approach	Ref.1	Ref.2	Ref.3	Expected Value
Cameraman	10465	9765	9765	9338.4	High

Table.4: MSE of proposed scheme and references

High value of MSE shows that the encrypted image has more variations of pixel values than original image. Table.4 shows the Mean Square Error value calculated for our algorithm and the comparision with other schemes.

4.5 PSNR

The PSNR is stands for Peak Signal to Noise Ratio. This ratio is frequently used as a quality and quantity among the original and an encrypted image. PSNR characterizes a quantity of the peak error. It is mathematically calculated as,

$$PSNR = 10 \times log_{10}\left[\frac{R^2}{MSE}\right]$$

Where,R is the maximum possible pixel value of image
MSE is the Mean Square Error value.

Image name	Our approach	Ref1	Ref2	Ref3	Expected Value
Lena	8.6973	8.5952	NA	NA	Low
Cameraman	7.9333	6.9999	8.2341	8.4281	

Table.5: PSNR of proposed scheme and reference

The higher value of MSE and lower value of PSNR means, the encryption algorithm is better for encryption and the randomness of encryption image pixel values are high. From Table.5 it is observed that the proposed system has less PSNR values and ecryption is better than other schemes.

4.6 Structural Similarity Index

The Structural Similarity (SSIM) index is a method for measuring the comparison between two images.

The SSIM index can be observed as a quality measure of one of the images being compared with other image which is observed to ensure the similarity of original and decrypted image.

$$SSIM\ (x,y) = \frac{(2\mu_x\mu_y + c_1)\,(2\mu_{xy} + c_2)}{(\mu_x^2+\mu_y^2 + c_1)(\sigma_x^2+\sigma_y^2 + c_2)}$$

Where, μ_x and μ_y are mean of x and y
σ_x and σ_y are covariance of x and y
c_1 and c_2 are constants

Image name	Our approach	Ref2	Ref3	Expected Value
Cameraman	1	0.9966	0.9899	1

Table.6: SSIM of proposed scheme and references

SSIM value is calculated by comparing the original image and decrypted image and it is expected to be 1. Our result from Table.6 shows that the image is decrypted using our proposed encryption algorithm without error.

5. Conclusion

In this proposed scheme, the encryption algorithm is implemented with modified hill cipher approach and two reference images Lena and Cameraman were tested using MATLAB2015b. Various performance parameters were calculated and analyzed with various schemes. Our entropy value 7.9963 for the cipher image shows that our proposed image encryption algorithm is efficient. The calculated SSIM value of 1 show that the original image and decrypted image are similar and there is no error while encryption and decryption process. Other performance parameters such as MSE, PSNR, NPCR, and UACI calculated for our proposed algorithm show that, our new proposed scheme is efficient and more secure for image encryption process.

References

[1] Ziad E.Dawahdeh, Shahrul N.Yaakob, Rozmie Razif bin Othman, A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher, Journal of King Saud University - Computer and Information Sciences, (2017). https://doi.org/10.1016/j.jksuci.2017.06.004.

[2] HossamDiab, Aly M. Elsemary, Secure Image Cryptosystem with Unique Key Streams viaHyper-chaotic System, Signal Processing, (2017). doi:10.1016/j.sigpro.2017.06.028.

[3] Congxu Zhu, A novel image encryption scheme based on improved hyper-chaotic sequences, Optics Communications 285 (1) (2012) 29—37. doi:10.1016/j.optcom.2011.08.079.

[4] Xiao, Chun-Jie Hu, Adaptive medical image encryption algorithm based on multiple chaoticMapping, Saudi Journal of Biological Sciences 24 (2017) 1821–1827.

[5] Deng, S.J., Huang, G.C., Chen, Z.J., 2011. Research and implement of Self adaptiveimage encryption algorithm based on chaos. J. Comput. Appl. 31 (6), 1502–1504.

[6] Zhang, J., Hou, D., Ren, H., 2016. Image Encryption Algorithm Based on DynamicDNA Coding and Chen's Hyperchaotic System, Mathematical Problems inEngineering, Article ID 6408741, 11pages.

[7] Zhongyun Hua, Fan Jin, Binxuan Xu, Hejiao Huang, 2D Logistic-Sine-Coupling Map for Image Encryption, Signal Processing (2018), doi: 10.1016/j.sigpro.2018.03.010.

[8] Hui Wang, Di Xiao, Xin Chen, Hongyu Huang, Cryptanalysis and Enhancements of Image Encryption Using Combination of the 1D Chaotic Map, Signal Processing (2017), doi: 10.1016/j.sigpro.2017.11.005.

[9] Rushi Lan, Jinwen He, Shouhua Wang, Tianlong Gu, Xiaonan Luo, Integrated Chaotic Systems for Image Encryption, Signal Processing (2018), doi: 10.1016/j.sigpro.2018.01.026.

[10] Sakshi Dhall , Saibal K. Pal , Kapil Sharma , Cryptanalysis of image encryption scheme based on a new 1D chaotic system, Signal Processing (2017), doi: 10.1016/j.sigpro.2017.12.021.

[11] Zhongyun Hua, Shuang Yi, Yicong Zhou, Medical image encryption using high-speed scrambling and pixel adaptive diffusion, Signal Processing (2017), doi: 10.1016/j.sigpro.2017.10.004.

[12] M. Li, Y. Guo, J. Huang, Y. Li, Cryptanalysis of a chaotic image encryption scheme based on permutation-diffusion structure, Signal Processing: Image Communication (2018), https://doi.org/10.1016/j.image.2018.01.002.