GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

IMAGE ENCRYPTION USING ADVANCE HILL CIPHER AND SPLIT ENCRYPTION

A Report for the Final Evaluation of Project 2

Submitted by

Akshat Kumar

(1613101091 /

16SCSE101123)

in partial fulfillment for the award of the degree

of

Bachelor of Technology

IN

Computer Science and Engineering

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

Under the Supervision of

Dr. S. ANNAMALAI, M.Tech., Ph.D.,
Assistant Professor,
Galgotias University

APRIL / MAY- 2020

SCHOOL OF COMPUTING AND SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that this project report **"IMAGE ENCRYPTION AND DECRYPTION USING ADVANCE HILL CIPHER"** is the bonafide work of **" AKSHAT KUMAR(1613101091)"** who carried out the project work under my supervision.

SIGNATURE OF HEAD

Dr. MUNISH SHABARWAL,
PhD (Management), PhD (CS)
Professor & Dean,

School of Computing Science & Engineering

SIGNATURE OF SUPERVISOR

Dr. SANJEEV KUMAR PIPAL, M.Tech., Ph.D.,
Professor

School of Computing Science & Engineering

Abstract

We present this project using the image encryption technique based on Hill Cipher that provides a better security approach based on the research paper of S.K Muttoo, Deepaika Aggarwal and Bhavya Ahuja. The image is encrypted by rendering the image content completely scrambled using multiple self-invertible keys, block shuffling and a new developed Pel-Transformation. The Hill cipher algorithm is one of the symmetric key algorithms having several advantages in encryption. However, the inverse of the matrix used for encrypting the plain text in this algorithm may not always exist. Moreover this algorithm is susceptible to known plain text attack. The algorithm used in this is aimed aimed at better encryption of all types of images even ones with uniform background and makes the image encryption scheme more secure.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
1.	Abstract	3
2.	Introduction	4
3.	Existing System	7
4.	Proposed system	9
5.	A) Pel Transformation	
6.	B) Shuffling Image Block	
7.	Result / Screenshot	13
8.	Conclusion	15
9.	References	16

List of Acronyms

ACSAuto Configuration

Server ADAnno Domini

ADSLAsymmetric

Digital Subscriber Line

ADSL2Asymmetric Digital Subscriber Line 2, referred also as ITU G.992.3/4

AJAXAsynchronous JavaScript

XML AMDAdvanced Micro

Devices BSDBerkeley Software

Distribution BTBritish Telecom

CETCentral European Time

CPECustomer Premises Equipment

CSRFCross-Site Request Forgery

CWMPCPE WAN Management Protocol

DDoSDistributed Denial of Service

DHCPDynamic Host Configuration Protocol

DNSDomain Name System

DNSDomain Name System DOMDocument

Object Model DoSDenial of Service

Chapter:1

INTRODUCTION

With the rapid advancement in network technology especially Internet, it has become possible to transmit any type of data across networks. This has raised concern for the security of the transmitted data as access to data which has become easier by interception of communication media. Hence, data security is becoming an imperative and critical issue in data storage and transmission to prevent it from attacks. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important.

Encryption refers to the algorithmic schemes that encode the original message referred to as plain text using a key into non-readable form, a coded message known as cipher text so that it is computationally infeasible to be interpreted by any eavesdropper. The receiver of the cipher text uses a key to retrieve back the message in original plain text form .

Substitution cipher is one of the basic components of classical ciphers. A substitution cipher is a method of encryption by which units of plain text are substituted with cipher text 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 plain text are retained in the same sequence as in the cipher text, but the units themselves are altered.

For substituting large group of letters, we use polygraphic substitution ciphers. We also have mono-alphabetic substitution ciphers that use a fixed substitution over the entire message. Hill cipher is one of such ciphers and we have used this for image encryption in the paper.

The Hill cipher has several advantages such as disguising letter frequencies of the plain

text, using simple matrix multiplication and inversion for enciphering or deciphering, high speed and high throughput. But some problems have been noticeable in the encryption scheme. Inverse of a matrix may not exist due to which decryption will not be possible. Due to its linear nature, it succumbs to known-plain text attack. On application of the encryption algorithm which images with uniform background, the images could not be encrypted properly as pixels with similar intensity values (as with uniform background) map against to similar intensity values. In order to address these issues and enhance secrecy of encrypted data using Hill cipher, we are proposing an algorithm which uses a different Self-Invertible Matrix Generation Method for Hill cipher system. This method can be used multiple times to generate a different self-invertible matrix for each block of the image. We have also applied a new pel transformation and block shuffling in the algorithm. Our algorithm works well for all types of gray scale as well as color images.

The organization of the paper is as follows. The present section i.e. Section 1 is the introductory. A brief review of Hill cipher is given in Section 2. The proposed method for encrypting and decrypting the images has been discussed in Section 3. Section 4 summarises the experimental results of proposed algorithm.

Hill Cipher :- The Hill cipher is a polygraphic block cipher based on linear algebra developed by Lester Hill in 1929. Using frequency analysis, substitution ciphers like mono-alphabetic ciphers can be easily broken. But Hill cipher completely hides single letter frequencies by encrypting pairs of plain text and so it's safe against cipher-text only attacks. It provides good diffusion as change in one letter of plain text affects all letters in the cipher text. All arithmetic is done modulo some integer z that is the total number of possible symbols.

For encryption, the algorithm takes m successive plain text letters and instead of that

substitutes m cipher letters. Each character is assigned a numerical value like a = 0, b = 1 and so on. The substitution of cipher text letters in the place of plain text letters leads to m linear equation. For m = 3, the system can be described as follows:

$$C_1 = (K_{11}P_1+K_{12}P_2+K_{13}P_3) \bmod 26$$

$$C_2 = (K_{21}P_1+K_{22}P_2+K_{23}P_3) \bmod 26$$

$$C_3 = (K_{31}P_1+K_{32}P_2+K_{33}P_3) \bmod 26$$

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

$$\begin{pmatrix} C1 \\ C2 \\ C3 \end{pmatrix} = \begin{bmatrix} K11 & K12 & K13 \\ K21 & K22 & K23 \\ K31 & K32 & K33 \end{bmatrix} \begin{pmatrix} P1 \\ P2 \\ P3 \end{pmatrix}$$

or simply C = KP , where C and P are column vectors of length 3, representing the plain text 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-1K = 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 plain text is recovered [4] [5]. In general term, we can write as follows:

For encryption: C = Ek (P) = KP **For decryption:** P= Dk (C) = K-1C = K-1 KP = P

If the block length is m, there are 26m different m letters blocks possible, each of them can be regarded as a letter in a 26m letter alphabet.

Chapter:2

Existing system by Bibhudendra Acharya

Bibhudendra Acharya along with his colleagues proposed an Algorithm using advance hill cipher but the main drawback of this algorithm was that it fails to encrypt the image having many large area covered with same colour or with a grey colour. This algorithm does provide more security against the brute force attack than the Hill Cipher Algorithm and also is resistant against known plaintext attacks.

The algorithm is given below and the block diagram for the encryption process is shown in Figure 1.

Image Encryption Algorithm :-

Step1. A involutory key matrix of dimensions mm×is constructed.

Step2. The plain image is divided into mm×symmetric blocks

Step3. The ith pixels of each block are brought together to form a temporary block.

a. Hill cipher technique is applied onto the temporary block. b.

b. The resultant matrix is transposed and Hill cipher is again applied to the this matrix.

Step4. The final matrix obtained is placed in the ith block of the encrypted image.

Evolutionary Key Matrix Algorithm :-

1. Select any arbitrary n/2 * n/2 matrix A22.
2. Obtain A11 = - A22
3. Take A12 = k(1 - A11) or k(1 + A11) where k is a scalar constant.
4. Then, A21 = (I + A11) / k or (I - A11) / k
5. Form the matrix completely.

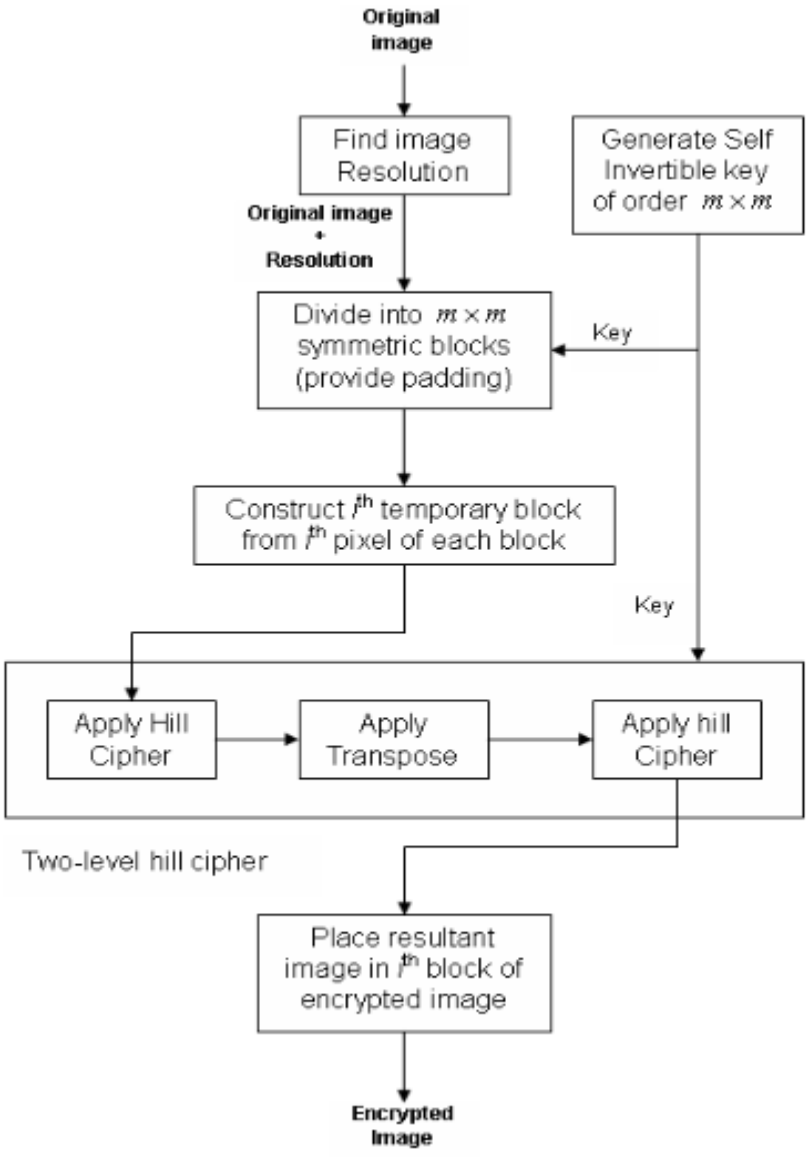

Original image
Find image Resolution
Generate Self Invertible key of order $m \times m$
Original image + Resolution
Divide into $m \times m$ symmetric blocks (provide padding)
Key
Construct i^{th} temporary block from i^{th} pixel of each block
Key
Apply Hill Cipher
Apply Transpose
Apply hill Cipher
Two-level hill cipher
Place resultant image in i^{th} block of encrypted image
Encrypted Image

Figure 1

Chapter:3

Proposed Secure Image Encryption Algorithm

In this section, we propose an encryption scheme based on Hill Cipher involving multiple key generation, pel transformation and block shuffling. The scheme intends to address some issues in the cipher scheme using a single self invertible key matrix for encryption .

The scheme proposed was susceptible to Known Plain Text attack in which the key can be found by attacker using some known plain text-cipher text pairs. Also the images with uniform background could not be encrypted properly. The images with very close pixel values or equal values map to similar values or to values that have very low perceptual difference giving very poor encryption results as is demonstrated in Figure 2.

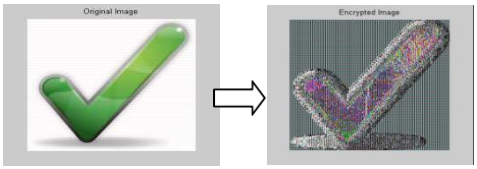


Figure 2

The pseudocode for the proposed encryption algorithm is given below:-

1)Input: The image to be

2)Encrypted Output : The Encrypted image

3) Begin

4)Divide the image into 8X8 blocks

5) Do for each block

6)Generate a 4X4 self -invertible key K for the block using the algorithm given in [3] Take four adjacent pixel values and if within epsilon threshold apply pel transformation Encrypt

the pixel values using the key K as C = K*values mod 256

7)Endo

8)Create a new image with these new pixel values and shuffle 8X8 blocks of the new image using a shuffling key

9)End.

The pseudocode for the proposed decryption algorithm is given below:-

1) Input: The image to be decrypted, block seed and t values, multiplier

2) Output: The Original image

3) Begin

4) Reshuffle the image blocks to their original locations using shuffling key pos

5) Divide the image into 8X8 blocks

6) Do for each block

7) Generate the 4X4 self-invertible key for the block using seed and the using of the key generation algorithm

8) Decrypt four pixel values at a time from the block Approximate the new pixel values if value of multiplier is not 1

9)Endo

10)Create the new decrypted image with these new pixel values

11)End

Pel-Transformation:-

If the pixel values are identical or very close, then after encryption they map to very close values or even to the same values as before encryption in case of equal intensity values. This is noticeable from the following example. Using constant k=1 in self-invertible key generation method:

Say key = $\begin{pmatrix} 12 & 120 & 245 & 136 \\ 176 & 224 & 80 & 30 \\ 13 & 120 & 224 & 136 \\ 176 & 225 & 80 & 32 \end{pmatrix}$

and Pixel Values = [20 20 20 20]. Then, NewPixelValuesT = Key *ValuesT mod 256 = [20 20 20 20].

This results in poor encryption results as old and new pixel values are same. So we propose that application of some pixel value transformations before encryption would result in better results. Let epsilon be the difference between values of adjacent pixels in a quadruple of pixel values to be encrypted. If all the differences between the four adjacent pixel values is less than epsilon, then pixel value transformation function T given below is applied.

$$\mathbf{vi' = T(vi) = \begin{cases} vi * zi\text{-}1 \bmod 256 & \text{if indicator} = 1 \\ vi & \text{otherwise} \end{cases} \quad for\ i=1,2,3,4}$$

$$\mathbf{indicator = \begin{cases} 1 & \text{if } abs(vi\text{-}vi\text{-}1) \leq epsilon \text{ for } i=2,3,4 \\ 0 & \text{otherwise} \end{cases}}$$

Here z is a random number except 0 and 1. z values for all blocks are also transmitted in an array multiplier. With this transformation the perceptual difference between the pixel values is increased and they are mapped to uncorrelated values in the domain [0,255]. Hence, after encryption they result in varied uncorrelated intensities.

Shuffling Image Blocks

A random permutation on the number of blocks is generated and the new block values are stored in array pos which serve as the shuffling key. The blocks then shuffled according to these new block positions. These results, in more secrecy as the blocks, are randomly

distributed throughout the image. Figure 3 demonstrates the block diagram for the proposed encryption algorithm.

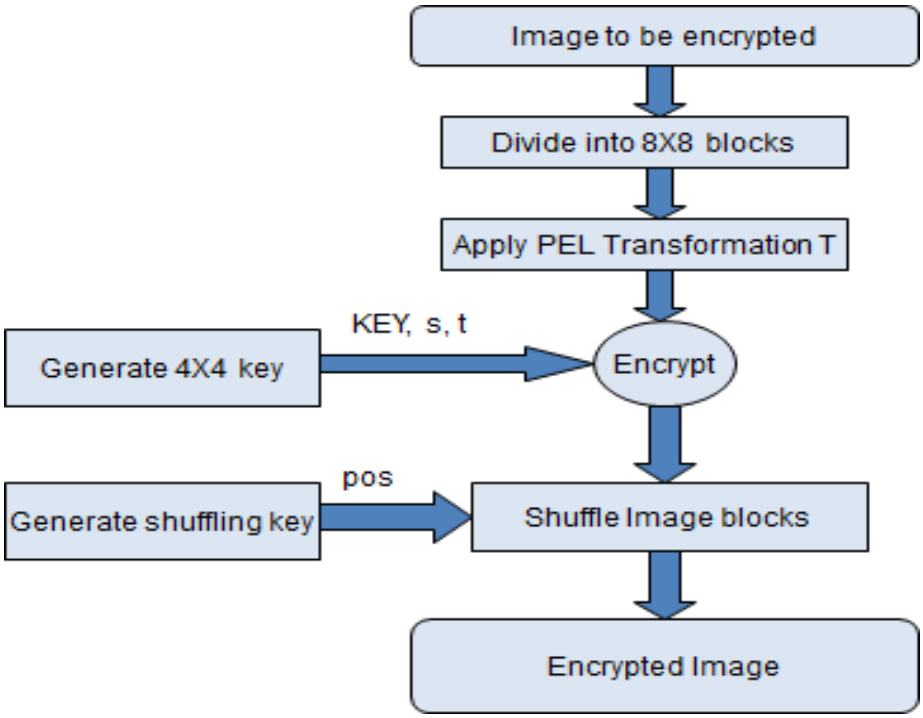


Figure 3

The sender transmits the encrypted image through the communication channel to the receiver. The block seeds and t values used for key generation, pos and multiplier are transmitted through a secure channel.

For RGB images the three color components are separately encrypted and the three components form the new RGB value

Chapter:4

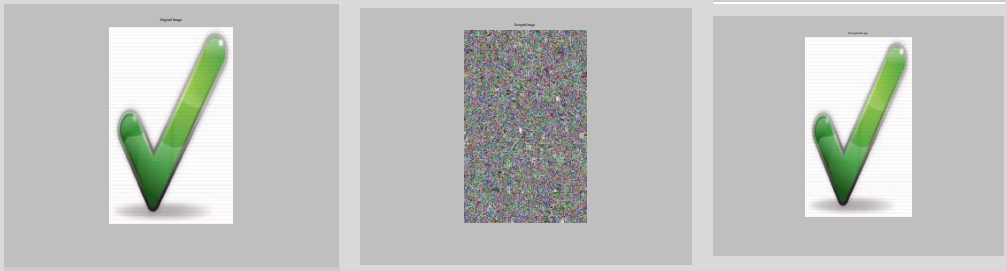
Experimental Results

This section represents the simulation results illustrating the performance of the proposed encryption algorithm.The encryption and decryption results using the proposed algorithm are given in Figure

(i)
rice.jpg

(ii)
cameraman.ti f

(iii)
check.jpg



(iv)
lenna.gif

(v)
cap.gif

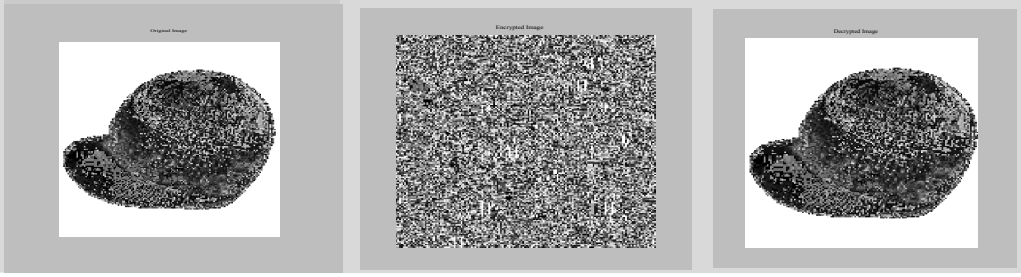
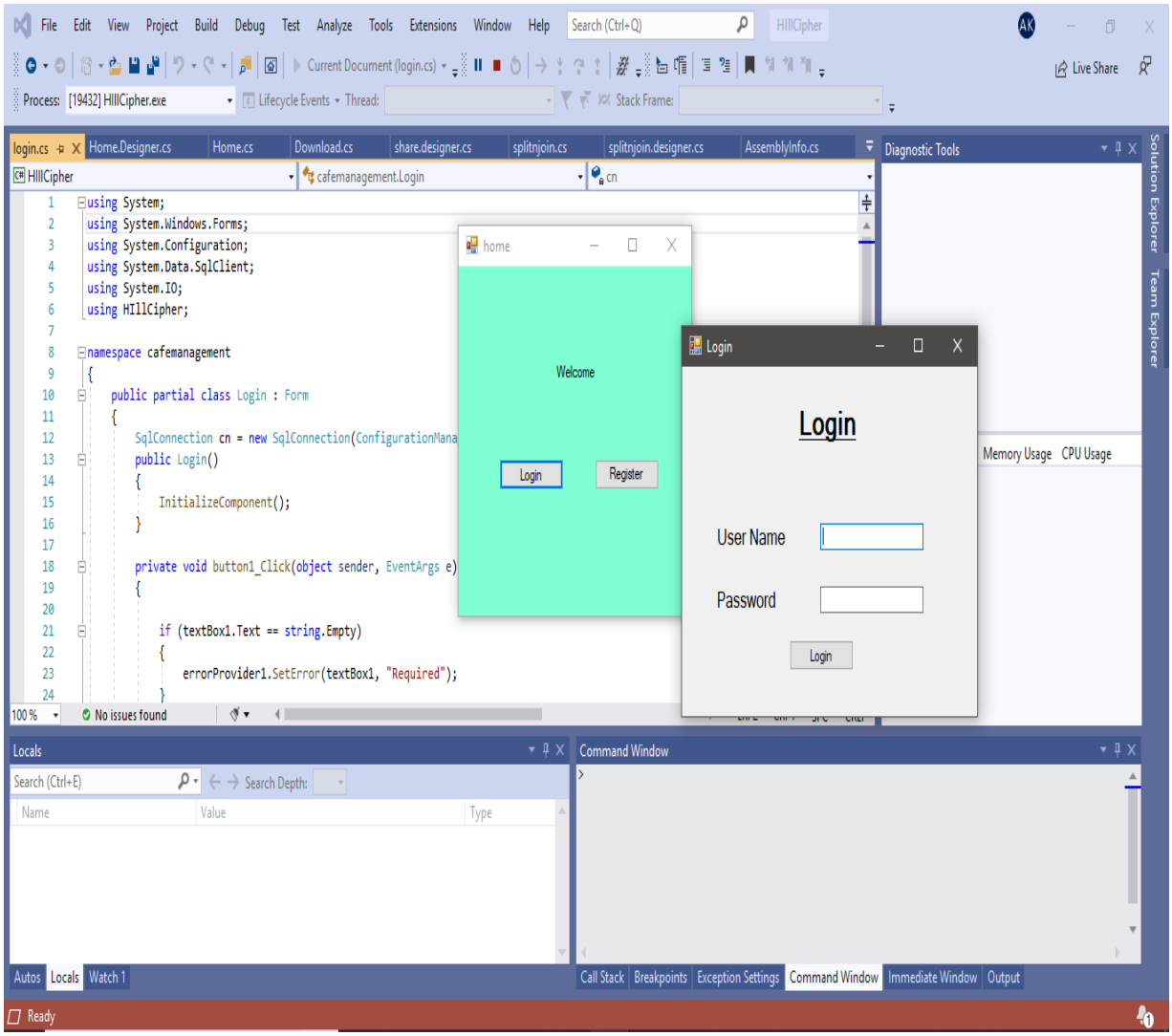


Figure 4. Encryption and decryption results using proposed algorithm: Original Image, Encrypted Image, Decrypted Image respectively.



Conclusion

In this project, a crypto-algorithm based on hill cipher is presented. The proposed cryptosystem uses a different key for each block encryption and the possibility of known plain text attack is highly reduced as the key used changes with every block and it is generated randomly using a seed and multiplier. Also in some cases, the encrypted pixel values are not the original intensity values but obtained from pel transformations. With block shuffling, the algorithm becomes more secure. For an image with uniform background, the results are improved due to changing keys, block shuffling and applying new developed pel transformation. The perceptual difference between close pixel values increases on applying pel transformation.

There may be cases in which the decrypted results are not completely similar to the original image. This is because the decrypted values are not exactly equal to the original values, in case the four values are within epsilon threshold, so in some regions like edges, degradations from the original image are noticeable. Hence, there is a trade-off between better encryption and better decryption results.

References

[1] Bibhudendra Acharya, Saroj Kumar Panigrahy and Debasish Jena. Image encryption using self invertible key matrix of Hill cipher algorithm. Ist International Conference on Advances in Computing. Chikhli, India. 21-22 February 2008.

[2] Bibhudendra Acharya, S K Patra, G. Panda. A Novel cryptosystem using matrix self invertible key matrix of Hill cipher algorithm. Ist International Conference on Advances in Computing, Chikhli, India. 21-22 February 2008.

[3] Lester S Hill. Cryptography in an algebraic alphabet. Amer. Math. 1929; 36: 306-312.

[4] William Stallings. Cryptography and Network Security. Fourth Edition. Prentice Hall. 2005.

[5] A Secure Image Encryption Algorithm Based on Hill Cipher System S.K.Muttoo, Deepika Aggarwal, Bhavya Ahuja Department of Computer Science, University of Delhi, India