

Encryption Approach for Images using Bits Rotation Reversal and Extended Hill Cipher Techniques

Naveen Kumar S K
Department of Electronics
University of Mysore
Karnataka, India

Sharath Kumar H S
Department of Electronics
University of Mysore
Karnataka, India

Panduranga H T
Department of Electronics
University of Mysore
Karnataka, India

ABSTRACT

A new method for image encryption with two stages has been described in the present study. In first stage, each pixel of image is converted to its equivalent eight bit binary number and in that eight bit number, number of bits equal to the length of password are rotated and then reversed. In second stage, extended hill cipher technique is applied by using involutory matrix generated by same password given in second stage to make encryption more secured. Performance of the proposed technique is evaluated by *Statistical Analysis*, *Differential Analysis* and also quantifying *Mean Square Error* (MSE) & *Peak Signal to Noise Ratio* (PSNR). The proposed approach is implemented for different images using MATLAB. Decryption involves the reverse process of encryption.

Keywords

Image Encryption, Bits Rotation, Bits Reverse, Extended Hill Cipher.

1. INTRODUCTION

With the fast development in communication and information technology, huge data is transmitted over a communication channel which needs security. There are many applications like information storage, information management, patient information security, satellite image security, confidential video conferencing, telemedicine, military information security and many other applications which require information security.

Komal D Patel and Sonal Belani [1] have presented a survey on existing work which is used different techniques for image encryption and also given a general introduction about cryptography. There are several methods for image encryption with some advantages and disadvantages. Ismet Ozturk and Ibrahim Sogukpinaar [2] have discussed the analysis and comparison of image encryption algorithms. And they classify the image encryption methods in to three major types: position permutation, value transformation and visual transformation. Mitra et al [3] have presented a new approach for image encryption using combination of different permutation techniques. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the bits, pixels and blocks using certain permutation techniques. Panduranga H T and Naveenkumar S K [4] have proposed an approach using bit reversal method. Bibhudendra Acharya et al [5] have proposed several methods of generating self-invertible matrix which can be used in Hill Cipher algorithm. Saroj Kumar Panigrahy et al [6] have implemented image encryption using Self-Invertible key matrix of Hill Cipher algorithm. Bibhudendra Acharya et al [7] have proposed a novel Advanced Hill Cipher encryption

technique which uses Involutory key matrix. H.S. Kwok, Wallace K.S. Tang [8] have proposed a fast chaos-based image encryption system with stream cipher structure. Yue Wu et al [9] have proposed a mathematical model for ideally encrypted images and then derived expectations and variances of NPCR and UACI under that model.

The organization of the paper is as follows. Following the introduction, image encryption technique by using *bits rotation and reversal* method based on password is explained in Section 2. Section 3 explains the Extended Hill Cipher technique for Image Encryption. In section 4, proposed image encryption method is explained. Finally, results and discussions are explained in Section 5. This paper is concluded by providing the summary of the present work in section 6.

2. BITS ROTATION AND REVERAL TECHNIQUE FOR IMAGE ENCRYPTION

In this method, a password is given along with input image. Value of each pixel of input image is converted into equivalent eight bit binary number. Now length of password is considered for bit rotation and reversal. i.e., Number of bits to be rotated to left and reversed will be decided by the length of password. Let L be the length of the password and L_R be the number of bits to be rotated to left and reversed (i.e. L_R is the effective length of password). The relation between L and L_R is represented by equation (1).

$$L_R = L \bmod 7 \text{ ----- eq. (1)}$$

where ‘7’ is the number of iterations required to reverse entire input byte.

For example, $P_{in}(i, j)$ is the value of a pixel of an input image. $[B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8]$ is equivalent eight bit binary representation of $P_{in}(i, j)$.

$$\text{i.e. } P_{in}(i, j) \xrightarrow{\text{decimal to 8 bit binary}} [B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8]$$

If $L_R=5$, five bits of input byte are rotated left to generate resultant byte as $[B_6 B_7 B_8 B_1 B_2 B_3 B_4 B_5]$. After rotation, rotated five bits i.e. $B_1 B_2 B_3 B_4 B_5$, get reversed as $B_5 B_4 B_3 B_2 B_1$ and hence the resultant byte has been generated as $[B_6 B_7 B_8 B_5 B_4 B_3 B_2 B_1]$. This resultant byte is converted to equivalent decimal number $P_{out}(i, j)$.

$$[B_6 B_7 B_8 B_5 B_4 B_3 B_2 B_1] \xrightarrow{\text{8 bit binary to decimal}} P_{out}(i, j)$$

where $P_{out}(i, j)$ is the value of output pixel of resultant image.

Since the weight of each pixel is responsible for its colour, the change occurred in the weight of each pixel of input image

due to *Bits Rotation & Reversal* generates the encrypted image. Figure 1 (a, b) show input and encrypted images respectively. For this encryption process given password is “sharu” whose effective length (L_R) = 5.

Note: - If $L=7$, then $L_R=0$. In this condition, the whole byte of pixel gets reversed.

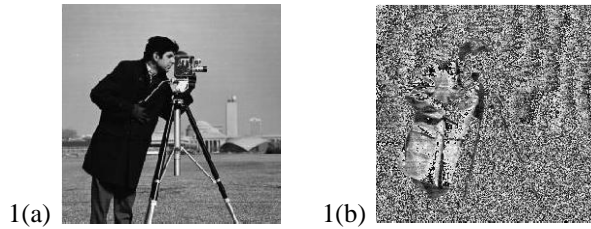


Fig 1: (a).Input Image. (b).Encrypted Image for password “sharu”.

3. EXTENDED HILL CIPHER TECHNIQUE

This is a new method for encryption of images proposed in this paper. The basic idea of this method is derived from the work presented by Saroj Kumar Panigrahy et al [6]. In this work, involutory matrix is generated by using the algorithm presented by Bibhudendra Acharya et al [7].

Algorithm of Extended Hill Cipher technique:


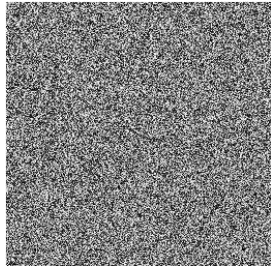

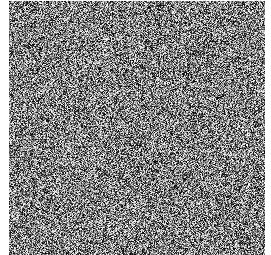
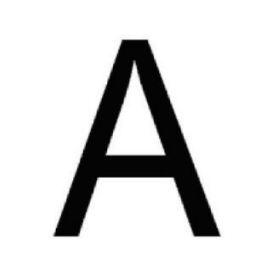
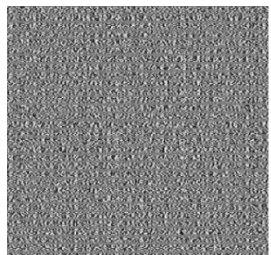

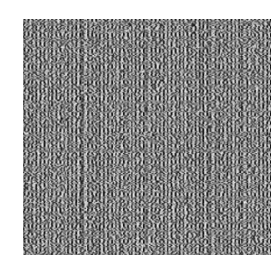
Step 1: An involutory matrix of dimensions $m \times m$ is constructed by using the input password.

Step 2: Index value of each row of input image is converted into x -bit binary number, where x is number of bits present in binary equivalent of index value of last row of input image. The resultant x -bit binary number is rearranged in reverse order. This reversed- x -bit binary number is converted into its equivalent decimal number. Therefore weight of index value of each row changes and hence position of all rows of input image changes. i.e., Positions of all the rows of input image are rearranged in *Bits-Reversed-Order*. Similarly, positions of all columns of input image are also rearranged in *Bits-Reversed-Order*.

Step 3: Hill Cipher technique is applied onto the *Positional Manipulated* image generated from Step 2 to obtain final encrypted image.

TABLE 1 shows various input and encrypted image respectively, where the encryption process is carried out by using *Extended Hill Cipher* technique. The password given to generate involutory matrix is “sharu”.

TABLE 1

Input Image	Encrypted Image
	
	
	
	

4. PROPOSED TECHNIQUE

This image encryption method consists of two stages, among which first stage is *Bits Rotation Reversal* stage and second stage is *Extended Hill Cipher* stage. For both stages, only one alphanumeric password is needed.

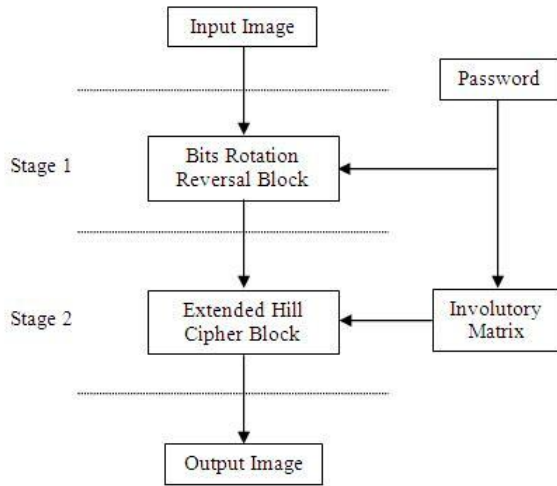



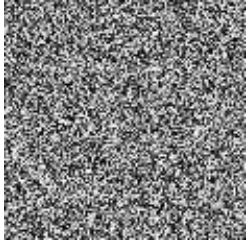
Fig 2: Block Diagram representation of proposed image encryption technique.

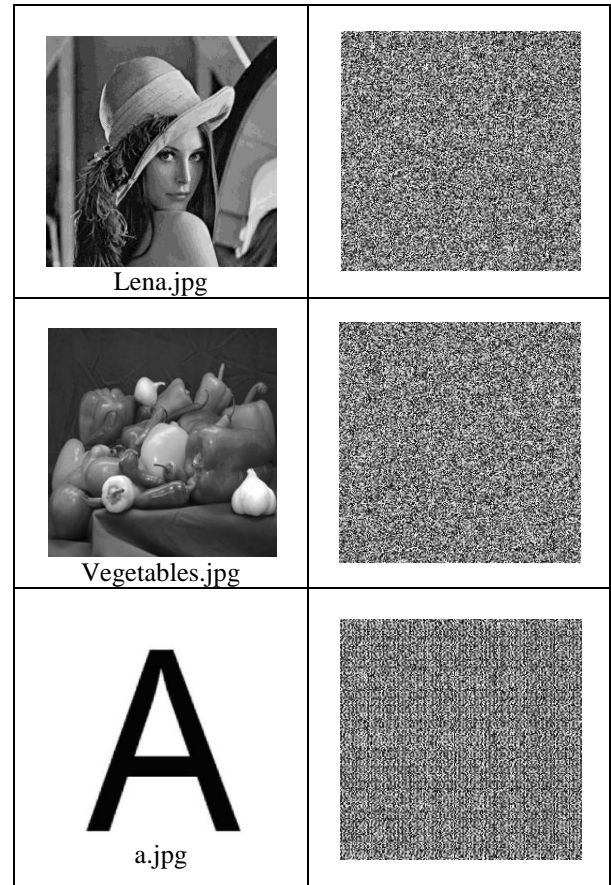
In first stage, input image of first stage is given along with an *alphanumeric password*. The encryption process is carried out as explained in Section 2. But the encrypted image generated in second stage can be decrypted by other passwords of same length as original password. To avoid this inconvenience second stage of encryption has designed. In second stage, an *Involutory Matrix* is generated by using the *alphanumeric password* given in first stage. By using password generated *Involutory Matrix*, *Extended-Hill-Cipher* technique is applied on encrypted image generated from first stage to obtain more secured final encrypted image. To generate an *Involutory Matrix*, minimum length of alphanumeric password should be four. Figure 2 shows block diagram representation of Proposed Image Encryption Technique.

5. RESULTS AND DISSCUSSIONS

Here, the above mentioned technique is implemented for different images and the alphanumeric word “sharath1234@#” is used as input password. Results of the proposed encryption technique for different images have been tabulated in TABLE 2.

TABLE 2

Input Image	Output Image
 Cameraman.bmp	



And also, in this section, some security analysis results on the proposed approach are described, including the most important ones like statistical analysis, and differential analysis.

5.1 Statistical Analysis

In order to resist the statistical attacks, the encrypted images should possess certain random properties. A detail study has been conducted and the results are summarized as followings. Different images have been tested, and similar results are obtained.

5.1.1 Histogram of Encrypted Images:

In order to appear random, the histograms of the encrypted image should be uniform distributed in all gray levels. **Figure 3&4** show the histograms of original and the encrypted images. It can be observed that a flat histogram is resulted from the encrypted image using our scheme.

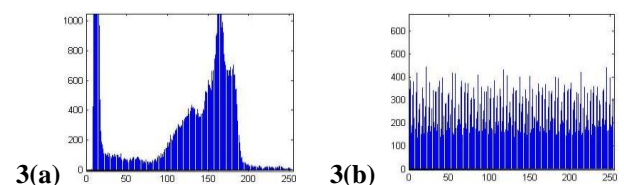


Fig 3: Histograms of the image ‘cameraman.bmp’. (a). Histogram of Original Image. (b). Histogram of Encrypted Image.

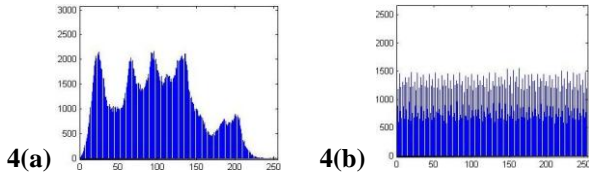


Fig 4. Histograms of the image 'lena.jpg'. (a). Histogram of Original Image. (b). Histogram of Encrypted Image.

5.1.2 Correlation of Adjacent Pixels:

The correlation between two vertically adjacent pixels, two horizontally adjacent pixels in a cipher image can be computed by using the formula.

$$cov(x,y) = E(x - E(x))(y - E(y)) \quad \text{-----eq. (2)}$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{var(x)}\sqrt{var(y)}} \quad \text{-----eq. (3)}$$

where x and y are gray levels of two adjacent pixels in the image. **Fig 5** shows the correlations of two adjacent pixels in the original image and in the encrypted image. The correlation coefficient of 'lena.jpg' image is computed in both horizontal and vertical directions and tabulated in **TABLE 3**. In **Fig 5**, correlation of adjacent pixels is represented graphically for the image 'lena.jpg'.

TABLE 3

	Original Image	Encrypted Image
Horizontal	0.9838	0.0139
Vertical	0.9706	0.0127

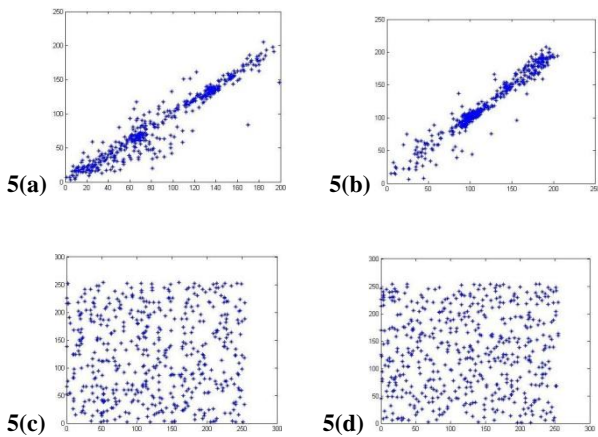


Fig 5: (a). Horizontal Correlation of adjacent Pixels of Original Image. (b). Vertical Correlation of adjacent Pixels of Original Image. (c). Horizontal Correlation of adjacent Pixels of Encrypted Image. (d). Vertical Correlation of adjacent Pixels of Encrypted Image.

5.2 Differential Analysis

The major requirement of all the encryption techniques is the encrypted image should be greatly different from its original form. Two measures are adopted to quantify this requirement. They are *Number of Pixel Change Rate* (NPCR) and *Unified Average Changing Intensity* (UACI). The NPCR is used to

measure the number of pixels in difference of gray level in two images. Let $C(i, j)$ and $C'(i, j)$ be the i th row and j th column pixel of two images C and C' , respectively, the NPCR can be defined as

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N} \times 100 \quad \text{-----eq. (4)}$$

where N is the total number of pixels in the image and $D(i, j)$ is defined as

$$D(i,j) = \begin{cases} 0 & C(i,j) = C'(i,j) \\ 1 & C(i,j) \neq C'(i,j) \end{cases}$$

Another quantity, *Unified Average Changing Intensity* (UACI) measures the average intensity of differences between the two images. It can be defined as

$$UACI = \frac{1}{N} \left[\sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255} \right] \times 100 \quad \text{-----eq. (5)}$$

Two quantities, NACP and UACI are calculates for various images using eq. (4) and eq. (5) respectively. The results are tabulated in the **TABLE 4**.

TABLE 4

Name of Input Image	NPCR	UACI
Cameraman	99.6246	35.6
Lena	99.6113	49.8
vegetables	99.6002	17.4
A	97.5937	97.1

Along with Statistical Analysis & Differential Analysis, *Mean Square Error* (MSE) & *Peak Signal to Noise Ratio* (PSNR) for the proposed technique has been computed for different images. It is known that, as the MSE increases, PSNR decreases, resulting more randomness in the encrypted image. MSE is calculated using the formula

$$MSE = \frac{1}{MN} \sum_{i=1}^N \sum_{j=1}^M [C(i,j) - C'(i,j)]^2 \quad \text{-----eq. (6)}$$

where, $C(i, j)$ and $C'(i, j)$ be the i th row and j th column pixel of two images C and C' , respectively. M and N are number of rows and columns of original image.

PSNR can be computed by

$$PSNR = 10 \times \log_{10} \left[\frac{R^2}{MSE} \right] \quad \text{-----eq. (7)}$$

where R is 255 as 8-bit image has been used in this experiment. Calculated results of MSE and PSNR are tabulated in **TABLE 5**.

TABLE 5

Name of Input Image	MSE	PSNR
Cameraman	108.0922	8.4221
Lena	88.4971	8.6092
vegetables	70.8896	8.3005
A	187.1933	5.1043

6. CONCLUSION

In this paper, an approach for image encryption which has two stages has been presented. For both stages, only one alphanumeric password is needed. From the experimental result it can be concluded that the original image can be predicted if only *Bits Rotation Reversal* technique is adopted, but it is difficult predict the original image, if *Extended Hill Cipher* technique is used. The original image can also be predicted if there is a uniform background in an image in case of *Bits Rotation Reversal* technique. If the combinational approach of *Bits Rotation Reversal* and *Extended Hill Cipher* technique is used, it is very difficult to decode the image. The performance of the proposed approach is evaluated based on the Statistical Analysis, Differential Analysis, MSE and PSNR. It has been concluded that the encrypted images using combinational approach is more scrambled as compare to individual technique.

7. ACKNOWLEDGMENTS

The work described in this paper is supported by a grant from the *University Grants Commission*, New Delhi, India.

8. REFERENCES

[1]. Komal D Patel, Sonal Belani. 2011. Image encryption using different techniques: A review. International

Journal of Emerging Technology and Advanced Engineering.

- [2]. Ismet Ozturk and Ibrahim Sogukpinaar. 2004. Analysis and Comparison of Image Encryption Algorithms. Transaction on engineering, Computer and Technology, 2004, vol.3, pp.38-42.
- [3]. A. Mitra, Y. V. Subba Rao and S. R. M. 2006. Prasanna. A New Image Encryption Approach using Combinational Permutation Techniques. IJCS.
- [4]. Panduranga H T, Naveenkumar S K. 2010. An image encryption approach using bit-reversal method. NCIMP.
- [5]. Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigrahy. 2007. Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm. International Journal of Security.
- [6]. Saroj Kumar Panigrahy, Bibhudendra Acharya, Debasish Jena. 2008. Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm. 1st International Conference on Advances in Computing, Chikhli, India.
- [7]. Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda. 2009. Image Encryption Using Advanced Hill Cipher Algorithm. International Journal of Recent Trends in Engineering
- [8]. H.S. Kwok, Wallace K.S. Tang. 2007. A fast image encryption system based on chaotic maps with finite precision representation. Chaos, Solitons and Fractals.
- [9]. Yue Wu, Joseph P. Noonan, and Sos Agaian, 2011. NPCR and UACI Randomness Tests for Image Encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT).