

A Combined Method for Image Encryption

Chinmoy Ghosh*, SatyendraNath Mandal**

*(Dept. of Computer Sc. and Engg., Jalpaiguri Govt. Engg. College, Jalpaiguri, West Bengal
Email: chinmoyslg@gmail.com)

** (Dept. of Information Technology, Kalyani Govt. Engg. College, Kalyani, Nadia, West Bengal
Email: satyen_kgec@rediffmail.com)

ABSTRACT

Many image encryption techniques have been developed to protect confidential image information in communication through the public channel. In this paper, a combined method of image encryption has been proposed to encrypt the image. The algorithm is divided into two parts. At first, the bits of pixels are reversed and rotated based on length of key. In second part, the encrypted image has been constructed after bit-wise XOR operation between the revised pixels and key. The proposed technique has been tested on different types of images. Finally, the performance of the algorithm has been verified by some statistical analysis.

Keywords-Bits reverse, Bits Rotation, Combined Method, Image Encryption, Statistical Analysis.

I. INTRODUCTION

During last few decades Information security is the imperative and important issue as compared to the growing internet application. To secure the information and to protect it from unauthorized access cryptography plays a vital role. Using cryptography by applying some methods or techniques plain text information is encrypted to make it cipher text which is not understandable by the intruder. Out of this information Image plays vital role in digital communication and due to this robust Image encryption methods or algorithm is very much necessary.

A technique of data hiding with cryptography by using a block of 3x3 pixels is presented [1]. They first changed the value of the pixels nearer to the ASCII value of available character range (65-90 and 97-122) and then in this 3x3 pixel value one character is inserted based on the key. In [2], authors developed a method of Image encryption by dividing the Image in N nos. of vector of length K bits, where K is the length of the KEY in bit and taken KEY as an input vector. Then diffusion operation is done by Boolean X-OR operation with first vector with the key and replace the vector with this new value. For the next vector the same operation is done with their previous vector and thus changing the value of each vector. Lastly confusion operation is done by rotating right each vector number of times equal to the number of 0's bit in it. Another recently used technique is to use receiver MAC address for Image encryption [3]. Here after reading the data the data is split into N/6 no of

vector where N is the no of data. Next X-OR Boolean operation between the MAC address vector and each of the data vector is performed and lastly Re-sequence or reorder the sequence of the vectors is done for final encryption. Many authors has made a comparative study [4] [5] [6] [7] [8] [9] on different methods of Image encryption and analyzed them in order to make familiar with the various encryption algorithms used in encrypting the image which has been transferred over network. The results of the their simulation show that every algorithm has advantages and disadvantages based on their techniques which are applied on images.

In TJ-ACA [10] methods at first pixels intensity is changed and then IKEDA MAPPING is applied for further encryption. In [11], authors used two steps to encrypt image. In the first step pixel rearrangement within image is done using sorting method and next image is encrypted using inter-pixel displacement algorithm. In SD-EI [12] [13] combined image encryption technique and basically has two stages: Image encryption technique by using bits rotation and reversal.

In this paper, image has been encrypted based on a combined method. The algorithm has two stages. At first, the bits of pixels are reversed and rotated based on length of key. The encrypted image has been constructed after bit-wise XOR operation between the revised pixels and key in second step. Finally, the performance of the algorithm has been verified by some statistical analysis.

II. PROPOSED ALGORITHM

Input: Key and Image
 Output: Encrypted Image

Method: Part 1

1. To read the Image in matrix form.
2. To read the KEY and find the Length L.
3. To Perform $L_E = L \bmod 7$. If $L_E = 0$ then $L_E = 7$
4. To Take P_i pixel and represent it by equivalent eight bit binary number.
 P_i is the i th no of pixel. Initially $i=1$.
5. To Perform BIT REVERSAL and ROTATION TECHNIQUE on P_i and convert the byte to decimal form.
6. Set $L=L+1$ and $i=i+1$.
7. Go to step 3 and repeat the steps upto the last pixel of the Image.
8. Output Encrypted Image (O), which is the input to the next part.

Part 2

1. To find the Effective key (E_k) and length of it.
2. To do Bit-wise XOR operation with O_i and E_{k_j}
 Where $i=1$ to total no. of pixel
 And $j=1$ to length of Effective key.
3. Repeat the above step upto the last pixel of the Image.
4. Result is Encrypted Image.

III. ILLUSTRATION WITH EXAMPLE

At first each pixel of input Image its equivalent eight bit binary number. Length of password which is given at the time of input image is considered for bit reversal and rotation. To do this Effective length of the password (L_E) is required and is represented by $L_E = L \bmod 7$ where L is the actual length of the password and '7' is the number of iterations required to reverse entire input byte. Say, [B8 B7 B6 B5 B4 B3 B2 B1] is equivalent to eight bit binary representation of X_{ij} , which is the value of a pixel of an input image. Now If $L_E=6$, six bits of input byte are reversed from left to generate resultant byte as [B3 B4 B5 B6 B7 B8 B2 B1]. After reversed, the whole byte rotated left by six positions and hence we get the resultant byte as [B2 B1 B3 B4 B5 B6 B7 B8]. This resultant byte is converted to equivalent decimal number Y_{ij} , where Y_{ij} is the value of output pixel of resultant image. Next value of L is incremented by one such that each

consecutive pixel gets different values of L so that No of Bit to be Rotate and shift can change time to time. Since, the pixel value represents its color, the change occurred in the value of pixel of input image due to Bits Reversal & Rotation generates the encrypted image.

Fig 1 and Fig 2 shows the input and Encrypted Image of Stage 1. Here password is "ghv123#"



Fig 1: Input Image



Fig 2: Encrypted Image after part 1

After this stage of encryption technique Logical XOR operation is performed between the each pixel value and the each character of the Effective Key i.e. if the Key is "Bell007" the Effective Key is "Bel07" and 1st pixel value will be X-ORed with the eight bit binary value of 'B' and next pixel with 'e' and so on. From 6th pixel same process repeat until the last pixel of the input image which is the output of previous stage is shown in Fig 3.



Fig 3: Final Encrypted Image

IV. EXPERIMENTAL RESULT

The algorithm has been applied on different types of Images and different testing has done to check the performance of the algorithm is furnished in Table 1.

Table 1: Key, Image and their Encrypted Images

V. TESTING

5.1. KEY SENSITIVITY ANALYSIS

The images are successfully decrypted by applying reversed operations with same key and they have been not decrypted with different keys. The decryptions of Lena image with proper key and wrong key are shown in Fig 4 and Fig 5. The algorithm is very much sensitive with key. The change of key has given the completely different image.



Fig 4: After Decryption with key “Kolkata98()”

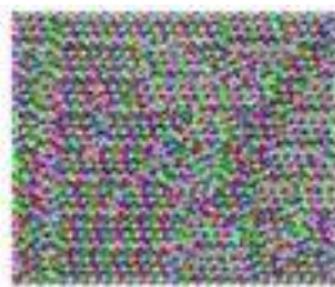


Fig 5: After Decryption with wrong key “kolkata”

5.2. ENTROPY ANALYSIS

Entropy of an Image is represented by the formula

$$H(m) = \sum p(m_i) \log_2 \frac{1}{p(m_i)}$$

$p(m_i)$ = Probability of pixel value m_i

Image entropy is used to describe the amount of information which must be coded for by a compression algorithm. An image, whose entropy is zero is perfectly flat and can be compressed to a relatively small size. Low entropy images, have very

little contrast whereas an image of high entropy has a great deal of contrast from one pixel to the next and cannot be compressed as much as low entropy images. Now output of the above equation will be 8 because a true random system should generate 2^8 symbols with equal probability. The entropy of the Original Image and the Encrypted Image has been given in the following Table 2 and it has been

KEY	ORIGINAL IMAGE	ENCRYPTED IMAGE
chin45!		
Kolkata98() 8()		
Chinmoy@12		
Chinmoy@12		

observe that the proposed algorithm is sustainable against entropy attack.

Table 2: Image and their Entropy values

Image Name	Original Image Entropy	Encrypted Image Entropy
Tusi	7.6402	7.9695
Lina	7.6116	7.9061
Eye	7.1974	7.9725
Linux	7.3269	7.9663

5.3.HISTOGRAM ANALYSIS

Histogram of an Image describes the statistical characteristics of that image. For an attacker it is very difficult to extract from the statistical nature of pixels of the plain image out of the encrypted image if the histogram of the encrypted Image are similar to random Image. The histogram analysis reference to Table 1 has been shown in the Fig 6.

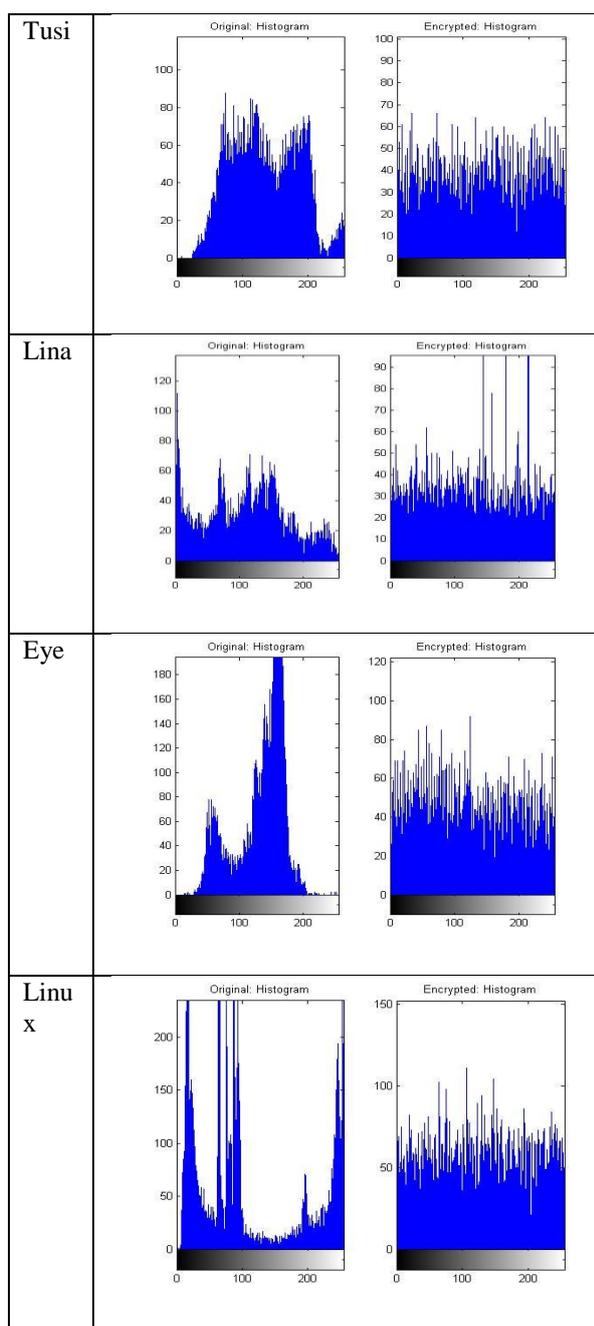


Fig 6: Histogram of Original and Encrypted Images

V. CONCLUSION

In this paper, a combined image encryption algorithm has been proposed and it has been tested on different images. The algorithm has successfully decrypted the encrypted images with proper key and it has not decrypted the encrypted images with wrong key. The entropy values of almost all encrypted images is nearly 8, it indicates that the pixels values are distributed among almost 255 different values. In histogram analysis, it has been observed that if there is even distribution of all image pixels then it is quite hard to recover the input image from encrypted image.

REFERENCES

Journal Papers:

- [1] Abhishek Gupta, Sandeep Mahapatra and Karanveer Singh, "Data Hiding in Color Image Using Cryptography with Help of ASK Algorithm" *IEEE, ETNCC 2011*, 15-17.
- [2] Mohammed Abbas Fadhil Al-Husainy, "A Novel Encryption Method for Image Security", *International Journal of Security and Its Applications*, 6(1), 2012, 1-8.
- [3] Mohammed Abbas Fadhil Al-Husainy, "MAC Address as a Key for Data Encryption", *(IJCSIS) International Journal of Computer Science and Information Security*, 30(30), 2013, 1-5.
- [4] Rajinder Kaur¹, Kanwalprit Singh,"Image Encryption Techniques: A Selected Review", *IOSR Journal of Computer Engineering (IOSR-JCE)*, 9(6), 2013, 80-83.
- [5] Bharti Ahuja, RashmiLodhi, "Different Algorithms used in Image Encryption: A review", *International Journal of Computer Science & Engineering Technology (IJCSSET)*, 4(7), 2013, 861-864.
- [6] Niraj Kumar, Prof. Sanjay Agrawal," A Technical Review on Symmetric Key Cryptography Algorithm on Images", *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(8), 2013, 1005-1009.
- [7] Komal D Patel, SonalBelani, "Image Encryption Using Different Techniques: A Review", *International Journal of Emerging Technology and Advanced Engineering*, 1(1), 2011, 30-34.
- [8] Sunil Singh Rathode , ChallaSrikar Reddy , Sai Praveen Reddy, "A Review Of Different Techniques Used In Image Encryption", *International Journal of Engineering*

Research & Technology (IJERT),2(9), 2013, 2315-2318 .

- [9] Swati Paliwal and Ravindra Gupta, “A Review of Some Popular Encryption Techniques”, *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(2), 2013, 147-149.
- [10] Taranjit Kaur, Reecha Sharma, “TJ-ACA: An Advanced Cryptographic Algorithm for Color Images using Ikeda Mapping”, *International Journal of Computer Trends and Technology, (IJCTT) - 4 (5), 2013, 1295-1300.*
- [11] AmneshGoel, Nidhi Chandra, “A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement”, *I.J. Image, Graphics and Signal Processing*, 2012, 16-22.
- [12] SomdipDey, SD-EI “A Cryptographic Technique to Encrypt Images”, *IEEE 2012, International Conference on Cyber security (CyberSec)*, 1(3), 2012, 28-32.
- [13] SomdipDey, “Amalgamation of Cyclic Bit Operation in SD-EI Image Encryption Method: An Advanced Version of SD-EI Method: SD-EI Ver-2”, *International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3)*, 2012, 221-225.

Books:

- [14] Behrouz A. Forouzan, D. Mukhopadhyay, “Cryptography & Network Security”, *Tata McGraw Hill Pvt. Ltd, 2013*
- [15] Rafael C. Gonzalez, R.E.Woods, S.L. Eddins, “Digital Image Processing Using MATLAB”, *Tata McGraw Hill Pvt. Ltd, 2010*
- [16] Atul Kahate, “Cryptography and Network Security”, *Tata McGraw Hill Pvt. Ltd, 2008.*