A New Image Encryption Technique Combining the Idea of One Time Pad with RGB Value

Jannatul Ferdush
Department of CSE
Jessore University of Science and Technology
Jessore-7408, Bangladesh

Mahbuba Begum
Department of CSE
Mawlana Bhashani Science and Technology University,
Tangail-1902, Bangladesh

Ashiq Mahmood
Department of CSE
Khulna University of Engineering and Technology
Khulna-9203, Bangladesh

ABSTRACT
Because of improvement of technology, at present data security is drawn attention to all. Image is an important medium of communication. An image can say thousands of words. So, improvement of image security is more important than security of text. Image is nothing but combination of some pixel values. On the other side, every pixel can be converted into binary value. In this paper, a new image encryption method is proposed based on displacement of RGB value with one time pad. Any 3D image can be encrypted using this method. The result shows that the proposed algorithm has large key space. So it can resist brute force attack as well as other attacks.

General Terms
RGB value, OTP, Cryptosystem etc

Keywords
RGB, DES, AES, Encryption, Image RGB Color Components

1. INTRODUCTION
In the field of communication, encryption is a way to transfer information in such a way that nobody can understand it without authorized user. Many new methods and approaches are forthcoming for encrypting images by considering images as block or stream. These methods encrypted the images either block by block or stream by stream. The traditional cryptographic algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES) etc. work with block data. But, they are not suitable to encrypt image/video because of their speed and large computational cost. Moreover, image encryption and text encryption are different. Because in image, there is a relation between pixels of image. But, in the case of text there is no such types of restriction.

In recent years, there has been proposed a lot of algorithms regarding image encryption using different ways. At first various chaos based image encryption techniques have been proposed [1][2][3]. But, the main problem of chaotic based system is that it is very sensitive to initial condition. Moreover, it has small key space. The result follows low security with low speed [4].

Various methods have been proposed on image RGB value. Images can be encrypted using the Transposition and Shuffling of RGB value. Quist-Aphetsi Kester proposed a method likely: Image Encryption based on the RGB PIXEL transposition and shuffling [5] which makes it possible for encryption and decryption of the images based on the RGB pixel. But, this research is not focused on employment of public key cryptography. Sourabh Singh proposed a novel approach which transforms a text file into an image by combining RGB substitution with AES [6]. But, the main problem of this method is that it converts the text into PNG format only. Shrija Somaraj and Mohammed Ali Hussain proposed "A Novel Image Encryption Technique using RGB pixel displacement for Color Images" in which the original plain image is splitted into its basic three components, that is the RGB components and the key image is also splitted into RGB Components. Further by application of XOR operation and scrambling of the three components the cipher image is generated. Their method is suitable for encrypting color images or 3D images [7]. Nashwan A. Al-Romema presents an image encryption scheme based on chaotic systems which encrypts the pixels RGB component instead of the pixels itself [8]. The simulation result shows that the proposed encryption scheme ensures high level of security, and requires less computational time of image data. Quist-Aphetsi Kester presents a method which encrypts and decrypts images based on the RGB pixel [9]. This conference paper is really effective interms of security analysis. Quist-Aphetsi Kester also proposed a method based on RGB pixel shuffling [10]. In this case, the author developed a new cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values. The simulation result shows that the proposed method increases the security of the image against all available attacks. But, this method is not focused on employment of public key cryptography.

A hybrid method combining with RGB based on DNA encoding and chaos map has large key space and also resist various attack like as exhaustive attack, statistical attack and other [11].

Due to above limitations, in this paper, a new image encryption technique has been proposed depending on image RGB value with One Time Pad. Here One Time Pad (OTP) is also used to enhance security.

2. THE ORIGINAL BACKGROUND
Nowadays information security is a major concerning issue. Due to the advancement of different technologies, a large part of confidential or private data can be exchanged over various types of networks. Different techniques have been used to provide this required protection. Encryption is one of the techniques for securing and protecting data in network, cloud or some data center. In cryptography, encryption is the process of converting an original message into its encrypted form using an algorithm which uses a key. Images are transferred everyday across the network. Some of these images are confidential. The security of images from unauthorized access is important. Therefore, we try to transfer these images securely. Image encryption acts a significant role in information hiding by preparing information unreadable so

that no hacker or eavesdropper has access to original message through public networks. Thus, image encryption can be used for protecting images from different kinds of attacks. It creates the ability to get the pixel values of the original image and transfers that image faster to the person. In Gaussian elimination with partial pivoting and row exchange algorithm of image encryption, each image is actually a matrix made up of RGB and alpha values. This algorithm makes the system robust so that the encrypted image is hard to hack to obtain the original image. But it is inefficient as it takes larger decryption time than encryption. One Time Pad (OTP) plays an important role in transferring images securely. This cryptosystem uses a truly random sequence of 0's and 1's of the same length as the message and the encryption is done by XOR operation. This requires perfectly random one time pads. The characteristics of this encryption method makes it attractive for communication with limited computing devices [12]. But, this cryptosystem belongs to key distribution problem along with the key problem of same length as plaintext. That is, the key of One Time Pad should never be reused. On the other hand, RGB color image is a three dimensional matrix in which the first two dimensional matrix is the red component, the second is the green component and the third is the blue component. Image encryption can be done using RSA and RGB randomized histograms in which image file is first selected from the database and then perform the splitting of the images. After this, apply the RSA algorithm on the split files [13].

3. SYSTEM MODEL

Figure 1 describes the proposed model. There are total four parties. Such as: sender, receiver and two key generators.

The algorithm of encryption and decryption is private and only known by sender and receiver. At first, sender wants to share an image with receiver. So, it requests for both key generator with image size. After receiving request, key generator-1 generates a false image and at the same time, sends it to both sender and receiver. On the other hand, key generator-2 generates two random matrices equal of image size (ignores the third dimension of image). It also sends it to both sender and receiver. After receiving image and matrix from both generators, sender encrypts original image using these private algorithm.

After encryption, image is sent over network to receiver. On the other hand, receiver receives the image and decrypts it with decryption algorithm.

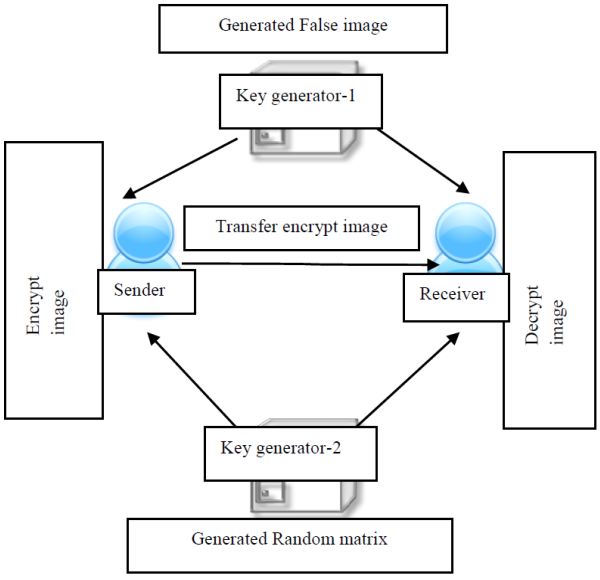


Fig 1: Proposed System Model

3.1 Sender Algorithm

Step 1: Start

Step 2: Read a RGB image.

Step 3: Performed bitwise XOR operation between RGB and false image. False image is generated by key generator-1.The bitwise XOR operation is also called One Time Pad (OTP).

Step 5: The R, G and B value of resultant image are swapped in such a way that:

Green Image=Blue Image
Blue Image=Red Image
Red Image = Green Image

Step 6: For every pixel value in red image performs the following operations:

$$R'(i,j) = [r(i,j) * rand_1(i,j)] \bmod 255$$
$$R''(i,j) = [R'(i,j) + rand_2(i,j)] \bmod 255$$

$rand_1(i,j)$ and $rand_2(i,j)$ means random value at postion (i,j).
Repeat this process for green and blue image and find G'(i,j) and B'(i,j).

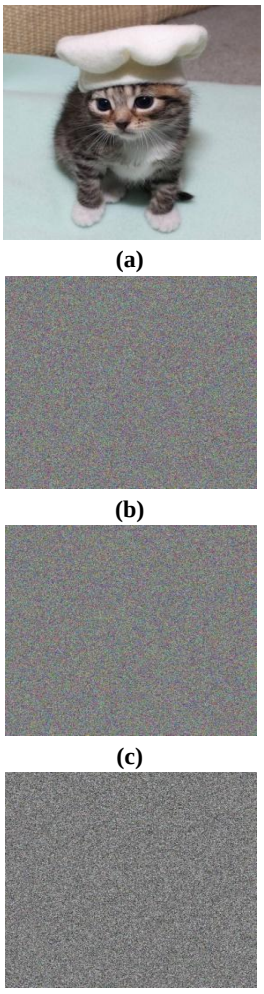
Step 7: Finally from the resultant red, green and blue image, we get our encrypted image.

Decryption process is just inverse of encryption process.

4. EXPERIMENTAL RESULT

In this section experimental result has been shown by an example.

Fig 2. Shows the output of each step of proposed model. Fig 2(d) is the final encrypted form of original image that is fig 2(a).



(a)

(b)

(c)

(d)

Fig 2: (a) Original Image [14](b) Image after XORing with False Image(c) Image after Swapping (d) Final Encrypted Image

5. EXPERIMENTAL ANALYSIS

5.1 Key Space Analysis

At first, random images of the same size are generated and their dimension will be the same as input image. If input image size is [mxnx3] then the false image is also [mxnx3]. So, there is total mxnx3 in numbers. Another random matrix size of [mxn] and other matrix from this random matrix is also generated. So, the key space is high. So, the encryption algorithm will be resistance to brute force attack.

5.2 Entropy Analysis

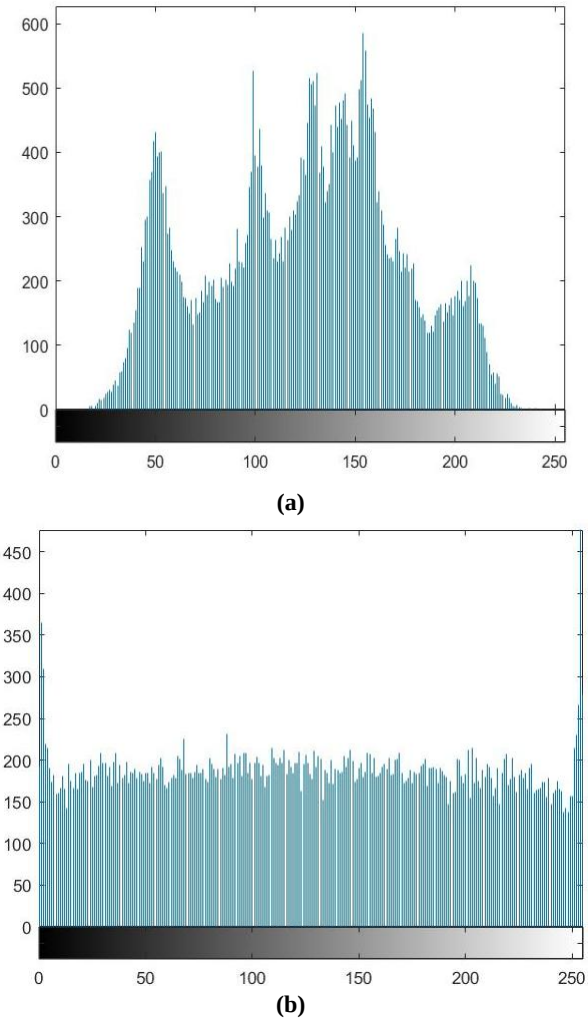
For same use, we run our application several times. For example from Table 1: we experiment on three images. Our average entropy is closer to 8. So, our image is random.

Table 1: Entropy of Encrypted Image

Image no	Entropy
cat.jpg	7.9709
dog.jpg	7.9707
flower.jpg	7.9708

5.3 Histogram Analysis

The histogram analysis result of original and encrypted image:



(a)

(b)

Fig 3: (a) Histogram of Original Image (b) Histogram of Encrypted Image

6. CONCLUSION AND FUTURE WORK

Nowadays, image can be used as an important medium of communication. This paper shows a mechanism in which an image is shared with an insecured communication channel. But, this mechanism is limited to larger calculation. In future, this research will extend to overcome this limitation and maximize the performance.

7. REFERENCES

[1] ErdemYavuz**,** RifatYazıcı**,** Mustafa CemKasapbaşı**,** EzgiYamaç , "A chaos-based image encryption algorithm with simple logical functions", Computers & Electrical Engineering Volume 54, August 2016, Pages 471-483.

[2] Junqin Zhao, Weichuang Guo, Ruisong Ye "A Chaos-based Image Encryption Scheme Using Permutation-Substitution Architecture", International Journal of Computer Trends and Technology (IJCTT) – volume 15 number 4 – Sep 2014.

[3] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps", Phys. Lett. A, 366(2007), 391–396.

[4] K. Sakthidasan@Sankaran and B. V. Santhosh Krishna "New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011

[5] Quist-Aphetsi Kester ,"Image Encryption based on the RGB PIXEL Transposition and Shuffling", I. J. Computer Network and Information Security, 2013, 7, 43-50, Published Online June2013 in MECS (http://www.mecs-press.org/).

[6] Sourabh Singh and Anurag Jain, "Combination of RGB Substitution for Text to Image Encryption Technique using AES", Spvryan's International Journal of Engineering Sciences & Technology (SEST) ISSN : 2394-0905.

[7] Shrija Somaraj and Mohammed Ali Hussain, "A Novel Image Encryption Technique using RGB pixel displacement for Color Images", 2016 IEEE 6th International Conference on Advanced Computing.

[8] Nashwan A. Al-Romema1, Abdulfatah S. Mashat2, Ibrahim AlBidewi, "New Chaos-Based Image Encryption Scheme for RGB Components of Color Image", Computer Science and Engineering 2012, 2(5): 77-85.

[9] Quist-Aphetsi Kester and Koumadi, Koudjo M, "Cryptographic Technique for Image Encryption based on the RGB pixel Displacement", 2012 IEEE 4th International Conference on Adaptive Science & Technology (ICAST).

[10] Quist-Aphetsi Kester,"A cryptographic Image Encryption technique based on the RGB PIXEL shuffling", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 2, January 2013.

[11] Quist-Aphetsi Kester,"A cryptographic Image Encryption technique based on the RGB PIXEL shuffling", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 2, January 2013.

[12] Sharad Patil and Ajay Kumar, "Effective Secure Encryption Scheme [One Time Pad] Using Complement Approach".

[13] Gajendra Singh Chandel and Pragna Patel, "Image Encryption with RSA and RGB randomized Histograms", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering.

[14] http://dy.163.com/wemedia/article/detail/C3LES2B70525A5LN.html" Image source, accessed date:11 November,2017