An Efficient Image Cryptosystem Using Pascal Triangle

Anitha Kumari[1], K Sugapriya[2]
{kak.it@psgtech.ac.in, suhapreyha@gmail.com[2]}

Associate Professor, Dept., of IT, PSG College of Technology, Coimbatore, Tamilnadu, India[1],PG Scholar, Dept., of IT, PSG College of Technology, Coimbatore, Tamilnadu, India [2]

Abstract. With the onset of Information Age, media are produced and consumed on computers leading to a paperless society. Profound number of security challenges are found when the data/images are sent over the transmission channel. Manifold ways are proposed to safeguard all these information from unauthorized access. In this paper, a novel method using Pascal triangle is used for encryption with bit-wise XOR operation for secure transmission of multimedia components. Image encryption and decryption is highly applied in the critical infrastructure including military, healthcare, cyber forensics and investigations etc., The image encryption algorithm evaluation has been performed by using parameters such as histogram, correlation, entropy and compression test. To ensure applicability to real-time applications resistant against various attacks are tested.

Keywords: Pascal triangle; Correlation; Entropy.

1 Introduction

With vast development in the field of communication technology, all information like data/image/video/audio are transmitted electronically. Whenever the data is in transit there arises a lot of security problems. Hence secure transmission of digital information has become an integral part of communication technology. There exist numerous methods to protect the multimedia data being transmitted which are categorized based on position permutation, visual and value transformation. This research work put forth an innovative method for secure transmission of multimedia components using encryption schemes. Encryption is a process which uses a set of instruction to convert the original data into unreadable encrypted form preventing unauthorized usage and to view the original data when decryption process is performed based on the generated key pair. Hence an innovative encryption approach is proposed based on Pascal triangle by performing a simple XOR operation by encrypting colour images. Encryption technique is applied to the image by extracting the red, blue and green channels of the image and encrypting them individually.

2.Related Work

EmaldaRoslin et al. [8] suggested a symmetric image encryption technique based on transposition. Based on this method, an image is splitted into sub images, followed by interchanging the pixels by applying appropriate permutation and merging them back again for transmission. Reverse process is performed on receiver side. Yashpalsingh Rajput and A K. Gulve [2] presented an image encryption technique which utilizes the enhanced adaption of hill cipher method for grouping and block-based conversion which makes the correlation to be low among the image pixels resulting in a strong cryptographic technique. Cooper et al. [5]

ICCAP 2021, December 07-08, Chennai, India

DOI 10.4108/eai.7-12-2021.2314617

proposed an efficient public key cryptosystem using the Pascal triangle that results in high dense set of numbers improving the security. T. Sivakumar and R. Venkatesan [4] presented a novel image encryption technique. XingyuanWangn et al [3] proposed a novel colour image encryption using a chaotic technique that uses combined permutation and diffusion of RGB for encryption. This paper also states that classical cryptographic techniques are not applicable for image encryption as RGB correlation is not considered in these techniques and thus it paves way for devising an innovative efficient scheme to work with image encryption.

Thus, image encryption based on chaotic technique, transposition, permutation, and scan pattern are utilized by researchers' community in recent times. In this paper, Pascal triangle method is used as an encryption methodology to apply visual and value transformation to the pixel positions of the image.

3. Proposed Methodology

3.1 Pascal triangle

Pascal triangle is formed by a triangular array of binomial coefficients. Each number in a row is the sum of the two numbers above it in the previous row which is illustrated in the Figure 1.

In this paper, Pascal triangle is applied to the image pixels as shown in the Figure 2. Here encryption is performed by performing bitwise XOR operation incorporating Pascal triangle. In the shown Fig. 2., the pixel value of b1 is encrypted as follows.

$b1 = a1 \oplus b2$ (1)

$b1 = b1 \oplus c2$ (2)

From (1) and (2),

$b1 = a1 \oplus b2 \oplus c2$ (3)

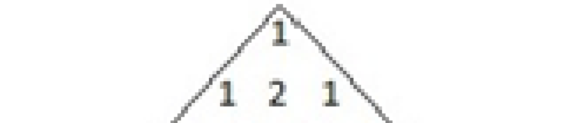


Fig 1. Image model based on Pascal triangle of French mathematician Blaise Pascal.

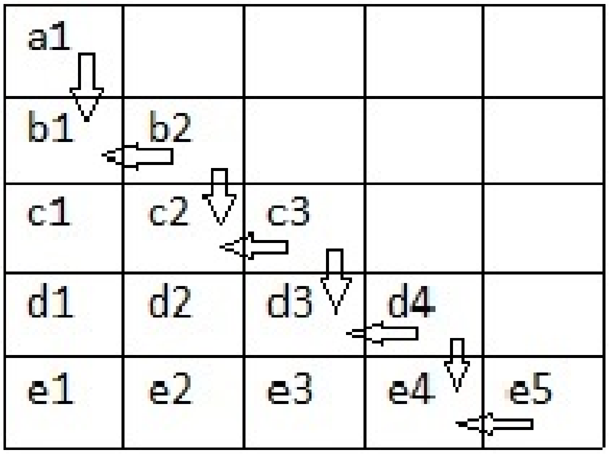


Fig. 2 Applying Pascal triangle to the image

3.2 Encryption Process

The block diagram of encryption is shown in Figure 3.

Input: Plain image of size m x m

Output: Cipher image of size m x m

Step 1: Let the original image to be encrypted is [m, m].

Step 2: Divide the image into their respective Red, Green and Blue channels and apply the following steps individually to each channel.

Step 3: Choose a diagonal for encryption from the image which serves as one of the keys.

Step 4: Apply Pascal triangle method to the image.

Step 5: Execute bitwise XOR operation to all the pixels in the selected image.

Step 6: Choose an angle and perform rotation to the image.

Step 7: Check whether the pixels are equally distributed. If so, keep the encrypted channel of the image and continue else repeat from step 2.

Step 8: Once RGB channels are encrypted, concatenate them to form the encrypted image [m, m].

3.3 Decryption Process

The block diagram of decryption is shown in Figure 4.

Input: Cipher image of size m x m

Output: Plain image of size m x m

Step 1: Let the image to be decrypted is [m, m].

Step 2: Divide the image into their respective Red, Green and Blue channels and apply the following steps individually to each channel.

Step 3: Choose the desired angle and perform rotation.

Step 4: Execute bitwise XOR operation to all the pixels in the selected image.

Step 5: Apply Pascal triangle method to the image.

Step 6: Decrypted R, G and B channels will be obtained.

Step 7: Concatenate the decrypted RGB channels to get the original image [m, m].

4. Results And Discussions

The proposed algorithm is tried and tested for color pictures of size 512x512. The work is tested with image type .TIFF and execution platform as Matlab R2014a. The obtained results of the proposed algorithm are shown in Figure 5 and 6. It is inferred that the resulting images are absolutely dissimilar from the selected input image. Histogram, dispersion, diffusion, confusion and compression are considered as the performance metrics to prove the efficiency of the proposed method when compared to existing methods.

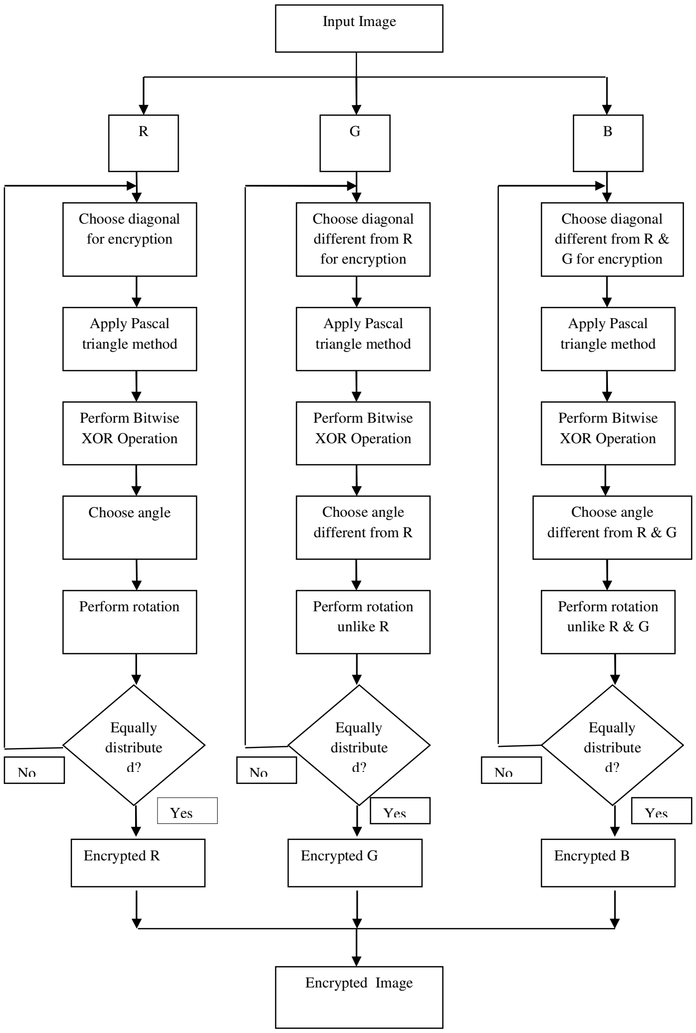

Input Image
R
G
B
Choose diagonal for encryption
Choose diagonal different from R for encryption
Choose diagonal different from R & G for encryption
Apply Pascal triangle method
Apply Pascal triangle method
Apply Pascal triangle method
Perform Bitwise XOR Operation
Perform Bitwise XOR Operation
Perform Bitwise XOR Operation
Choose angle
Choose angle different from R
Choose angle different from R & G
Perform rotation
Perform rotation unlike R
Perform rotation unlike R & G
Equally distribute d?
Equally distribute d?
Equally distribute d?
No
No
No
Yes
Yes
Yes
Encrypted R
Encrypted G
Encrypted B
Encrypted Image

Fig.3 Block diagram of encryption using Pascal triangle

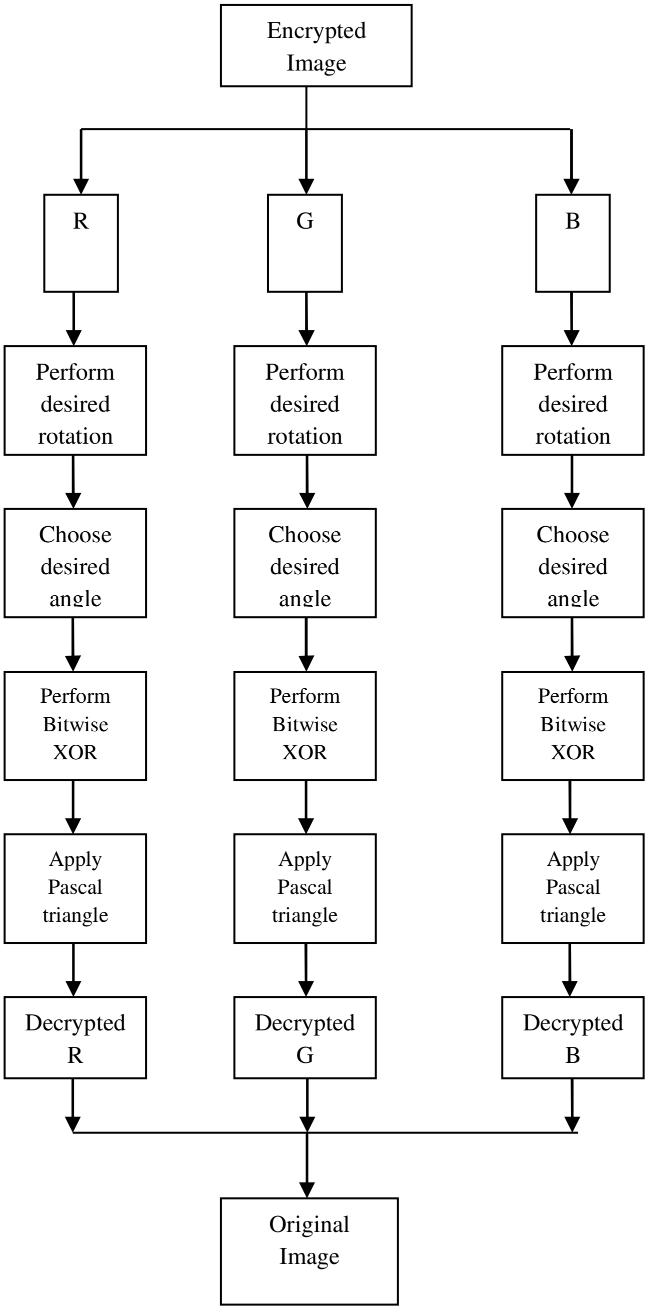
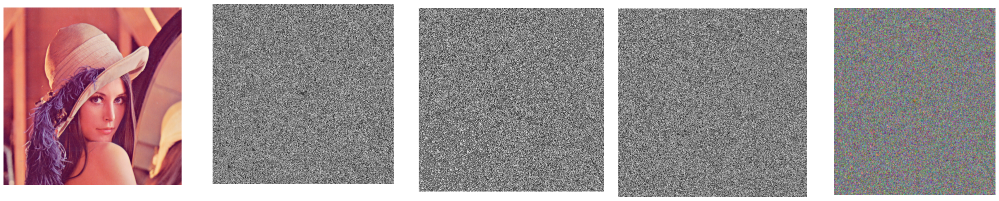


Fig 4. Block diagram of decryption technique using Pascal triangle



(a) (b) (c)(d)(e)

Figure 5: Result of Lena image a) Original Image b) R channel after encryption c) G channel after encryption d) B channel after encryption e) Encrypted Image

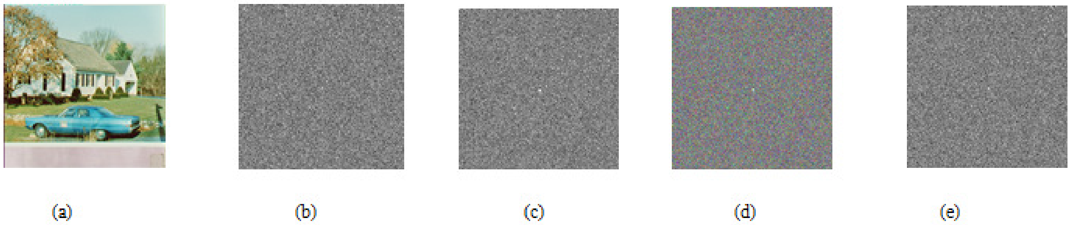
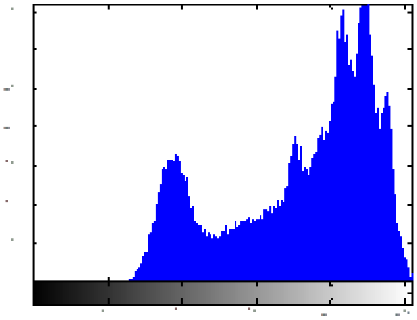


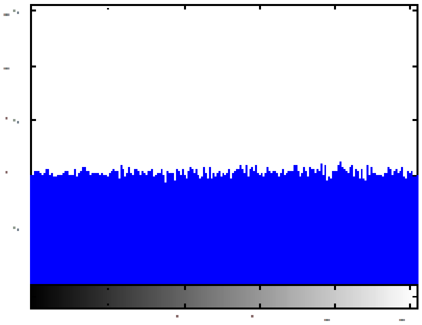
Figure 6: Result of House image a) Original Image b) R channel after encryption c) G channel after encryption d) B channel after encryption e) Encrypted Image

4.1 Histogram Analysis

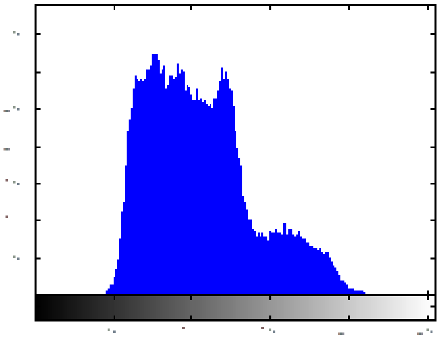
Distribution of pixels is shown in the histogram. For a dark picture, most of the information about data points resides either on left side or on center of the graph. On the other hand, for a brighter picture most of the information about data points resides either on right side or on center of the graph. A house image is considered and the Figures from 7a to 7h portrays step-by-step process of conversion. Finally, the encrypted image is entirely dissimilar to the initial input image and the points are completely scattered. Accordingly, the diffusion property is highly satisfied and proves its robustness to withstand against all possible harmful attacks. The encrypted image histogram is analogous to the methods explained by Sivakumar and Kishore kumar [4][9].



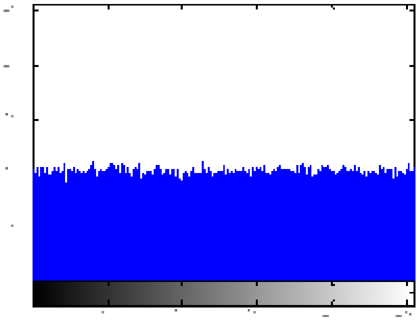
(a)



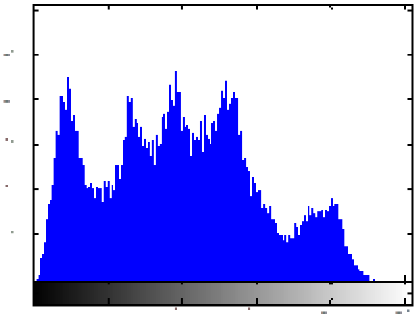
(b)



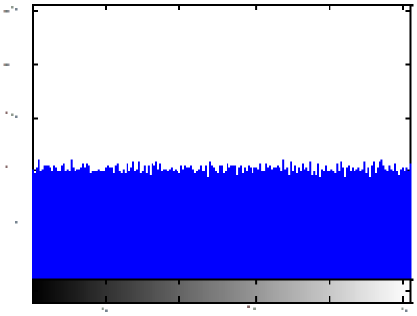
(c)



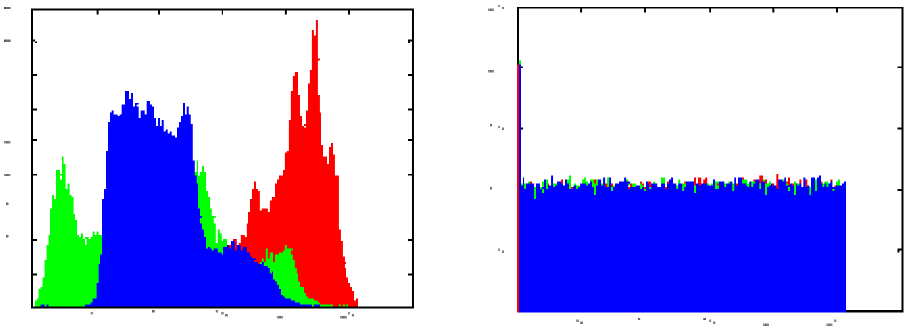
(d)



(e)



(f)



(g) (h)

Figure 7: Histogram results of House image a) Histogram of R channel of the image b) Histogram of R channel of the image after encryption c) Histogram of G channel of the image d) Histogram of G channel of the image after encryption e) Histogram of B channel of the image f) Histogram of B channel of the image after encryption g) Histogram of original image h) Histogram of encrypted image.

4.2 Correlation

Connectivity of variables between each other is indicated by the factor correlation ranging from - 1 to + 1. In computerized pictures, correlation seems to be high between contiguous pixels and is usually computed in different directions (vertical, horizontal, diagonal). The calculation is given in equation (4).

$$r_{xy}=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (4)$$

Adjacent pixels in the image are denoted by x and y. The right-side sub images of Figure 8 proves that the encrypted image is obtained in different orientations and the pixels are distributed uniformly whereas the pixels are present very close to the diagonal in the original input image.

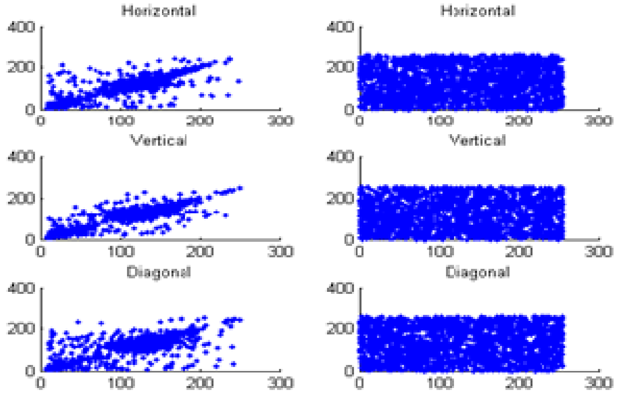


Fig. 8: Correlation value between original and encrypted image

4.3 Entropy

Quality/texture characteristics of the picture with high randomness is defined by the term "Entropy" and is denoted by

-sum(p.*log2(p)) (5)

where p is the count of pixels in the histogram. Eminent researches in the field already proves that for a good encrypted image entropy value will be mere closer to the value 8. Table 1 displays the entropy values of various encrypted images by applying the current research algorithm.

Table 1: Analysis of entropy value

Encrypted Image	Dimension	Entropy Value
Lena.tiff	512 X 512	7.7502
House.tiff	512 X 512	7.4858
Mandrill.tiff	512 X 512	7.7624

5. Conclusion

This paper proposes an innovative efficient image encryption technique based on Pascal triangle. Histogram analysis proves that the values are properly distributed in the encrypted image and it is completely different from the original input image. It also proves its robustness against invasive attacks. The correlation between the adjacent pixels of the cipher image is approximately close to zero ensuring low degree of correlation between the pixels in different directions (horizontal, vertical, and diagonal). In addition, the proposed method is appropriate for different dimension/size/format of the images with improved security.

References

[1]GarimaTanwar and Nishchol Mishra, “Survey on Image Encryption Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, 2015, Vol.5, pp.563-569.

[2]Yashpal singh Rajput and A K. Gulve,” A Comparative Performance Analysis of an Image Encryption Technique using Extended Hill Cipher”, International Journal of Computer Applications (0975 – 8887), June 2014, Vol 95– No.4.

[3]XingyuanWangn, LinTeng and XueQin,” A novel colour image encryption algorithm based on chaos”, Signal Processing 92 (2012) 1101–1108, Elsevier ,2011.

[4]T. Sivakumar and R. Venkatesan, “A Novel Image Encryption Approach using Matrix Reordering”, WSEAS Transactions on Computers, 2013, Issue 11, Vol 12.

[5]Cooper, R.H., Fredericton, NB, Hunter-Duvar, R. and Patterson, W., “A more efficient public-key cryptosystem using the Pascal triangle”, 'World Prosperity Through Communications', IEEE International Conference, 1989, vol.3, pp.1165 – 1169.

[6]Blessy Joy A. and R. Girish.” RGB Image Encryption Based on Bitplanes Using Elliptic Curve Cryptography”, International Journal of Advanced Research in Computer Science and Software Engineering, 2015, Vol.5, pp.128-132.

[7]B. Acharya, S. Patra, and G. Panda, “Image encryption by novel cryptosystem using matrix transformation,” Emerging Trends in Engineering and Technology, 2008.

[8]S. EmaldaRoslin, N.M. Nandhitha and Anita Daniel, “Transposition Based Symmetric Encryption and Decryption Technique for Secured Image Transmission through Internet”, International Conference on Circuit, Power and Computing Technologies [ICCPCT], IEEE, 2014.

[9]K. Kishore Kumar, S. Jayanthi, M. Saranya, V. Elamaran, “A Novel Encryption Method with Super Resolution Imaging Using DWT”, Advances in Intelligent Systems and Computing, Springer, 2015, Vol.397, pp 839-849.

[10]Majid Khan and Tariq Shah,” A Literature Review on Image Encryption Techniques”, Springer, 2014.

[11]Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, “Image Encryption using Elliptic Curve Cryptography”, Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015), Science Direct, 2015.

[12]MATLAB and Statistics Toolbox, The MathWorks, Inc., Natick, Massachusetts, United States, http://www.mathworks.com.

[13]William Stallings, “Cryptography and Network Security-Principles and Practice”, Pearson Education, 2011.