Digital Image Encryption Technique Using Block Based Scrambling and Substitution

Punita Kumari[1]

[1] Maharana Pratap University of Agriculture and Technology

Received: 14 December 2016 Accepted: 1 January 2017 Published: 15 January 2017

Abstract

A novel non-chaos based digital image encryption technique using a combination of diffusion and substitution process has been presented. A secret key of 128 bit sizes is used in the algorithm. In the diffusion (permutation) method, image is divided into different dynamic blocks which are key dependent. Further, each block is made to pass through eight rounds of permutation process. In this process, a zigzag mechanism is used to scramble the block pixels within the block. Then the resultant image i.e. the partially encrypted image is divided into various key based dynamic sub-images. Pixels of the sub-images are replaced with another pixel values within the block when each of the sub-images are passed through the substitution process. The substitution process comprises of four rounds. The proposed scheme is then compared with the standard AES algorithm. Investigation outcome shows that the proposed design methodology is efficient, fast and secure

---

Index terms**—** information security, image encryption, secret key, diffusion, substitution, AES.

1 I. Introduction

ue to the increasing use of computers and several advancements in information and technology, huge bulk of digital data is being transferred over the network. The transmitted information over the network needs security to protect the data [1,2]. Not only this, due to the rapid growth of internet, cell phones, multimedia technology in our society, digital image security is the most critical problem. Therefore, security of the digital data has become a major concern during its transmission and storage. Digital data can be secured in three different ways from unauthorized access. They can be classified as cryptography, steganography and watermarking [3] **??**4] **??**5] **??**6]. Among the three different techniques, cryptography provides a high level of security. Cryptography deals with converting the information into its coded form and then again decoding it into its original form. While communicating securely using cryptography, which is the main goal of our proposed work, in which encryption and decryption mechanisms are performed by one or more keys. Encryption and decryption techniques that use the same secret key are classified under private key cryptography and the algorithms are categorised under symmetric key cryptography **??**7] **??**8] **??**9]. When the key used in the encryption and decryption process are different, This paper reports a novel non-chaos based digital image encryption technique for the design of a secure and efficient encryption scheme.

2 II. Chaos and Non-Chaos Based Image Encryption Technique

For encryption and decryption of an image data different techniques have been used to protect the information from an unauthorized user. These techniques include (a) Non-chaos based image encryption schemes, and (b) Chaos-based image encryption schemes. In this paper, we discuss in brief about these techniques.

3 a) Chaos based encryption technique

Chaos refers to a state which is not deterministic in nature [20][21][22]. A chaotic system is dynamic and very sensitive to initial conditions; therefore the system depends completely on the initial condition. Hence, the results deviate largely with a small change in the initial conditions.

A chaotic system is also very useful and applied in various disciplines like physics, economics, environmental science, computer science etc.

In the present day scenario, security of digital images has become the fundamental need and has their own uses in numerous fields such as medical imaging, internet communication, Tele-medicine, multimedia systems, military communication etc. It includes various aspects like authentication, integrity, confidentiality, access control etc. It has been observed that traditional encryption algorithms like DES, AES etc **??**13] **??**14][15][16][17][18][19] are not suitable to encrypt images directly because of the two reasons, firstly; the size of image is larger than that of text. Therefore, traditional encryption algorithms will take more time to encrypt and decrypt images as compared to that of text. Secondly, in text encryption, both the size of the original and decrypted text must be equal. But this is not possible in case of images because due to the characteristics of human perception, decrypted image with small distortion is usually acceptable. We can reduce this observable information by decreasing the correlation among image pixel elements using different techniques.

4 b) Non-chaos based encryption technique

A non-chaotic system refers to a state having deterministic behavior [23] like DES, AES etc.

In this paper, a non-chaos based image encryption technique has been proposed. A novel diffusion-substitution technique for image encryption has been applied to encrypt a digital image along with its performance and security parameters to test the histogram analysis, correlation coefficient, entropy etc. However, the proposed methodology is used to achieve an efficient and secure image transmission over the network.

5 III. proposed methodology for digital image encryption based on block based scrambling and substitution

In the present work, an image encryption technique design is proposed. Detailed architecture of the diffusion-substitution mechanism in the proposed image encryption algorithm has been described. To design the encryption technique, scrambling of the image pixel values is performed and then further modification in the pixel values of the partially encrypted image is being done so as to reduce the correlation among the pixels of an image. In this scheme, a secret key of 128 bit size is used. Then, image is separated into various dynamic blocks. Diffusion process involves eight rounds and block size in each round is kept different which depends on the secret key used in the proposed scheme. In this scrambling process, shuffling of the pixel values within the same block is performed by a zigzag path which is shown in Figure 2. After the diffusion process, substitution process is applied. In this process, the blocks are reframed and are then passed through four rounds. Since each block depends on the secret key, therefore block size in substitution process differs from the diffusion process. In substitution mechanism, modification in the pixel values are performed within each block and the pixel values are replaced with another pixel values.

The proposed scheme is performed to achieve a secure and efficient multimedia communications while its transmission over the network. Moreover, performance and security of the proposed image encryption technique is assured by performing the NIST (National Institute of Standard and Technology) test. The design flow given in Figure 1 shows the working of the proposed technique for the encryption of an image. Different units along with their functions that are used in the proposed scheme have been described below in detail.

6 a) Block size of plain image

In the permutation and substitution process, the image pixels are partitioned into various nonoverlapping squared dynamic blocks. The size of these blocks is a secret key dependent which is used in the algorithm. The plain image block sizes in diffusion process are decided by using Equation **??**.B r = 4 1 p= ? K (4*(r-1)+p) (Permutation process) ? (1)

where, K i = i th subkey and B r = block size in r th round.

7 b) Diffusion process

In the diffusion process, pixel values of each dynamic block are shuffled by a zigzag mechanism. For example, the pixels of a block having the size 8*8 are rearranged by a path which is shown in Figure 2. In this figure, suppose the pixel location is at (2, 3) before traversing, the pixel path is found to be at (3, 2) when the traversing process is completed. The block pixels are organized sequentially i.e. row by row and column by column in the same block during the traversing mechanism. The pixels are separated into three RGB channels (red, green and blue). All of these channels pass through eight rounds of scrambling process. The Year 2017

8 ( ) F

Digital Image Encryption Technique using Block based Scrambling and Substitution image pixels in each round are partitioned into various non-overlapping squared dynamic blocks which is discussed above in subsection a. When traversing is started, the path in blocks of r th round of a pixel (X r , Y r) depends on a secret key which is shown in Equation **??**.X r = 3 1 p= ? K (4*(r-1)+p) , Y r = 4 2 p= ? K (4*(r-1)+p) ?? (2)

where, K i is the i th subkey.

9 c) Substitution process

In the substitution process, a simple computation is performed on pixels to change their properties. Each RGB channel of pixels comprises of four rounds. In each round, pixels are partitioned into various non-overlapping dynamic squared blocks which is explained earlier in sub-section a.

In this process, bitwise XOR operation is accomplished on the pixels with randomly selected subkey so that their properties can be changed. In the proposed methodology, four rounds are used in the substitution mechanism and each round is secret key dependent used in the algorithm. To illustrate substitution process for random selection of sub key, we have used srand() function of C++ programming language. For first round, seed value for srand() function is used as summation of first four sub keys i.e. K 1 ..K 4 and for second round, seed value for srand() function is chosen as summation of next four sub keys i.e. K 5 .. K 8 and so on. Substitution process is described below: In the proposed encryption algorithm, which consists of two major processes -permutation and substitution [24][25][26]. Both permutation and substitution processes completely depends on the secret key. The steps of algorithm are described below.

10 IV. Experimental Results

The data sets required to evaluate the proposed methodology was generated using USC-SIPI image database (http://sipi.usc.edu/database/). The implementation of the proposed algorithm has been performed in C++ programming language and for the analysis of the image data, MATLAB application tool has been used. The permutation and substitution based methodology is evaluated with performance and security measures by which the performance and security of the proposed image encryption algorithm is tested and analysed.

11 a) Pixel distribution

The plain images and its corresponding encrypted images of different sizes are examined and evaluated by histograms. The proposed image encryption algorithm is consistent with the security defined by Shannon [27,28].

A preferred image ”Lena” is analysed by histogram analysis. Histograms of RGB channels of plain image (Figure **??**(a)) are shown in Frames (b), (c) and (d) of Figure **??** respectively. In Frames (f), (g) and (h) of Figure **??**, the histograms of RGB channels of the encrypted image (Figure **??**(e)) for the proposed scheme is shown. In Frames (j), (k) and (l) of Figure **??**, the histograms of RGB channels of the encrypted image (Figure **??**(i)) for AES algorithm is shown respectively.

From the histogram analysis of the original, proposed and AES algorithm encryption scheme, we analyze that the histograms of the encrypted image of the proposed methodology i.e. its RGB components are very close to the uniform distribution which is not in case of the original image and do not correspond to the original image. Therefore, the cipher image does not reveal anything about the original image. Year 2017 ( )

12 b) Correlation between original and encrypted images

The correlation coefficient between the different colour channels of the plain and its corresponding encrypted image is calculated using the proposed image encryption scheme and AES algorithm. In Table **??** and Table 2, for some images, the results have been calculated. Since the correlation coefficients calculated are very low (C? 0) which is shown in Table **??** and Table 2, which therefore indicates that the plain images are different from the encrypted images. And this shows that our result is consistent with the full security defined by Shannon.

Table1: Correlation coefficient for the proposed algorithm between plain images and their corresponding encrypted images.

Image size 3 shows the entropy value for the proposed encryption scheme and AES algorithm for different images. The information entropy value obtained for the proposed scheme is 7.99 which is very close to the ideal case but in case of AES algorithm, the value obtained is 2.91 which deviates a lot from an ideal case. This shows that the proposed image encryption algorithm achieves a high order of diffusion and substitution and has a robust performance. C R1R2 C R1G2 C R1B2 C G1R2 C G1G2 C G1B2 C B1R2 C B1G2 C B1B2

13 Conclusion

The paper presents a block based scrambling and substitution based image encryption technique for designing an efficient, robust and secure encryption scheme for digital data. The proposed image encryption scheme is designed to secure the communication of multimedia data. The necessary security and performance constraints are incorporated in the proposed methodology which provides a good, secure and an efficient image encryption algorithm. The results clearly elaborates that the proposed method is able to generate an encryption scheme which is secure and efficient as compared to the popular standard algorithm. [1] [2]

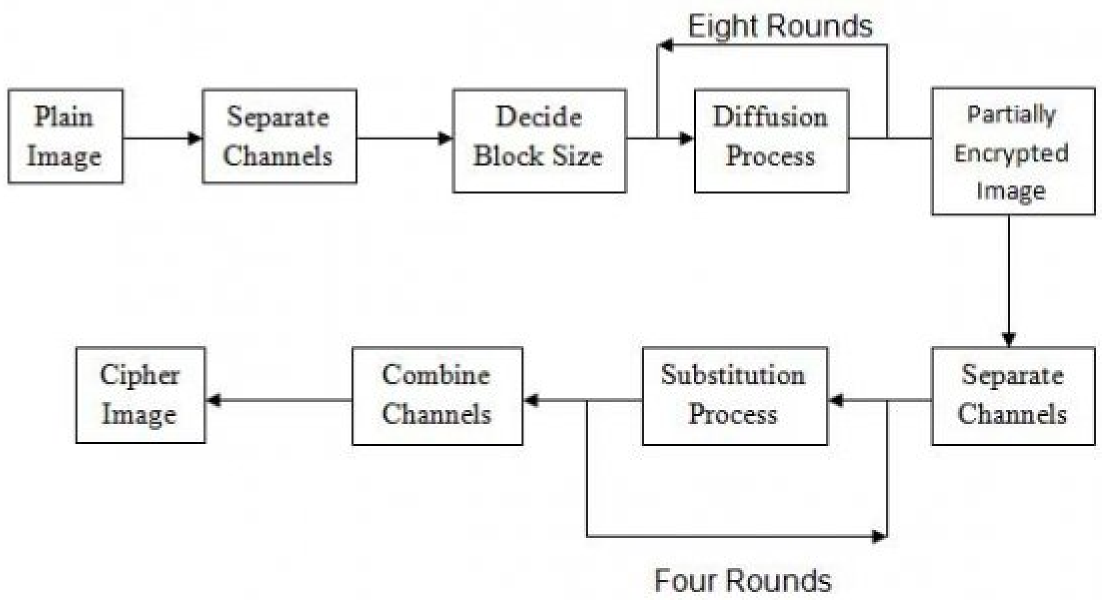


Figure 1: D

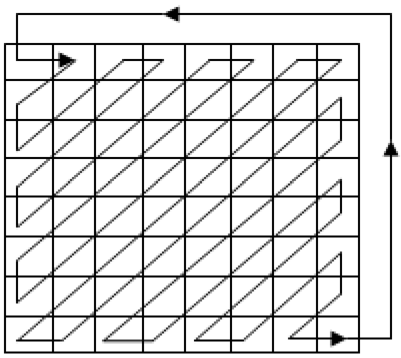


Figure 2:

[1] © 2017 Global Journals Inc. (US)

[2] . Chen, T., Wang, J., & Zhou, Y. 2001. Combined

Figure 3: F

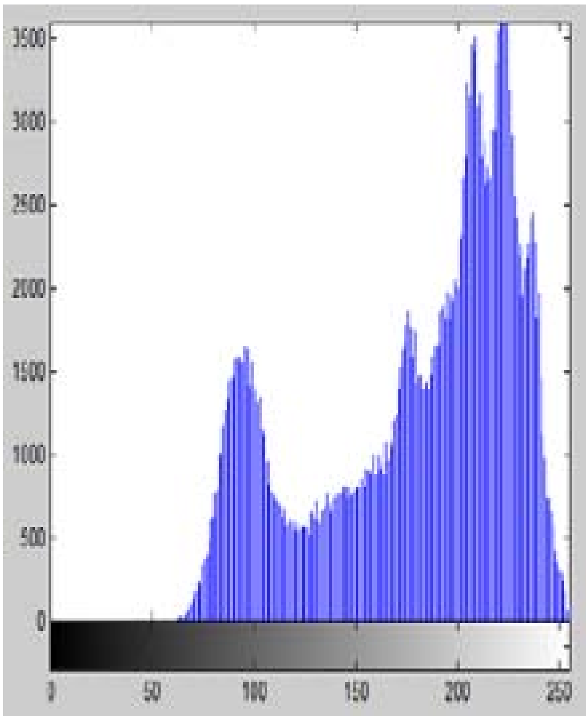
1 

Figure 4: Figure 1 :

2

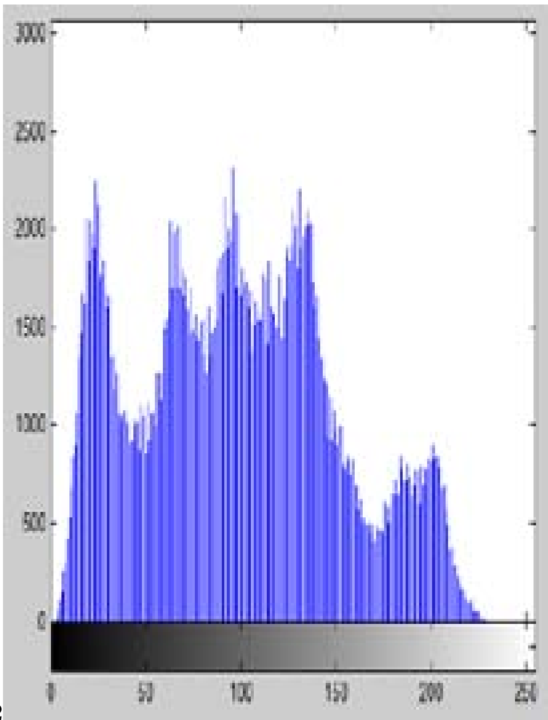


Figure 5: Figure 2 :

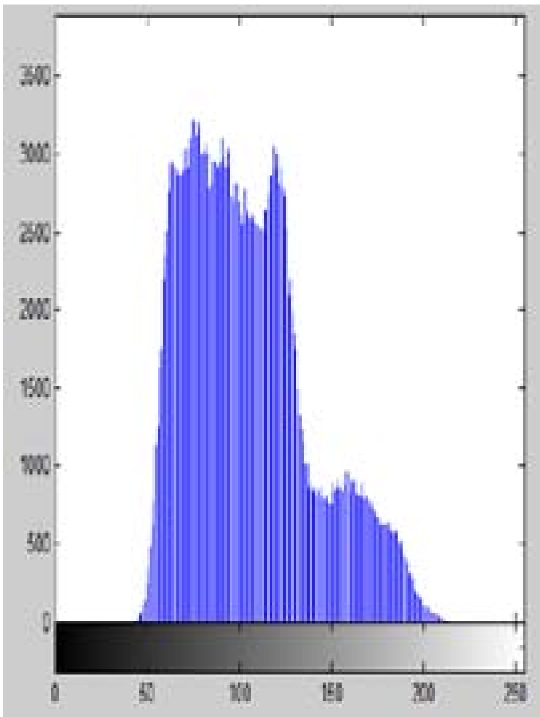


Figure 6: Row=For

201

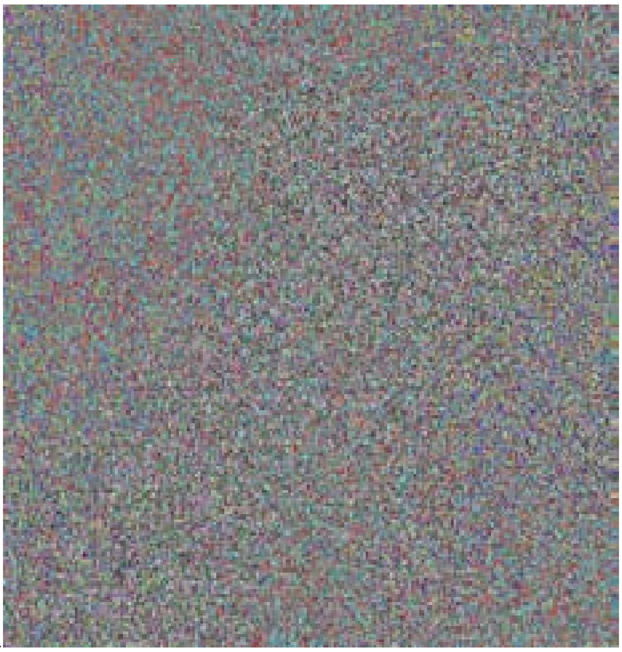


Figure 7: Input:© 20 7 1 F

2

Lena 512*512	-0.0013	-0.00095	0.0001	-0.0006	-0.0022	0.00094	0.00027	-0.0027	0.00044
Baboon 200*200	-0.0039	-0.0081	-0.0031	-0.0120	-0.0019	0.00079	-0.0101	0.00061	-0.000
Peppers 200*200	-0.0012	0.0012	0.0039	0.00052	0.0020	0.0012	-0.0020	0.00005	0.005
Tiger 800*600	0.00046	-0.00065	-0.0009	-0.00006	-0.0008	-0.0007	0.00025	-0.0008	-0.000
Sunset 440*262	0.00045	0.0036	0.0024	0.0016	0.0057	0.0015	0.00051	0.0021	-0.000
Airplane 512*512	0.0044	0.0045	0.0021	0.0042	0.0042	0.0015	0.0041	0.0036	0.000

Figure 8: Table 2 :

3

Images	Entropy of plain images by proposed and AES Algorithm	Entropy of encrypted images by Proposed Algorithm	Entropy of encrypted images by AES Algorithm
Lena	7.7502	7.9997	2.9109
Baboon	7.6430	7.9983	2.9184
Peppers	7.7150	7.9982	2.9234
Tiger	7.8261	7.9999	2.9076
Sunset	7.3460	7.9988	2.9097
Airplane	6.6639	7.9995	2.9127
V.			

Figure 9: Table 3 :

[Fips ()] *140-1: Security requirements for cryptographic modules*, P Fips . 1994. p. 11. National Institute of Standards and Technology

[Fips ()] *140-2. Security Requirements for Cryptographic Modules*, P Fips . 2001. p. 25.

[Yu et al. ()] 'A chaos-based image encryption algorithm using wavelet transform'. Z Yu , Z Zhe , Y Haibing , P Wenjie , Z Yunpeng . *IEEE 2nd International Conference in Advanced Computer Control*, 2010. 2 p. .

[Zhao et al. ()] 'A Chaos-based Image Encryption Scheme Using Permutation Substitution Architecture'. J Zhao , W Guo , R Ye . *International Journal of Computer Trends and Technology* 2014. 15 (4) p. .

[Shannon ()] 'A mathematical theory of communication'. C E Shannon . *bell System technical Journal* 1948. 27 p. .

[Zeghid et al. ()] 'A modified AES based algorithm for image encryption'. M Zeghid , M Machhout , L Khriji , A Baganne , R Tourki . *International Journal of Computer Science and Engineering* 2007. 1 (1) p. .

[Lai et al. ()] 'A Novel Image Encryption Algorithm Based on Fractional Fourier Transform and Chaotic System'. J Lai , S Liang , D Cui . *IEEE International Conference on Multimedia Communications*, 2010. p. .

[Yahya and Abdalla ()] 'A shuffle image-encryption algorithm'. A A Yahya , A M Abdalla . *Journal of Computer Science* 2008. 4 (12) p. .

[Rijmen and Daemen ()] 'Advanced encryption standard'. V Rijmen , J Daemen . *Proceedings of Federal Information Processing Standards Publications*, (Federal Information Processing Standards Publications) 2001. p. . National Institute of Standards and Technology

[Shannon ()] 'Communication Theory of Secrecy Systems'. C E Shannon . *Bell System of Technical Journal* 1949. 28 (4) p. .

[Pub ()] *Data Encryption Standard (DES). FIPS PUB*, F Pub . 1999. p. .

[Narendra and Pareek ()] 'Design and analysis of a novel digital Image encryption scheme'. K Narendra , Pareek . *International Journal of Network Security & Its Applications* 2012. 4 (2) p. .

[Noura et al. ()] 'Design of a Fast and Robust Chaos-Based Cryptosystem for image encryption'. H Noura , S El Assad , C Vl?deanu . *IEEE 8th International Conference on Communications (COMM)*, 2010. p. .

[Subramanyan et al. ()] *Image encryption based on AES key on Emerging of Information Technology*, B Subramanyan , V M Chhabria , T S Babu . 2011. p. .

[Diffie and Hellman ()] 'New directions in cryptography'. W Diffie , M Hellman . *IEEE transactions on Information Theory* 1976. 22 (6) p. .

[Jolfaei et al. ()] 'On the Security of Permutation-Only Image Encryption Schemes'. A Jolfaei , X W Wu , V Muthukkumarasamy . *IEEE Transactions on Information Forensics and Security* 2016. 11 (2) p. .

[Daemen and Rijmen ()] 'The design of {Rijndael}:{AES}—the {Advanced'. J Daemen , V Rijmen . *Journal of Cryptology* 1991. 4 (1) p. .