An Efficient Adaptive Encryption Algorithm for Digital Images

Shashank Shekhar, Harshita Srivastava, and Malay Kishore Dutta

Abstract—**This paper proposes an efficient method for encryption of digital images using an adaptive algorithm. According to the proposed algorithm the image used was segregated into significant and non significant blocks. For making the level of security different for different blocks, total and partial encryption has been utilized for the significant and non significant blocks respectively. Spatial as well as transform domain for the significant and non significant blocks respectively are used in this proposed method. The final encrypted image reflects the efficacy of the proposed algorithm. A comparative study between the conventional approaches of spatial and transform domain for the encryption of the image with the proposed encryption algorithm reveals the superior performance of the proposed algorithm. The experimental results suggest that the decrypted image is of excellent quality and signal to noise ratio is maintained well within the limit. The computational time utilized is very less as compared to the conventional approach, which suggests the enhanced overall performance and makes it suitable for high speed online applications.**

Index Terms—**Arnold catmap, image encryption, logistic map, spatial and transform domain.**

I. Introduction

Security of Security of digital images is a seriously challenging issue in recent times. With the advent of increase in transmission and distribution of the image, illegal practice has also boomed. To restrict these illegal and piracy operations security of various level is required. The proposed algorithm for the encryption of image turns out to be effective and efficient way of protecting the digital images over the internet. Most of the conventional encryption techniques are based on the spatial and transform domain which gives same level of security to the entire image, and the computational time used is very high. In [1] the Wang et. al. have used image encryption method in transform domain, whereas in [2] spatial domain has been used individually. In both these cases the computational time consumed is large as compared to our proposed algorithm. In the proposed algorithm we have used a combination of the spatial as well as transform domain. Wavelet based partial image encryption [3] is also proposed for digital image security. In [4] the impact of using random coefficient permutation is investigated to provide confidentiality to wavelet based still image compression pipelines. In [5], [6] Arnold cat map and in [7] logistic map has been proposed for encryption of images. Use of chaotic system proposed in [8] for encryption of digital images. In the proposed algorithm image is divided into significant and non significant block. The level of security provided is different for different blocks using different encryption technique. Significant block is encrypted using total encryption technique while the non significant is encrypted using partial encryption technique thereby providing us with reduced computational resources and time. Arnold map employs shearing and wrapping operation to completely scramble a matrix after several iterations and hence the pixels are traversed to new position with each of the iteration. With Arnold cat map we get a distorted matrix of image, it is a preferable method for the image scrambling. Owing to perfect chaotic properties Logistic map has been used as a pseudorandom sequence generator. Both these map have enormous key space thereby making the image far less vulnerable. The paper is organized as follows. Section 2 gives an overview of the segregation of the image. The next section 3 describes the encryption method of the image. Section 4 describes the decryption method. Experimental results are presented in section 5. Finally, Section 6 concludes the paper.

Manuscript received April 9, 2012; revised May 23, 2012.

S. S. Author is with the Delhi College of Engineering, Delhi, 110084, India (e-mail: shashankshekhar74@gmail.com).

H. S. is with IIT Delhi, Delhi, and 110017 India (e-mail: harshita.1589@gmail.com)

M. K. D is with the Electrical Engineering Department, Amity University, oxide, 201303.India(e-mail: malaykishoredutta@gmail.com)

II. Segregation of the Image

To make the encryption part more efficient and adaptive, the original image has been segregated into significant and non significant block. Total encryption is applied to the significant block. DWT has been applied in the non-significant block and only the approximate coefficients have been encrypted which saves as lot of computational resources.Following steps describes the various steps for the segregation.

- PREWITT edge detector is used to produce an edge detected output of the original image.
- Next the original image as well as the edge detected image is divided into non- overlapping blocks of size m*m, thereby giving 'p' number of blocks, and 'm' is user defined.
- Total number of EDP is calculated, denoted by E_{total}
- Now calculate the average number of EDP's in a block using the formula $E_{average}=E_{total}/p$
- For identifying the significant portion of the image a threshold is defined , as given by Ethreshold=Eaverage*Q
- Similarly total number of EDP's is calculated for each

of the block separately.

- Those block which has EDP > $E_{threshold}$ are termed as significant block leaving the rest as non significant block.
- After this step a 1*p row matrix named as Binary significant vector (BSV) was created where each term was given a value either '1' or '0'.A '1' represent that the block is significant and '0' indicates non significant block.

where EDP is edge detected pixels which represent the total number of pixels, whose value is '1'. Q is defined as 1.25

III. Encryption of the Image

The segregated image obtained above is encrypted using spatial domain encryption for the significant block and transform domain encryption for the non significant part.

A. Encryption of Significant Part (Module 1)

For the encryption of significant block, we have used Logistic map as a pseudorandom sequence generator. The Logistic Map has high sensitivity towards initial condition. Hence even with slightly different initial condition, the chaotic output generated by the logistic map is completely different, thereby providing high level of security to the encrypted image in case of any intrusion.A single dimension Logistic map is mathematically represented as $X_{n+1} = r X_n (1-X_n)$, where $0 <= X_n <= 1$ and r represents "growth rate". Following are the steps describing the Encryption of the significant block.

- The significant block is scrambled using n iterations of the Arnold cat map.
- The Logistic map is iterated using the initial condition t and is used to generate a chaotic matrix of size m*m, where m denotes the block dimension.
- The scrambled block obtained in the first step is summed with the discretise output of the chaotic matrix obtained in the second step to get the modified version of the original significant block.

B. Encryption of the Non-Significant Block (Module 2)

DWT is applied to the non significant block, resulting in separation of approximate coefficients. Further we scramble the approximate coefficient part with the help of Arnold cat map iterations and Logistic map. The various steps for the encryption are described below.

- The insignificant block obtained during the segmentation has to go L-level DWT.
- The approximate co-efficient obtained during the first step is scrambled using Arnold Catmap.
- To generate completely scrambled block, L level IDWT is performed.
- The output obtained is summed with the discretise output of the logstic map.
- Thus we get the encrypted counter part of non significant part as shows in Fig 5.
-

IV. Decryption of Image.

Corresponding to the BSV received through the additional channel significant and non significant block are identified.

C. Decryption of Significant Part.

Following steps are used for the decryption of the significant blocks.

- Iterate the Logistic map with initial condition t to generate random vector which is rearranged into a block of size m*m.
- The descritised output of the random vector is subtracted from the encrypted block.
- The output of the step 2 is descrambled using (y-n) iterations of Arnold cat map to generate the decrypted output. Where, n is the number of iteration used in the encryption process and y is the periodicity of Arnold cat map.

D. Decryption of Non-Significant Part.

Following steps are used for the decryption of the non-significant blocks.

- Iterate the logistic map with initial condition t to generate random vector which is rearranged into a block oh m*m.
- The output of the random vector is subtracted from the encrypted block.
- Perform L-level DWT and descramble approximate coefficient using y-n iteration of the Arnold catmap.
- Perform L-level IDWT to retrieve the correct sub-band. Where n is the number of iteration used in the encryption process and y is the periodicity of Arnold catmap.
-

V. Experimental Result

The paper proposed encryption technique for still visual data. In the experiment seven different images of size 256*256 pixels were tested. The sole aim of the paper is basically to make a comparative analysis of the conventional encryption approach with our proposed algorithm. For this purpose we have considered two cases. In the first case the entire image is encrypted with the module developed for significant block. In the second case complete image data is encrypted with the module developed for the non significant block. These two cases denote image encryption in complete spatial and transform domain respectively. Two tests were conducted, one for PSNR and the other for computational time analysis. The result for the Computational time has been shown in Table I. In Table II, we have represented the various EDPs calculated for different blocks. Following graph shows the relative study of PSNR for spatial, transform and proposed algorithm.

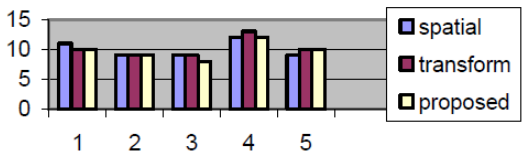

Fig. 1.PSNR (dB) for different images using different Encryption Technique

Formula:PSNR= $[10\log(R\text{^}2)]/MSE$ dB

$$MSE = \frac{\sum [I(m,n) - J(m,n)]^{\wedge}2}{M * N}$$

MSE = Men Squared Error
I = Original Image
J = Decrypted Image
M = No. of columns
N = No. of rows

Table I, Gives the comparative analysis of the conventional timing and proposed algorithm. It has been observed that computational time of our proposed algorithm is much less than conventional algorithm. In Table II we have calculated the EDPs for various significant and non significant blocks**.**

TABLE I: TIME TAKEN BY DIFFERENT ENCRYPTION ALGORITHM

	Spatial	Transform	Proposed Encryption
Lena	10.07	8.88	8.25
Mendrill	11.50	9.91	7.87
Cameraman	9.86	8.27	7.98
Barbara	9.87	8.99	7.12
Hut	10.24	9.67	7.93

TABLE II: EDP OF DIFFERENT BLOCKS

Blocks	EDPs	Nature
1	7	Non-significant
2	45	Non-significant
3	36	Non-significant
4	190	Non-significant
5	53	Non-significant
6	232	Significant
7	147	Non-significant
8	119	Non-significant
9	192	Non-significant
10	302	Significant
11	386	Significant
12	292	Significant
13	250	Significant
14	59	Non-significant
15	109	Non-significant
16	109 Total= 2528	Non-significant

$E_{average}$ = 2528/1
Therefore,
$E_{threshold}$ =158*1.25=198

Fig. 2. Original lena

Fig. 3. Edge detected

Fig. 4. Significant block

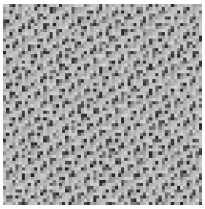

Fig. 5. Scrambled image

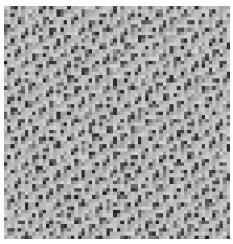

Fig. 6. After sum operation

Fig. 7. Non significant block

Fig. 8. DWT of the non significant part

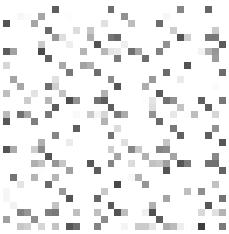

Fig. 9. Scrambled CA

VI. CONCLUSION

A novel prototype of encryption scheme has been proposed in this paper. Different level of encryption is performed depending upon the significant and non significant block, leading to the enhanced overall performance by reducing the computational resources as well as the computational timing. On the basis of comparison between the proposed encryption technique and spatial / transform domain encryption technique it is found that the PSNR of the spatial or transformation domain encryption is same to the proposed encryption technique. This indicates a similar level of incomprehensibility in the encrypted output of these cases.

Apart from the PSNR analysis, the computational time consumed is also observed. It is observed that computational time required for spatial and transform domain is higher than the proposed algorithm. On an average, the proposed algorithm is 18% faster than the transform domain encryption technique where it is 30-35% faster than conventional spatial domain encryption technique.

ACKNOWLEDGMENT

F. A. Author thanks the Professors at Priyadarshini College of Computer Science for their unconditional support and encouragement.

REFERENCES

[1] Q. Wang, Q. Ding, Z. Zhang, and L. Ding, "Digital Image Encryption Research Based on DWT and Chaos," *2008 Fourth International Conference on Natural Computation*, 2008.

[2] Z. M. Liao, X. Feng and Z. Qing "Spatial Domain Image Selective Encryption Algorithm Based on Quadtree Encoding," *Jisuanji Gongcheng / Computer Engineering*, vol. 34, no. 18 .Sept. pp. 174-175, 178, 2008.

[3] N .A. Flayh, R. Parveen, and S. I. Ahson, "Wavelet Based Partial Image Encryption," *Multimedia, Signal Processing and Communication Technologies*, IMPACT'09, 2009.

[4] R. Norcen and A. Uhl, "Encryption of wavelet-coded imagery using random permutations," in *Proc. IEEE Int. Conf. Image Process*, Singapore, pp. 3431-3434, 2004.

[5] L. L. Wu, J. Zhang, W. Deng, and D. He, "Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm," *Information Science and Engineering (ICISE)*, 2009 1st International Conference, pp. 1164-1167, 2009.

[6] W. B. Chen and Z. Xin, "Image Encryption Algorithm based on Henon Chaotic System," *Image Analysis and Signal Processing*, ISAP 2009.

[7] M. K. Sabery and M. Yaghoobi, "A New approach for the image encryption using cahostic logistic map," in *Proc IEEE, Phuket*, January pp. 585-590, 2009.

[8] Y. Wang, G. Ren, J. Jian, and Z. L. Sun, "Image encryption method based on chaotic map," *Industrial Electronics and Applications*, 2007.