A New And Secure Chaos Based Multimedia Encryption Scheme

Payal Maggo[1], Dr. Rajender Singh Chhillar[2]
[1](Research Scholar, Department of Computer Science and Applications, M.D. University, Rohtak, Haryana-124001
[2](Head of Department, Department of Computer Science and Applications, M.D. University, Rohtak, Haryana-124001

ABSTRACT

There has been a sudden rise in the usage of Multimedia data in the digital world. Be it images, videos or audios, there has been a high demand in their usage and transfer. Lots of applications are based on this type of Multimedia data. And this gives rise to the need for their protection. Data security has seen many types of traditional algorithms for the protection purpose but they have struggled to combat multimedia data as compared to regular textual data. A separate group of Algorithms based on Substitution-Permutation techniques have been used widely in the security. This paper proposes a scheme based on a new permutation technique and chaos based substitution method. The scheme works well on normal as well as highly redundant images. Various types of attacks like statistical, differential and visual have been performed on the algorithm and observations have been reported. The result shows improvements over recent schemes in the field of Multimedia Security.

Keywords **–** Chaotic Maps, Image Encryption, Image Security Analysis, Multimedia Security, Shuffling Schemes

I. INTRODUCTION

With the advancements in the field of Information Technology especially in Computer Science and Telecommunications, Multimedia [1] data has gained a lot of importance in a number of applications. Unlike ordinary data, Multimedia applications have the following characteristics - High data rate, Power utilization, Real-time constraints, Synchronous, Continuous and may have Different distribution channels like Internet, TV, Satellite and Wireless. With the ease of hacking and illegal capturing of this type of data, major challenge arises to protect the content of media from eavesdropper while sending it over a public or private network. Multimedia security [2] aims at designing the set of schemes that can protect this type of content. In order to cover such an enormous task, Cryptography [3] [4] has been taken help of and lots of encryption techniques [5] have been proposed, designed and developed.

These techniques can be broadly divided into four categories [6]. First being the **Substitution** based scheme, where a part of plaintext is being replaced or substituted by the cipher text. Second is the **Permutation** based scheme [7] where plain image is encrypted by permuting the positions of all pixels in a secret way. The other two are the combination of **Substitution-Permutation** scheme [8] and **Chaos Based** scheme using a chaotic map [9]**.** However such encryption schemes have been found weak and were unreliable and non-robust. Later on Symmetric key Crypto-systems were introduced. All the Symmetric key cryptosystems have a common property that they rely on a key that is being shared by both sender and the receiver for encryption and decryption respectively. The Advanced Encryption Standard (AES) [10] [11] algorithm is one of the symmetric key cryptosystem that processes 128-bit data blocks using cipher keys with lengths of 128, 192, or 256 bits.

AES [12] became very popular as it was quite difficult to decipher the text within a shorter time span and thus provided high security. However, AES could not be used directly to encrypt the multimedia images due to the intrinsic characteristics of images such as bulk data capacity, high correlation among the pixels and high redundancy. This way multimedia data's encryption via AES remains a big challenge for everyone unless redundancy is removed. Therefore, researchers have moved towards Chaos based Encryption Techniques for multimedia encryption. This is due to the fact that this set of schemes has the features that fulfill the requirements of cryptography, such as aperiodicity, sensitive dependence on initial conditions, ergodicity and random-like behaviors. The mix of all these features helped the chaos based encryption techniques to provide a good combination of speed, complexity, high security and less overhead. Many security models and crypto-systems based on number theory and chaotic map have already been proposed [13] [14] [15] [16] [17] [18]. But it is found that some of them [13] [14] [19] are weak in view of computational complexity and strength of security [15] [17].

Therefore developing a cryptosystem that could provide Integrity, Availability as well as Confidentiality to the multimedia content has become the curious field of research. In this paper, we are presenting a multimedia security scheme which aims at providing a newly established shuffling scheme for multimedia to work efficiently at bit level and providing security through usage of chaotic maps at byte level. The chaotic encryption uses a 1D logistic map and Circle Map which takes initial conditions as input via secret key for generating a chaotic sequence. The proposed scheme has been compared with a Chaos Based scheme called PESH [20] and byte level implementation [21] of new shuffle with PESH.

This paper has been organized in the following manner – Section 2 talks about existing scheme, Section 3 explains the proposed methodology, Section 4 displays implementation and results and Section 5 concludes the paper. References are mentioned at the end.

II. Existing Scheme

The existing scheme PESH can be denoted through the block diagram given in Fig. 1.

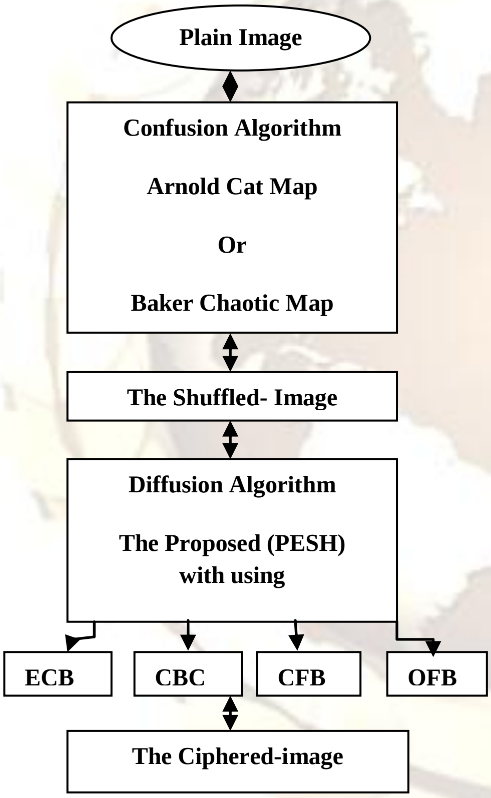


Figure 1. The Diagram for illustration of Encryption & Decryption process for PESH Scheme

The process starts with a random permutation of pixels using Arnold cat map or Baker Chaotic map which is diffused using PESH scheme based on Chaos based diffusion process in varied modes like ECB, CBC, CFB and OFB.
Similarly, a new scheme [21] was devised to replace the permutation process in the start. The permutation was divided into five stages as shown in Fig. 2. The main criterion for this scheme is to change the pixel position on the basis of key in four different directions to spread the pixels uniformly across the given space.

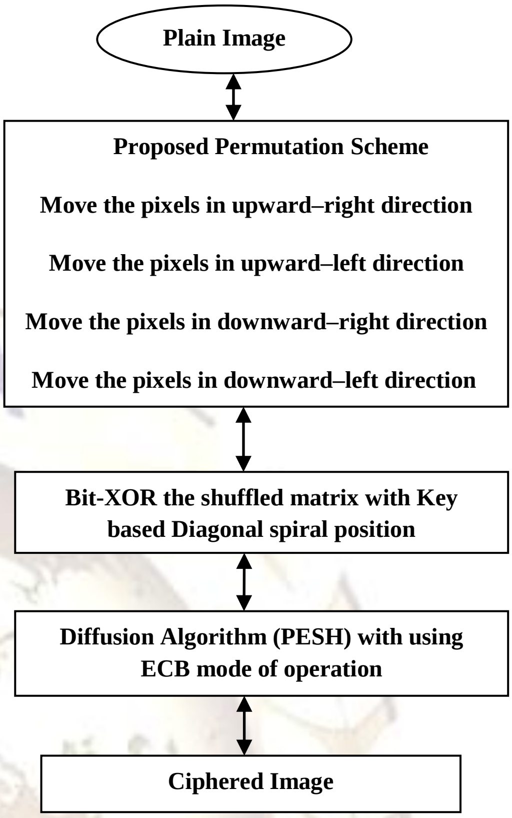

Plain Image
Proposed Permutation Scheme
Move the pixels in upward–right direction
Move the pixels in upward–left direction
Move the pixels in downward–right direction
Move the pixels in downward–left direction
Bit-XOR the shuffled matrix with Key based Diagonal spiral position
Diffusion Algorithm (PESH) with using ECB mode of operation
Ciphered Image

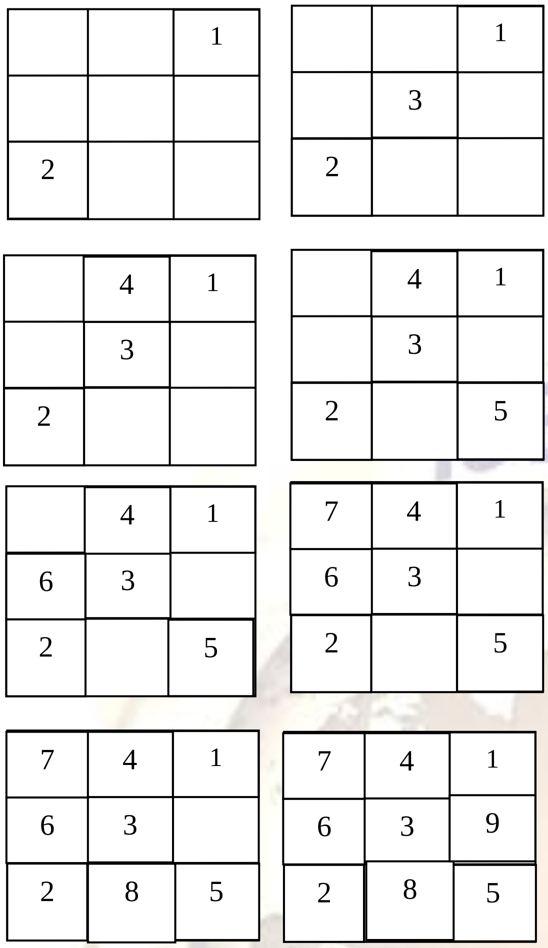
Figure 2. The Diagram for illustration of Encryption & Decryption process for New permutation process with PESH Scheme

The new permutation scheme works on a standard principle of generating a magic square through Siamese Method [21] [22]. The positions are filled according to the following format:

- A location is selected in the matrix as the start position for row and column
- The position is incremented to reach the adjacent diagonal position in four different directions as per four different schemes respectively
- In case of a collision i.e. already filled up position, the vertical or horizontal adjacent positions are filled instead of diagonal ones with respect to the direction of algorithm
- A simple case of filling a 3x3 empty matrix with a sequence of numbers from 1-9 in the upward right direction diagonal only and start position as (2,2) is depicted as

	Start	

		1



		1
2		

		1
	3	
2		

	4	1
	3	
2		

	4	1
	3	
2		5

	4	1
6	3	
2		5

7	4	1
6	3	
2		5

7	4	1
6	3	
2	8	5

7	4	1
6	3	9
2	8	5

Figure 3. The step by step illustration of filling up of 3x3 matrix with sequence of number from 1-9 in upward right directions. The boundary conditions are also kept intact. Similarly other three directions can be worked on the matrix.

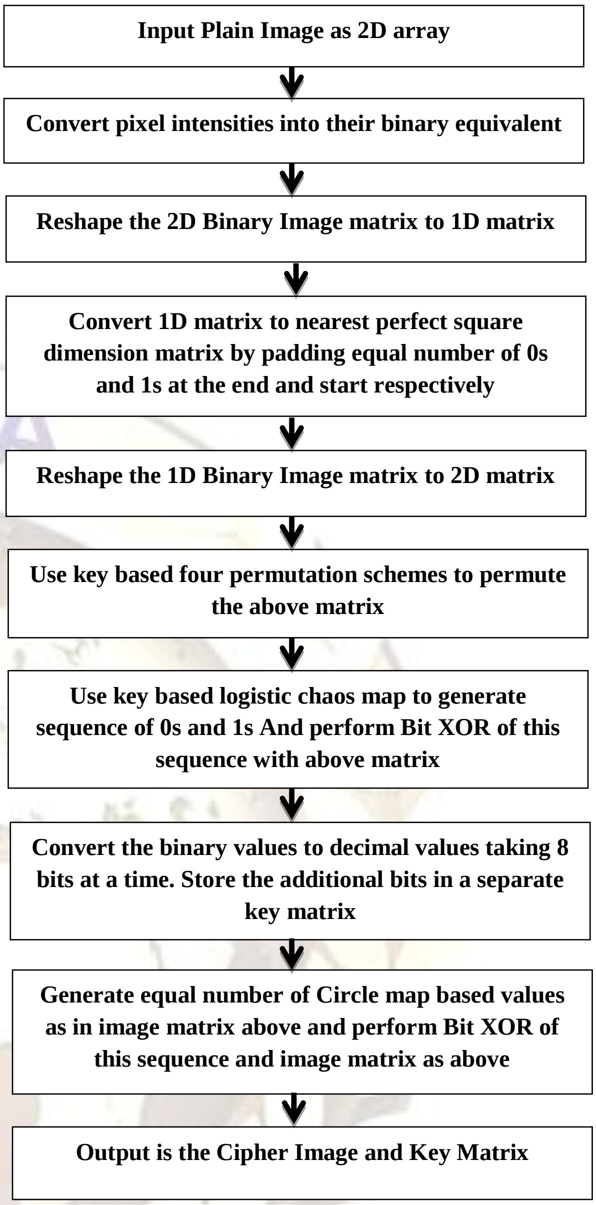
The four permutation schemes on pixels are performed for a certain number of rounds to increase the randomness of the pixels. The experimental results for this scheme proves better results [21] [22] than using Arnold Cat map as permutation tool.

III. Proposed Algorithm

The proposed algorithm uses the four permutation schemes presented earlier on pixel value to operate on bit level for those pixels. The pixel values are converted into binary equivalent and then the schemes are applied. There has been usage of two chaotic maps as well viz., 1D Logistic map and Circle map for the diffusion purpose. The maps are defined in Equation 1 and Equation 2 respectively.

$$X(k+1) = 4x(k)[1-x(k)] \quad \text{Eq. 1}$$

$$x_{n+1} = \mathrm{mod}[\{\sqrt{k_1} + k_2 x_n + \sin(2\pi k_3 x_n)\}, 1] \quad \text{Eq. 2}$$



Input Plain Image as 2D array

Convert pixel intensities into their binary equivalent

Reshape the 2D Binary Image matrix to 1D matrix

Convert 1D matrix to nearest perfect square dimension matrix by padding equal number of 0s and 1s at the end and start respectively

Reshape the 1D Binary Image matrix to 2D matrix

Use key based four permutation schemes to permute the above matrix

Use key based logistic chaos map to generate sequence of 0s and 1s And perform Bit XOR of this sequence with above matrix

Convert the binary values to decimal values taking 8 bits at a time. Store the additional bits in a separate key matrix

Generate equal number of Circle map based values as in image matrix above and perform Bit XOR of this sequence and image matrix as above

Output is the Cipher Image and Key Matrix

Figure 4. The Diagram for illustration of Encryption process for Proposed Scheme

The Encryption process depicted in Fig. 4 can be explained in steps as follows:

Input: Image Matrix

Step 1

Convert the data matrix into bits matrix.

e.g. 2x2 matrix

1 2
3 4

will become 2x16 matrix

00000001 00000010
00000011 00000100

Step 2

Convert the 2D matrix to 1D to make it 1X32 Matrix

00000001 00000010 00000011 00000100

Step 3
Pad it to the nearest square numbers with equal number of 1's and 0's. Nearest square number is 36 so pad the bits accordingly. Equal number of 1's at starting and 0's at end. In case of odd number of bits to be padded, take one 0 bit extra at end
11 00000001 00000010 00000011 00000100 00

Step 4
Create NxN matrix out of it. So it becomes 6x6 matrix of following bits
110000
000100
000010
000000
110000
010000

Step 5
Use key based permutation schemes 1,2,3,4 to shuffle this matrix in step 4 and hence shuffled zeros and ones matrix will be obtained

Step 6
Use key based 1D logistic chaotic map to generate sequence of zeroes and ones up to NxN (36) numbers

Step 7
Perform BitXOR of Step 5 and Step 6 matrix

Step 8
Divide the matrix in step 7 into blocks of 8 bits each and convert them into decimal number. Except the first four numbers, the last number becomes the key matrix for decryption. Key = [a,b,c,..]

Step 9
Generate another sequence of numbers (0-255) using key based Circle chaotic map and perform BitXOR operation with the step 8 data matrix. Key matrix remains intact now and one gets the Encrypted Matrix

Similarly the decryption process is shown in the Fig. 5 and the steps for decryption can be explained as follows:

Input: Cipher Image Matrix, Key Matrix

Step 1
Generate Sequence of Circle chaotic map (0-255) using the initial conditions and perform BitXOR operation on them with cipher image

Step 2
Take the binary equivalent of all the pixels and concatenate the key matrix of 0s and 1s at the end of the matrix obtained

Step 3
Generate sequence of 0s and 1s from Logistic chaotic map

Step 4
Perform BitXOR operation between the sequence of Step 3 with matrix generated in Step 2

Step 5
Apply permutation scheme in reverse order of what applied in Encryption process, 4,3,2,1 to obtain reverse permuted matrix of bits

Step 6
Calculate valid bits and subtract from bits in step 5. Amongst the rest of the bits, extract half of them as ones from starting and half of them as zeroes from end

Step 7
Convert the binary bits to Decimal Numbers and plain text matrix is obtained

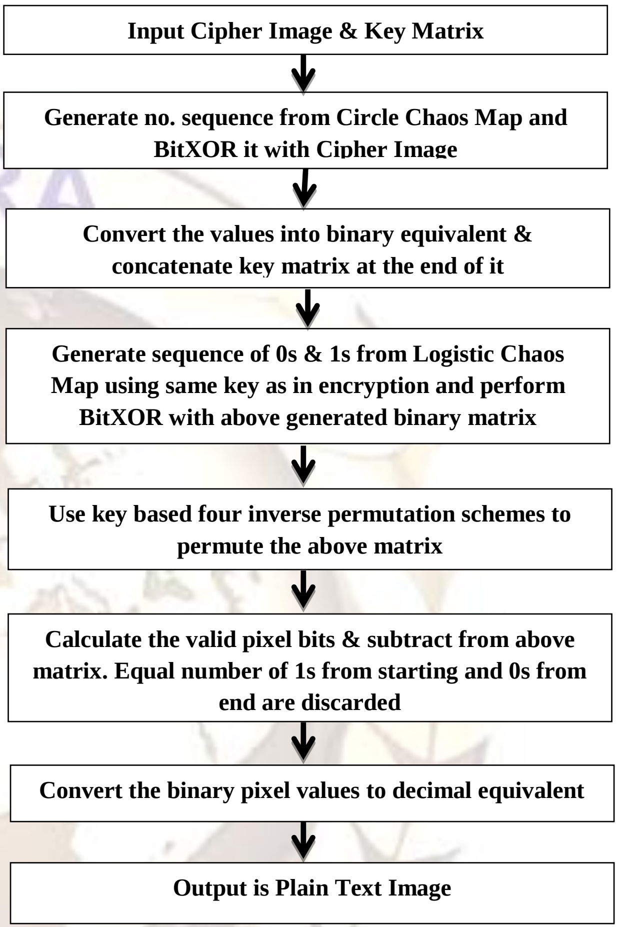

Input Cipher Image & Key Matrix
Generate no. sequence from Circle Chaos Map and BitXOR it with Cipher Image
Convert the values into binary equivalent & concatenate key matrix at the end of it
Generate sequence of 0s & 1s from Logistic Chaos Map using same key as in encryption and perform BitXOR with above generated binary matrix
Use key based four inverse permutation schemes to permute the above matrix
Calculate the valid pixel bits & subtract from above matrix. Equal number of 1s from starting and 0s from end are discarded
Convert the binary pixel values to decimal equivalent
Output is Plain Text Image

Figure 5. The Diagram for illustration of Decryption process for Proposed Scheme

IV. Implementation and Results

The scheme has been implemented in MATLAB 2010a and has been tested on a system with Pentium dual core processor, 1 GB RAM and 80 GB Hard Disk. Two images have been used to test the results – Lena 256x256 in grey scale mode and a pure white Image 256x256 size. The various types of attacks tested are – Visual attack, Statistical attack and Differential Attack. For visual attacks, the encrypted images are provided after various schemes and rounds. For Statistical testing purpose, the histograms are depicted for the cipher and plain text images along with the correlation coefficient for the plaintext and cipher text images. For differential attacks, values of Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI) are reported. The formula for NPCR and UACI are shown with Equations 3 and 4 respectively.

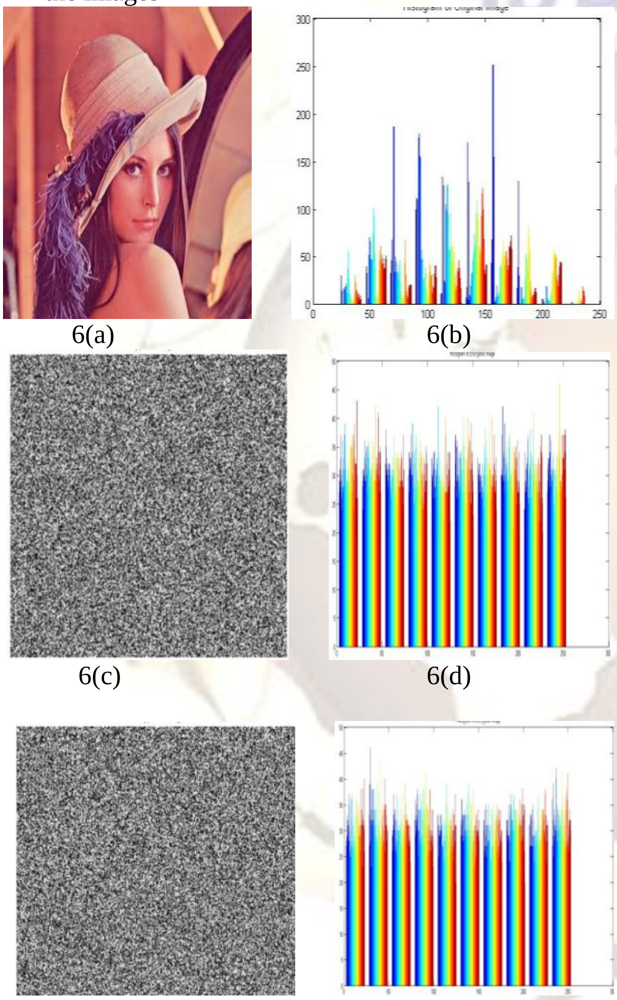
$$\mathbf{NPCR} = \frac{\sum_{i,j} D(i,j)}{M\times N} \times 100\% \qquad \text{Eq. 3}$$

$$\text{where } D(i,j) = \begin{cases} 0, & A(i,j) = AH(i,j) \\ 1, & A(i,j) \neq AH(i,j) \end{cases}$$

$$\mathbf{UACI} = \frac{1}{M\times N}\sum_{i,j}\frac{|A(i,j)-AH(i,j)|}{255} \times 100\%$$

Eq. 4

A and AH are the matrices of the original image and the encrypted image respectively. M is the height by pixels of the image and N is the width by pixels of the images



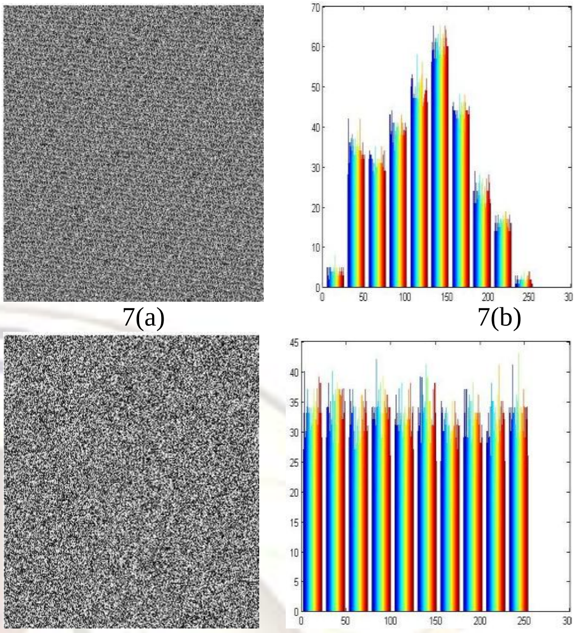
6(a) 6(b)

6(c) 6(d)

6(e) 6(f)

Fig. 6. (a) Original Lena Image used in Grey Scale mode (b) Histogram of Original Lena Image (c) Encrypted Lena Image using Proposed bit level scheme (d) Histogram of Proposed bit level scheme encrypted Lena (e) Encrypted image of pure white image using proposed scheme (f) Histogram of pure white image encrypted using proposed algorithm

The results obtained for Encrypted images and their Histograms from the byte level shuffling and Arnold cat map with PESH are depicted in Fig. 7 (a-d).



7(a) 7(b)

7(c) 7(d)

Fig. 7. (a) Encrypted Lena Image using Arnold and PESH scheme (b) Histogram of Arnold & PESH scheme encrypted Lena (c) Encrypted image of Lena using Byte level new permutation scheme (d) Histogram of Lena using byte level new permutation scheme

The values of the various parameters are shown in Table 1.

Table 1. Values for various parameters on Lena Image

ARNOLD CAT MAP + PESH			
ARNOLD NO OF ROUNDS	CC	NPCR(%)	UACI(%)
2	-0.00470000	99.3622	10.9393
5	-0.00061421	99.3942	10.9379
10	0.00056602	99.4156	10.9306
BYTE LEVEL SHUFFLE SCHEME + PESH			
PERMUTATION NO OF ROUNDS	CC	NPCR(%)	UACI(%)
2	0.00020433	99.6155	13.2847
5	-0.00150000	99.5941	13.2910
10	0.00049334	99.6078	13.2630
PROPOSED BITS SHUFFLE SCHEME			
IMAGE	CC	NPCR(%)	UACI(%)
Lena	-0.000026859	99.5956	13.6480
Pure white	N.A.	99.6033	49.5679

The result shows improvement over the previous algorithms for the proposed schemes. Even visually there were some patterns that could be identified in the images encrypted by Arnold and PESH Scheme while better results were obtained using the algorithm with new permutation scheme. The results were good for bit level processing and the scheme is a better version of byte level processing.

V. CONCLUSION

The proposed scheme is a better variant of the previously proposed schemes. The scheme can be utilized in various Image Encryption Application, Digital Watermarking Applications and Steganography Applications where more security of data is required. Though the scheme works well but has a limitation of excessive computation due to bit level processing. So the current scheme will be better adapted for data involving uncompressed images which are not to be processed on real-time basis. The future work includes the bit level processing on Videos and Audios with work to be extended in transform domain as compared to the spatial domain.

REFERENCES

[1] B. Furht (ed.), *Encyclopedia of Multimedia* Springer, 2005

[2] W. Stallings, *Cryptography & Network Security: Principles and Practice* Third Edition, Pearson Education, 2004

[3] D.R. Stinson, *Cryptography: Theory and Practice* Third Edition, Chapman & Hall, 2005

[4] A.J. Menezes, P.C. van Oorschot and S. Vanstone, *The Handbook of Applied Cryptography* CRC Press, 1996

[5] B. Furht and D. Kirovski, *Multimedia Security Handbook* CRC Press, Boca Raton, USA, 2005

[6] A. Marwa , El-Wahed, S. Mesbah, and A. Shoukry *Efficiency and Security of Some Image Encryption Algorithms, Proceedings of the World Congress on Engineering, Vol I*, 2008

[7] Mitra , Y.V. Subba Rao , and S.R.M. Prasanna, *A new image encryption approach using combinational permutation techniques, International Journal of Computer Science, Vol. 1, No. 2*, pp. 1306-4428, 2006

[8] S.S. Maniccama and N.G. Bourbakisa, *Image and video encryption using SCAN patterns, Pattern Recognition 37*, pp. 725 – 737, 2004

[9] D. Chattopadhyay, M.K. Mandal and D. Nandi , *Symmetric key chaotic image encryption using circle map, Indian Journal of Science and Technology, Vol. 4, No. 5*, pp-593-599, 2011

[10] J. Daemen and V. Rijmen, *The block cipher Rijindael, Proceedings of the Third International Conference on smart card Research and Applications*," *CARDIS'98, Lecture Notes in computer Science, vol.1820, Springer, Berlin*, pp. 277_284, 2000.

[11] J. Daemen and V. Rijmen, *The Design of Rijndael: AES – The Advanced Encryption Standard, Springer-Verlag*, 2002

[12] Federal Information Processing Standards Publications (FIPS 197), *Advanced Encryption Standard (AES)*, 26 Nov. 2001

[13] C. Alexopoulos , N.G. Bourbakis and N. Ioannou, *Image encryption method using a class of fractals, J.Elec. Imaging. 4*, pp. 251-259, 1995

[14] N. Bourbakis and C. Alexopoulos, *Picture data encryption using scan patterns, Pattern Recog. 25*, pp. 567–581, 1992

[15] J.K. Jan and Y.M. Tseng, *On the security of image encryption method," Information Proc. Letts. 60*, pp. 261-265, 1996

[16] P.P. Dang and P.M. Chau, *Image encryption for secure internet multimedia applications, IEEE trans. consumer elec. 46*, pp. 395-403, 2000

[17] H. Cheng and X. Li, *Partial encryption of compressed images and videos, IEEE Trans. Signal proc. 48*, pp. 2439-2451, 2000.

[18] J.C. Yen and J.I. Guo, *A new chaotic key-based design for image encryption decryption, Proc. IEEE Int. Conf. Circuits Systems. 4*, pp. 49-52, 2000

[19] H. Ker-Chang and JL Liu, *A linear quadtree compression scheme for image encryption, Signal Proc, Image Commun. 10*, pp. 279-290, 1997

[20] M. Abu Zaid Osama, A. El-Fishawy Nawal, E. M. Nigm and S. F. Osama, *A Proposed Encryption Scheme based on Henon Chaotic System (PESH) for Image Security, International Journal of Computer Applications (0975 – 8887) Volume 61– No. 5*, January 2013

[21] P. Maggo and R.S. Chhillar, *Lightweight Image Encryption Scheme for Multimedia Security, International Journal of Computer Applications, Vol 71(13)*, pp. 43-48, June 2013. Published by Foundation of Computer Science, New York, USA

[22] R. Gupta, A. Aggarwal & S. K. Pal, *Design and Analysis of New Shuffle Encryption Schemes for Multimedia, Defence Science Journal, Vol. 62, No. 3*, May 2012, pp. 159-166.