Defence Science Journal, Vol. 62, No. 3, May 2012, pp. 159-166, DOI: 10.14429/dsj.62.1008
© 2012, DESIDOC

Design and Analysis of New Shuffle Encryption Schemes for Multimedia

Rajan Gupta[*], Ankur Aggarwal, and Saibal K. Pal[†]

University of Delhi, Delhi–110 007, India
[†]*Scientific Analysis Group, Delhi–110 054, India*
[*]*E-mail: guptarajan2000@gmail.com*

ABSTRACT

Securing the contents of visual data and multimedia requires specific design consideration for use in different applications. The major issue with this type of data has been occurrence of redundancy, at various places particularly in images, which makes data values repetitive at several places. The focus of this paper is on design of new shuffling schemes that can efficiently destroy redundancy in the visual data ensuring its secured transmission and distribution over public networks. Different variants of these shuffling schemes will be used as pre-processing schemes on multimedia data values especially in light weight devices using images. Standard as well as chaotic permutation and substitution schemes together with S-box rotation have been used to shuffle and map the plain data into random uncorrelated values via various variants of the presented schemes. For further improving the security, the processed data is encrypted using a computationally fast algorithm in its normal mode of operation. Security analysis using different types of images show that the proposed schemes satisfy the parameters required for securing visual contents even with very high redundancy.

Keywords: Multimedia security, shuffle, S-box, chaotic encryption, security analysis

1. INTRODUCTION

Cryptography[1,2] has been one of the most significant areas of research and practice for secure transmission and storage of data. It enables the transfer of information in a secured way assuming the presence of adversaries or unauthorized parties between the sender and the receiver. The process of cryptography involves two phases: encryption at the sender's end and decryption at the receiver's end. Encryption involves conversion of plaintext into a scrambled form that does not convey any information regarding the original data. Similarly, decryption involves conversion of cipher text into plaintext data. Generally, the process of encryption uses a scheme that is assumed to be publicly known along with a piece of secret information called the key.

The data to be encrypted can be of varied types - simple textual or numeric data, still images, maps and pictures, audio data including speech and music, video data and multimedia[3]. With increasing number of devices and applications exchanging visual data and multimedia, the need to secure such type of data has increased by many folds. However, the process of encrypting voluminous multimedia is quite different from that of simple textual data. Still images, audio and video data have substantial amount of redundancy (like repetition of data values at several places) that is not destroyed by using traditional encryption schemes which only works for normal data. Schemes like DES, IDEA, and AES[4] in their normal mode of operation are not suitable for encrypting multimedia[5]. Also, the entire audio or visual data is not perceptually significant to the same degree and hence need not be encrypted with the same computation effort particularly for real-time applications.

Block ciphers process the data in blocks and encrypt each block using a secret key shared between the communicating parties. The basic primitives used in block ciphers are mainly based on transposition or permutation of chunks of data and substitution of a sample or set of values by the other. A number of rounds of these operations are used to convert the plaintext into encrypted form without leaving any clues of the original data. A secret key is used in this process and is used to derive sub-keys for each round of operation. All of these operations on a block of data use substantial computational operations which may not be suitable for each sampled value representing the voluminous multimedia. Multimedia encryption schemes[6,7] use similar concepts but try to reduce the computational cost to the maximum possible extent without compromising much on the security. The following primitives are normally used for encrypting multimedia contents which can be compared to confusion-diffusion[8] methods too:

(a) *Transposition Based*: The values/samples of multimedia are mapped to different positions[9] such that the original data gets scrambled up and its spatial structure is lost. This is helpful in changing the position of the data value but doesn't help in changing the data value itself. Different schemes like the Arnold transformation[10,11] and Fibonacci transformation[12] are used for this purpose. Using these transformations, new positions of the data value are calculated which are utilized to scramble the data based on location. A secret key is sometimes used to vary the change in positions to which the data is to be mapped. Though these schemes are computationally light, they often provide limited security and are unsuitable for many

Received 23 May 2011, revised 03 April 2012, online published 3May 2012

present day applications.

(b) *Substitution Based*: The sampled values of multimedia data are substituted by some other permitted values but keeping their original positions intact. This helps in changing the data values but their positions remain unchanged. Since only value changes and not the position, a function or lookup table is normally used. Many standard schemes like the DES and AES use substitution boxes or S-box[13] for this purpose. Design of substitution boxes is an important aspect of the strength of block ciphers.

(c) *Transposition-substitution Based*: The values are trans-positioned as well as substituted with some other permissible value. This gives a fair amount of security as both the schemes are being involved within a round of operation. SCAN patterns[14] is one of the schemes based on this category in which the data values are modified with respect to their positions in various ways of scanning a data matrix and subsequently by substituting with different values.

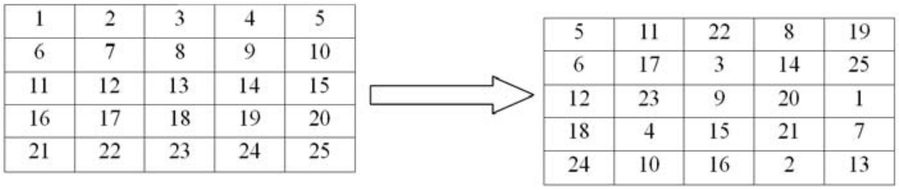
(d) *Chaos Based*: The chaotic properties of certain functions are being utilized in encrypting the data. Various chaotic maps[15] like Tent, Logistic etc. are used to generate values which ultimately help in either scrambling the data or substituting with different values. Chaos based encryption schemes[16,17] have been one of the active research areas as these ensure adequate security at low computational costs.

All these primitives have been successfully used in the design of Multimedia encryption schemes. Since many present day devices using multimedia applications have reduced in size, the need for any image encryption scheme for this purpose has shifted from being more secure to more computationally efficient and lightweight. There has been a surge of lightweight devices like mobile phones, PDAs, tablet PCs and various handheld devices that don't have memory comparable to desktop computers. So any scheme must be efficient in terms of its memory utilization and the computational overhead required for the encryption process. Traditional block encryption schemes in their safer modes of operation have not been computationally efficient for these lightweight devices. On the other hand, by carefully using cryptographic primitives it is possible to design secure as well as efficient multimedia encryption schemes[18] suitable for present day applications.

Designing the various shuffling schemes, our focus is on removing the redundancy in the visual data using minimal computations by processing the image prior to application of the actual encryption algorithms. These shuffling schemes distributes the image data more uniformly, which had some clusters of similar values in particular areas earlier, resulting in a flatter histogram thereby reducing the computational efforts required by the encryption scheme. The shuffled data is now more uniform and very less repetitive. The need for preprocessing also arises in case of images or video frames having white or black background or chunks of almost single colour image regions. Preprocessing helps in destroying the redundant data so that any traditional lightweight encryption scheme works equally well as it does on normal data. This shuffle spreads out the data uniformly and most of the similar values are mapped on to different values in the shuffled data.

2. EW SHUFFLE SCHEMES

Based on the characteristics of existing primitives, four new shuffle schemes are reported in this section. These schemes employ a unique method of permutation of data that is similar for all the shuffle schemes while the substitution process is different with special consideration for computational load and the level of security required for different applications. Permutation of data can be described by working out on the data table given in Fig. 1.



1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25

5	11	22	8	19
6	17	3	14	25
12	23	9	20	1
18	4	15	21	7
24	10	16	2	13

Figure 1. Depicting a 5X5 data matrix before and after applying New Permutation Scheme.

In the above data table, start with initial position of row and column and apply our permutation algorithm on the data.

- The positions are scanned in a new data table, which is empty initially, and its locations will be searched and filled with data from the original data matrix. The data from original matrix is read linearly in row major order starting from 1, 2, 3, and so on till value 25.
- Initially row position value and column position value are 1 each for new data table. The starting positions can be decided as per the value derived from some key to be used later.
- The row value position is incremented by 2 and column position value is decremented by 1 and the new position is being checked.
    - ♦ If the location is empty, the position is filled with data value from original matrix else we increment column position by 1 and decrement row position by 1 to get the new position, which has to be empty. This algorithm ensures that no collision occurs among various positions and has been developed using the concept of standard magic squares[19].
    - ♦ The boundary conditions are kept in mind with respect to the maximum row and maximum column value of a data table.
        - ▪ If row position value reaches the maximum row value, it is reset to the first row position.
        - ▪ If column position reaches zero, it is reset to maximum column position.
- This process goes on until the original data table is scanned completely and is scrambled with their new positions.
- Example: In the above data table, take data value at first position on original matrix and put it at new position after considering initial row and column position value as 1

each. So incrementing 1 by 2, gives us 3 and decrementing 1 gives us 0, so we set it to maximum column value, i.e. 5. Therefore, the position to place 1 is in third row and fifth column in the new data table. From there again row position is incremented by 2 and column is decremented by 1. In case of already filled position like that after filling value 5 at first row and first column, we increment rows by 2 and decrementing column by 1 taking us to third row and fifth column which is already filled by value 1. So we again increment the column position by 1 and decrement the row position by 1 to get to new position of second row and first column where value 6 is being placed.

The permutation technique in conjunction of different type of substitution techniques are used for the new shuffle schemes. The different schemes are as follows:

Scheme 1 : Start position value of row and column, S-box rotation

Step 1 : Permutation of data table with above described scheme.
Step 2 : Element of permuted data table are XORed with another element at same position in S-box table.
Step 3 : S-box rotation with key[20].
Step 4 : Rotated S-box is used for final substitution of table obtained after Step 2.

The scheme applies permutation on the data matrix and the standard S-box of AES is used. Similar position elements are being XORed and placed in the data matrix. The normal S-box is rotated which is then used to substitute the values of data matrix that are stored after applying XOR function.

Scheme 2 : Start position of row and column, S-box generation

Step 1 : Permutation of data table with above described scheme.
Step 2 : Data retrieved in row major order and XORed with data table's position value considered as a single data table scanned linearly.
Step 3 : Repeat *Step 1*.
Step 4 : S-box generation[21] with the help of key.
Step 5 : Standard substitution with S-box.

After permutation of the data matrix, the row major order scanning is done and XOR function is applied on it with the data table's positions value. Again, a round of permutation is applied with different starting position. Then S-box is generated with the help of key and this helps in substitution of the normal data matrix values.

Scheme 3 : start position of row and column, number of rounds

Step 1 : Permutation of data table with above described scheme.
Step 2 : Data values are XORed with data table's position values.
Step 3 : Repeat *Step 1*.
Step 4 : Standard substitution of data table obtained in *Step 3* using S-box table.
Step 5 : The above steps are performed for a specific number of rounds, e.g. 3, 5, 10, etc.

This scheme applies permutation of the data which is XORed with data table's position value. Again, permutation of data matrix is being applied and standard substitution with S-box is carried out. The steps are repeated for a particular number of times which may be 3, 5, 10, etc.

Scheme 4 : Start position of row and column, control parameters of chaotic map

Step 1 : Permutation of data table with above described scheme.
Step 2 : S-box generation[21] with chaotic map.
Step 3 : Standard substitution with generated S-box.

In this scheme, after permuting the data matrix, S-box is generated with the help of chaotic map using control parameters which are extracted from key. Then this generated S-box is used for the standard substitution process.

3. MAIN ENCRYPTION SCHEME

The major block algorithms for encryption are advanced encryption scheme (AES)[4] and Tompkins Paige algorithm[22]. These two algorithms are shown in Figs 2, 3, and 4. The AES algorithm used in the electronic code book (ECB) mode of encryption may leak out the redundancy of the plaintext in the cipher as same plaintext blocks are encrypted to same ciphertext blocks for the same key. The AES scheme Rijndael[4] is based

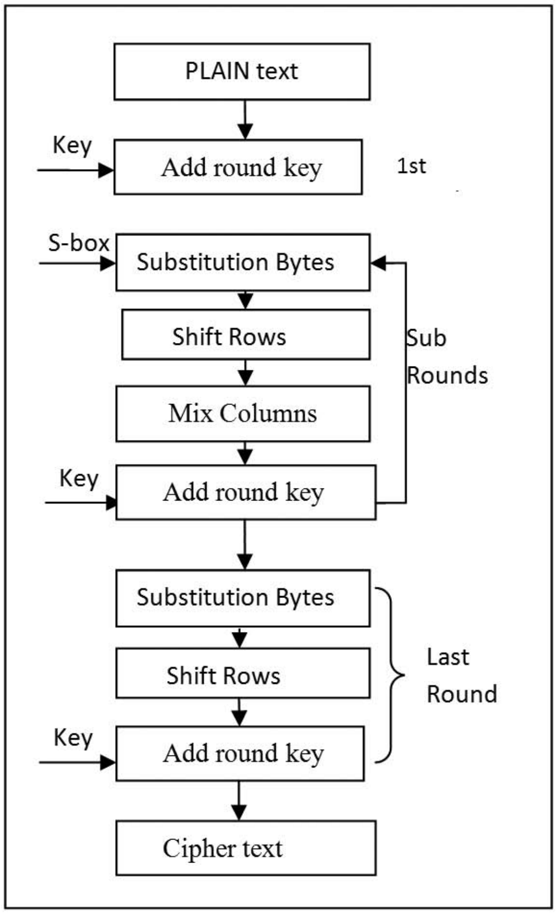


Figure 2. Operations used in the advanced encryption scheme.

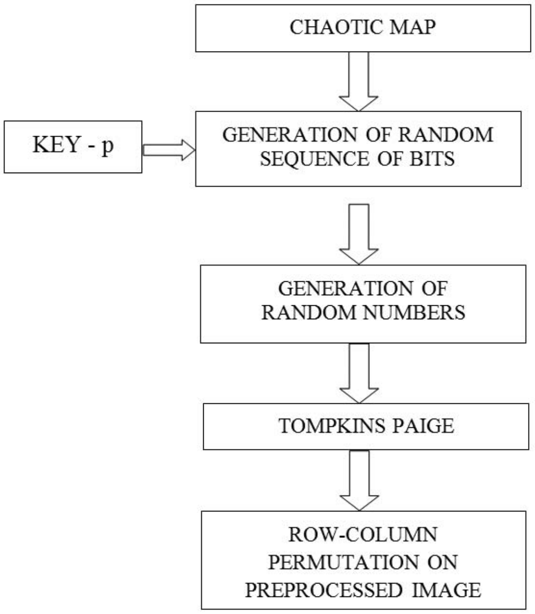

CHAOTIC MAP
KEY - p
GENERATION OF RANDOM SEQUENCE OF BITS
GENERATION OF RANDOM NUMBERS
TOMPKINS PAIGE
ROW-COLUMN PERMUTATION ON PREPROCESSED IMAGE

Figure 3. Chaotic Permutation.

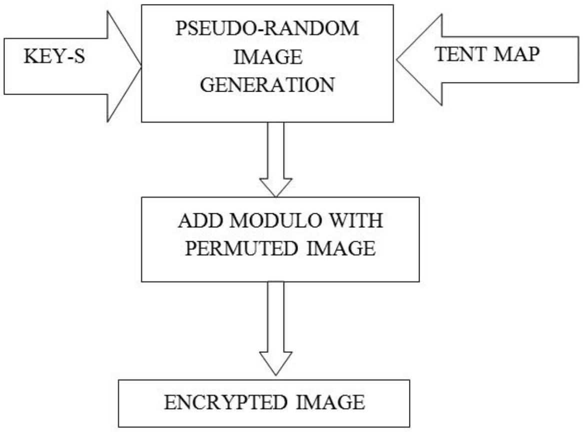

KEY-S
PSEUDO-RANDOM IMAGE GENERATION
TENT MAP
ADD MODULO WITH PERMUTED IMAGE
ENCRYPTED IMAGE

Figure 4. Chaotic substitution.

on transposition-substitution scheme with multiple rounds and subkey generation for each round. It uses a block of size 128 bits while key size can be of 128,192, or 256 bits.

The process and operations used in AES are depicted in Fig. 2 which is a phased process. In the first phase, key expansion takes place in which round keys are generated from the main secret key. The initial round of Add round key takes place where each byte of the state is XORed with the round key obtained in expansion phase. Then the next phase begins where four operations are performed. These are Substitution Bytes, Shift Rows, Mix Columns and Add Round Key. Sub Bytes is actually a simple substitution which is non-linear in nature and is realized with the help of a simple look up table. Shift Rows shifts the rows in a cyclic manner for certain number of rounds. Mix column is an operation combining the 4 bytes in each column. Last phase is similar to third phase except the fact that mix column is not performed in this phase. In the ECB mode of operation, the message is divided into different blocks and each one is encrypted separately independent of the other. The ECB mode is the cheapest in terms of computational efforts but is not secure particularly when handling multimedia.

Tompkins Paige algorithm is another block cipher algorithm which is based on chaotic maps and is suitable for multimedia. It involves two phase namely chaotic permutation and chaotic substitution.

The newly designed shuffle schemes can be used effectively with the above mentioned cipher block schemes. These new shuffling schemes are used as pre-processing technique which evenly distributes the data value in the image data matrix/table. The usage of the shuffle schemes are not carried out independently on the data unless security concerns are not the priority. Experiments were conducted on different types of images. Some of the images reported in this paper are the standard 256X256 gray scale images of Lena and Baboon as shown in Figs. 5 and 6. The images were obtained without any data loss after the process of decryption so not depicted in the figures separately. The pure white image was also used to the study the effect of shuffling on highly redundant data matrix having maximum repetitive data values. The encrypted images and their histograms are shown in following figures.

Figure 5. Lena image.

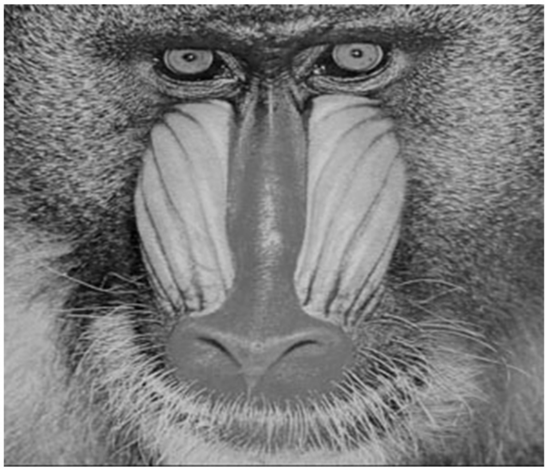


Figure 6. Baboon image.

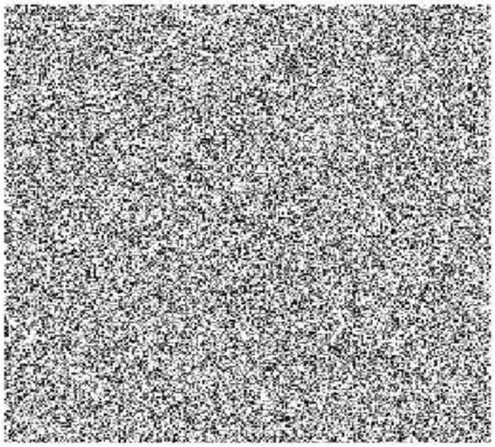


Figure 7. Encrypted lena image.

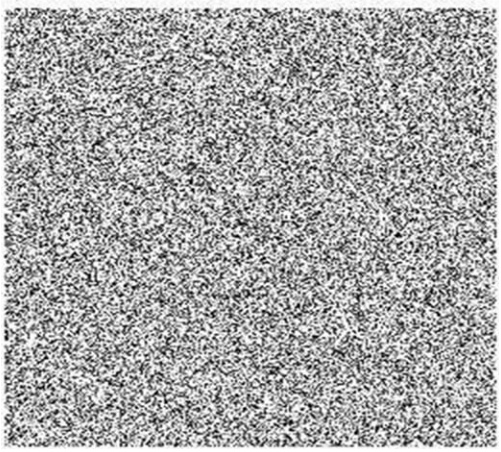


Figure 8. Encrypted baboon image.

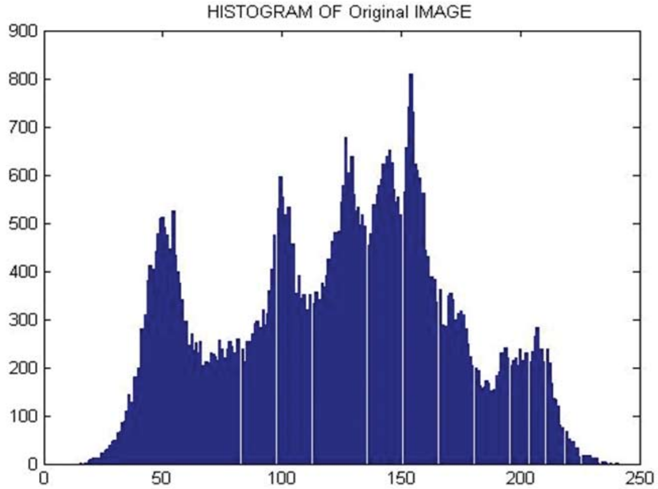


Figure 9. Histogram of original lena.

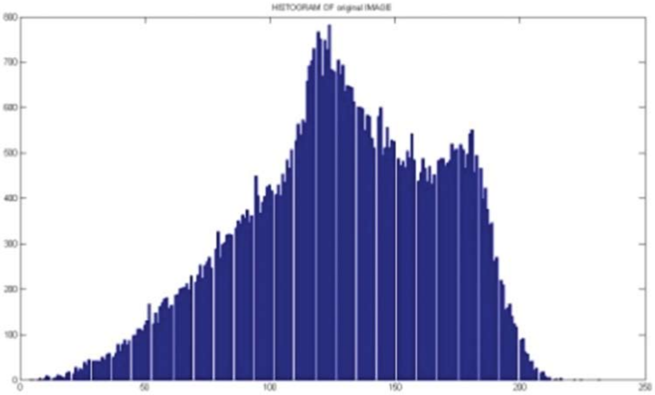


Figure 10. Histogram of original Baboon.

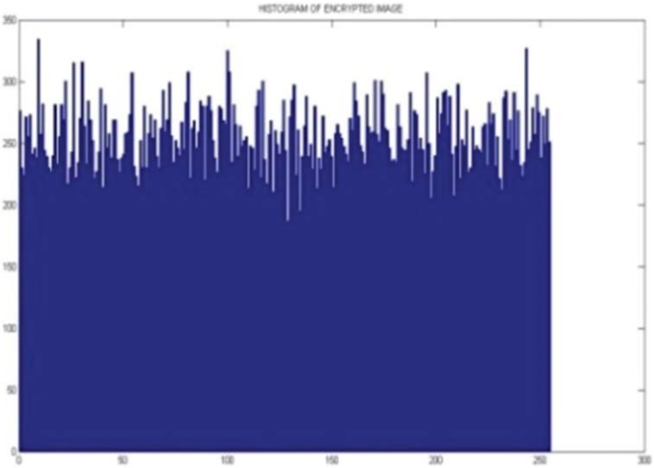


Figure 11. Histogram of encrypted lena.

Figures 5 and 6 shows the gray scale images of Lena and Baboon used to demonstrate the strength of our schemes. High quality coloured versions of these images have also been used by extending the schemes for shuffling and encrypting the RGB planes independently. Figures 7 and 8 show the encrypted images of Lena and Baboon respectively. The scheme followed for both these images has been the fourth shuffle algorithm mentioned earlier and then the block cipher AES in ECB mode. Histograms of original images of Lena and Baboon are shown in Figs 9 and 10 and those of encrypted ones are shown in Figs 11 and 12. Figure 13 represents the histogram of pure white image after application of the fourth shuffle scheme only and Figure 14 represent histogram of pure white image in conjunction with Tompkins Paige block cipher scheme. Various combinations of shuffle and encryption may be applied for securing the contents of images or multimedia. Any of the four mentioned shuffle schemes can be used with any of the valid block cipher schemes.

4. SECURITY ANALYSIS

The encrypted images shown in the previous section depicts the visual aspect of the algorithmic strength. Flatness of the histogram irrespective of the type of image also proves the effectiveness of the shuffle schemes. However, there are few other parameters[23, 24] used to determine the actual security strengths in the proposed scheme. With the help of the value of these parameters, one can easily analyze for the weakness of the schemes. The purpose of the encryption algorithms is to provide additional security against cryptanalytic attacks. The various parameters used to quantify the strength of the schemes are mentioned below:

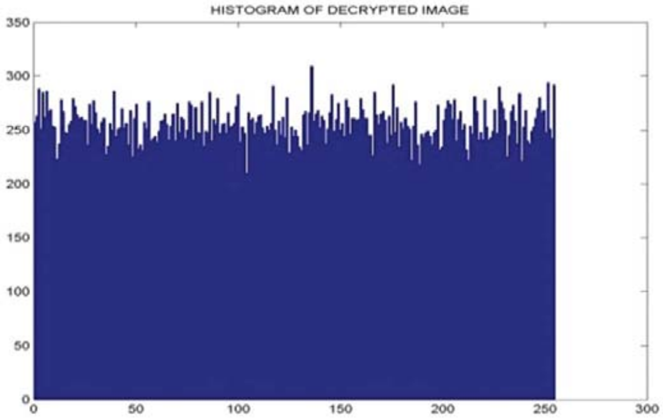


Figure 12. Histogram of encrypted baboon.

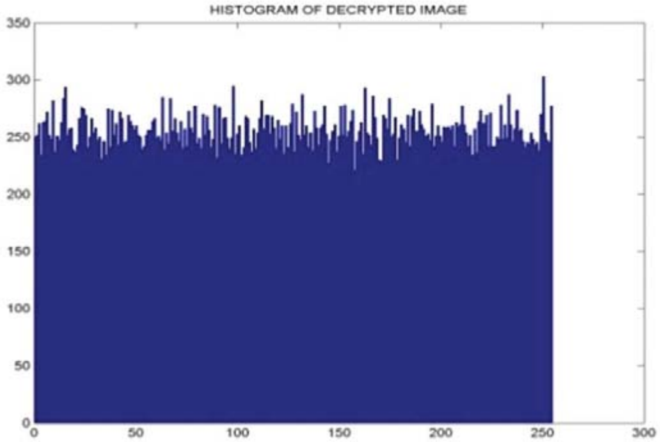


Figure 13. Histogram of pure white image.

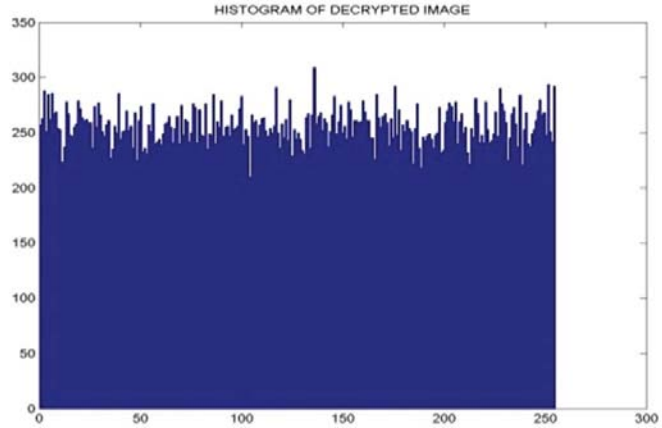


Figure 14. Histogram of pure white image.

4.1 Differential Attack Parameters

With the help of these attacks, the attacker tries to identify the pattern in the encryption scheme by changing just one pixel value in the plain image and applying the scheme on it. The new cipher image is compared to the original cipher image without pixel change. This change actually determines the strength of the algorithm. There are two variables, number of pixel change rate (NPCR) and unified average change intensity (UACI)[25] which are checked for their values. They are:

(i) Number of pixel change rate - It can be calculated using

$$NPCR = \frac{1}{W*H}\sum_{i,j} D(i,j) \tag{1}$$

(ii) Unified average change intensity - It can be calculated using

$$UACI = \frac{1}{W*H}\left[\sum_{i,j}\frac{C_1(i,j)-C_2(i,j)}{255}\right] \tag{2}$$

here, C_1, C_2 are two ciphered images of same size whose corresponding original images differ by only one pixel; $C_1(i, j)$, $C_2(i, j)$ determines grey scale values of the pixel at grid (i, j); $D(i, j)$ is determined by $C(i, j)$; W and H are the column and rows of the image.

4.2 Encryption Quality

It is expressed as the change or deviation caused in pixel value at every location. It can be calculated with the following steps:

(i) $X = |I - E|$

(ii) $H = \text{histogram}(X)$

(iii) $D = \frac{1}{256}\sum_{i=0}^{255} h_i$

(iv) $S(i) = |H(i) - D|$

(v) $AS = \sum_{i=0}^{255} D(i)|$

where I is the plain image, E the encrypted image, H denotes the histogram distribution and h_i represent the amplitude of the absolute difference histogram at the value i. The area covered under AS determines the Encryption Quality. Generally lower the area better is the image encryption quality.

4.3 Correlation Coefficient

Statistical analysis such as correlation coefficient factor is used to measure the relationship between two variables; the image and its encrypted counterpart. This factor demonstrates to what extent the proposed encryption algorithm strongly resists statistical attacks. Therefore, encrypted image must be completely different from the original one. Value closer to 1 means that there is a lot similarity between the two values. Ideally the value should be close to zero. It is calculated using the following formulae

$$C.C. = \sum_{i=1}^{N}\frac{(x_i-E(x))(y_i-E(y))}{\sqrt{\sum_{i=1}^{N}(x_i-E(x))}\sqrt{\sum_{i=1}^{N}(y_i-E(y))}} \tag{3}$$

4.4 Entropy

It used to calculate the effectiveness of the image encryption algorithm. Higher the entropy of the encrypted image, more randomized and unpredictable the values indicating stronger encryption.

Table 1 shown below depicts the readings of the above discussed parameters calculated by the schemes mentioned in previous sections for pure white image and Lena image.

In the Table 1, AES_ECB signifies AES algorithm used in ECB mode and Tompkins signifies the Tompkins Paige algorithm discussed earlier in the paper. S1, S2, S3 and S4 represent the first, second, third, and fourth shuffle schemes respectively, described earlier in the paper and are used in

Table 1. Security analysis parameter values for the proposed schemes

Schemes	Image	NPCR	UACI	Encryption quality	Correlation	Entropy
AES_ECB No Shuffle Scheme	Lena	0.3152	0.1020	42377	-0.0075	0.8966
	White	0.3859	0.1892	122880	-	0.0019
AES_ECB_S1	Lena	0.3216	0.2112	42200	-0.0063	0.9968
	White	0.4027	0.2126	75421	-	0.0374
AES_ECB_S2	Lena	0.4021	0.1576	42336	-0.0030	0.9378
	White	0.4201	0.2012	78111	-	0.0445
AES_ECB_S3	Lena	0.4120	0.2010	32903	0.0036	0.9970
	White	0.4112	0.2026	75941	-	0.0482
AES_ECB_S4	Lena	0.3921	0.1220	32592	-0.0052	0.9761
	White	0.4221	0.1921	79470	-	0.0920
TOMPSKIN No Shuffle Scheme	Lena	0.3105	0.0910	42524	0.0099	0.0372
	White	0.3845	0.1330	37942	-	0.0361
TOMPSKIN_S1	Lena	0.3998	0.1120	42187	-0.0046	0.0376
	White	0.4135	0.1494	34112	-	0.0370
TOMPSKIN_S2	Lena	0.3860	0.1571	42509	0.0007	0.0372
	White	0.3922	0.1546	34161	-	0.0387
TOMPSKIN_S3	Lena	0.3865	0.0920	42301	0.0004	0.0395
	White	0.4012	0.1321	34244	-	0.0384
TOMPSKIN_S4	Lena	0.3602	0.1091	41192	0.0093	0.0377
	White	0.4216	0.2012	33971	-	0.0382

combination with either AES or Tompkins algorithm.

The results depicted in the Table 1 suggests improvements in the basic encryption schemes used along with new shuffle scheme rather than used individually on images. The increasing values of NPCR and UACI, with introduction of new shuffle schemes, suggest improvement in the quality of the encryption process. Higher values of NPCR and UACI indicate improvements in image encryption. Similarly, lower area under encryption quality curve shows betterment of the schemes. Without introduction of Shuffle schemes, the area values are much higher than after introduction of new shuffle schemes. Also the correlation coefficient is desirable to be close to zero for a better quality which can be seen in the values clearly. The higher entropy values also indicate better quality. The execution speed of each shuffle scheme was found very small as compared to traditional algorithms.

5. CONCLUSIONS

Designing efficient and secure encryption schemes for multimedia has always been a challenging activity. Destruction of redundancy available in plain visual images at low computational costs was one of the main objectives addressed in the paper. Experimental results show that the shuffle scheme helps to remove the redundancy normally found in digital images and produce a flat histogram not normally possible with traditional data encryption schemes. Even a pure white/black image (with high redundancy) can be encrypted efficiently without any leakage of information in its cipher. The scheme can be used in conjunction with a computationally simpler encryption scheme to provide security to digital media. Therefore, the amount of computations and the number of rounds used for normal encryption of data may be reduced here as per the security requirements of the application. For securing voluminous visual data with requirements of real-time communication and use in resource constrained applications such schemes would be in demand in the future as well.

REFERENCES

1. Stinson, D.R. Cryptography: Theory and practice. Ed 3rd , **1**, Chapman & Hall, 2005.
2. Menezes, A.J.; Oorschot P.C.van & Vanstone, S. The handbook of applied cryptography, CRC Press, 1997.
3. Multimedia Design. Encyclopedia of multimedia. Edited by B. Furht. Springer, Berlin, 2006. pp. 834-43.
4. Advanced Encryption Standard. Stallings, W. Cryptography and network security: Principles and practices. Ed 4th, Pearson Education, 2004. pp. 135-173.
5. Agrawal, P. & Rajpoot, M. Partial Encryption Algorithm for Secure transmission of Multimedia messages. *Int. J. Comp. Sci.,* 2012, **3**(1), . 467-70.
6. Complete Encryption. Lian, S. Multimedia content encryption – Techniques and applications. CRC Press, Taylor & Francis Group, 2009. pp. 21-42.
7. Lian, S. & Zhang, Y. Handbook of research on secure multimedia distribution. Information Science Reference, IGI Global, 2009.

8. Ahmed, F. & Resch C.L. Characterizing cryptographic primitives for lightweight digital image encryption. *In* the Proceeding of Mobile Multimedia/Image Processing, Security, and Applications. SPIE 7351, 73510G, 2009, pp. 10G 1-11
9. Mitra, Y.V.; Rao, S.R. & Prasanna, S.R.M. A new image encryption approach using combinational permutation techniques. *Int. J. Comp. Sci.,* 2006, **1**(2), 127-31.
10. Li, B. & Xu, J. Period of Arnold Transformation & its application in image Scrambling, *J. Central South Univ. Technol.*, 2005, **12**(1), 278-82.
11. Ma, X.; Fu, C.; Lei, W. & Li, S. A novel chaos based image encryption scheme with an improved permutation process. Int. J. Advancements in Computing Technol., 2011, **3**(5), pp. 223-33.
12. Zou, J.; Ward, R.K. & Qi, D. The generalized fibonacci transform & application to image scrambling. *In* Proceedings of the ICASSP, 2004, pp. III-385-88.
13. Nedjah, N. & Mourelle, M.L. Designing substitution boxes for secure cipher. *Int. J. Innovative Computing Appl.*, 2007, **1**(1), 86-91.
14. Shahid, Z.; Chaumont, M. & Puech, W. Selective and scalable encryption of enhancement layers for dyadic scalable H.264/AVC by scrambling of scan patterns. *In* the Proceedings of the ICIP, Cairo, Egypt, 2009, pp.1273-276.
15. Fridrich, J. Image encryption based on chaotic map. *In* the Proceedings of the IEEE International Conference on System, Man and Cybernetics, Orlando, Florida, 1997, **2**, 1105-110.
16. Yang, T.; Wu, C.W. & Chua, L.O. Cryptography based on chaotic systems. *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, 2001, 44(5), 1997, pp. 469-72.
17. Nien, H.H.; Changchien, S.K.; Wu, S.Y. & Huang, C.K. A new pixel-chaotic-shuffle method for image encryption. *In* the Proceedings of the International Conference on Control, Automation, Robotics and Vision, Hanoi, 2008, pp. 883-87.
18. El-Wahed, M.A.; Mesbah, S. & Shoukry, A. Efficiency and security of some image encryption algorithms. *In* the Proceedings of the World Congress on Engineering, 2008, **I**, London, U.K.
19. Wikipedia, Magic Square, http://en.wikipedia.org/wiki/Magic_square [Accessed on 10 July 2010].
20. Kazlaukas, K. & Kazlaukas, J. Key-dependent S-box generation in AES block cipher system. *Informatika*, 2009, **20**(1), pp. 23-34.
21. Krishnamurthy, G.N. & Ramaswamy, V. Making AES stronger: AES with key dependent S-box. *Int. J. Comp. Sci. Network Secu.*, 2008, **8**(9), pp. 388-98.
22. Borujeni, S.E. & Eshghi, M. Chaotic image encryption design using TOMPKINS-PAIGE algorithm. *In* Mathematical Problems in Engineering. Hindwai Publishing Corporation, Online journal , 2009. pp. 1-22.
23. Standaert, F.X.; Piret, G. & Quasiquater, J.J. Cryptanalysis of block ciphers: A survey. UCL Crypto Group Technical Report Series, Technical Report No. CG-2003/2. http://www.dice.ucl.ac.be/crypto/, [Accessed on 21 August 2011].
24. Furht, B. & Kirovski, D. Multimedia security handbook. CRC Press, Boca Raton, USA, 2005.
25. Wu, Y. & Noonan, JP. NPCR and UACI Randomness Tests for Image Encryption. *J. Sel. Areas Telecommumn.*, 2011, 31-38.

Contributors

Mr Rajan Gupta completed his post-graduation studies in Computer Science from University of Delhi in 2011 and post-graduate program in Management from IMT, Ghaziabad and is presently pursuing his PhD. He is currently associated with University of Delhi as a Guest Faculty. His area of interest includes: cryptography, multimedia and operating system in technical area and marketing research in management area. He has over 10 research publications under his name in different areas of Technology and Management Studies.

Mr Ankur Aggarwal completed his post-graduation studies in Computer Science from University of Delhi in 2011. He is presently working with ONE97 Company. His area of interest includes: Cryptography, multimedia and mobile services. He has presented his work at both national and international forums and has 2 publications under his name in Multimedia area.

Mr Saibal K. Pal completed his post-graduation studies in Computer Science from University of Allahabad in 1990 and PhD (Information Security) from University of Delhi. He is presently working as Scientist ‘F’ at Scientific Analysis Group, Delhi. His areas of interest include: Cryptography & network security, multimedia & signal processing, computational intelligence & data mining. He has over 100 research publications in different areas of science, technology & management studies.