Lightweight Image Encryption Scheme for Multimedia Security

Payal Maggo
M-Tech Scholar
Department of Computer Science and Applications,
M. D. University, Rohtak, Haryana-124001, India

Rajender Singh Chhillar,Ph.D
Head
Department of Computer Science and Applications,
M.D. University, Rohtak, Haryana-124001, India

ABSTRACT
Due to abundant growth of multimedia application it becomes necessary to secure multimedia data. The scope of this paper is confined to secure multimedia data especially images. The major issue that exists in images is the presence of redundant data. The main focus of this paper is to design a new shuffling scheme that can eliminate redundant data .The new shuffling scheme has been implemented on different images. In this paper comparative analysis is done before and after applying new shuffling scheme with the existing PESH algorithm. The shuffling schemes are applied on pure white images in order to test its efficiency, as white images have maximum redundant data. The new scheme is designed for the light weight devices which require less computation power.

Keywords
Multimedia Security, Image Security Algorithms, Multimedia Security Analysis, Image Encryption

1. INTRODUCTION
In today's world, transferring multimedia data through communication networks requires the transmission in secured manner. With increase in application exchanging digital images over network, securing such images has become an important concern. Multimedia security aims at protecting the media from distortion by various attackers while it is being sent over communication network. A digital image is formed of group of pixels having intensities in the range of (0-255) for 8-bit values and is interpreted as a two dimensional array [1] [2] for gray scale plain. The most common scheme used among all to secure multimedia images is Encryption, which is a technique to protect the original image from unauthorized access, quality of Encryption is tested if

- It can withstand various attacks like plaintext attack, cipher-text attack, brute-force attack, statistical attack and differential attack [1] [2].
- By measuring correlation coefficient between original and encrypted image ,by Measuring execution time, by analyzing histogram, by observing the values of NPCR (Number of pixel change rate) and UACI (Unified average change intensity) and the likes [1][2][3].

We broadly classify cryptography as symmetric key cryptography and asymmetric key cryptography. Multimedia security relies on symmetric key cryptography along with fast block cipher algorithms, where same key is used for encryption and decryption process. Traditional encryption schemes like Advanced Encryption Standard (AES) and Data Encryption Standard (DES) individually are not suitable for securing multimedia images due to its inherent characteristics such as high redundancy as a result of correlation of pixels values, bulky size of images which requires them to be compressed before storage and transmission [2] [3] [4].These traditional schemes are used directly for textual data .Though AES a block cipher algorithm provide high security but it take much time for encryption and decryption process due to large number of rounds involved in it. There are various schemes that have been designed for securing digital images which are based on-

i. Transposition Based Scheme – In this scheme pixel values are shuffled by changing their position. It comprises of bit permutation, pixel permutation or block permutation [1] [2] [3].
ii. Substitution Based Scheme – In this scheme data values in original image are diffused or replaced with some other value taken from lookup table, S-box [1][2][3]. Here positions of pixels are unaltered.
iii. Transposition-Substitution Based Scheme- In this scheme both position and data values are altered by applying both transposition and substitution scheme [1] [2] [3].
iv. Chaos Based Scheme – In this scheme chaotic maps or functions are used to change the positions and to substitute with different data values [2] [3] [5].

These schemes individually ensure less security and are weak schemes. Various Chaos based encryption technique are proposed and designed which are more efficient, provide high security, high speed, less complexity and less computational overhead [2] [5] [6]. These features make chaos based encryption techniques suitable for light weight devices like mobile phones and various hand held devices, as they require limited bandwidth, limited storage memory, fast processing taking in to consideration computational cost and time constraints.[2][3][4].

This paper focuses on existing scheme or algorithm based on Henon chaotic system(PESH) of securing digital images .In this scheme firstly Arnold Cat map or Bakers chaotic map is used to shuffle the positions of the original image then PESH algorithm is applied in order to encrypt the image. This paper aims at removing redundancy in digital image and hence proposed a new shuffling scheme in place of Arnold cat map to be applied with existing PESH algorithm. This proposed scheme is tested using various analysis tools and its results are also observed over white images to ensure its efficiency.

This paper is organized as follows section2 will describe the existing PESH algorithm. Section 3 describes new proposed shuffling scheme to be applied with existing PESH algorithm. Section 4 presents the comparative results of both existing and proposed scheme. Section 5 concludes the paper.

2. A EXISTING ENCRYPTION SCHEME BASED ON HENON CHAOTIC SYSTEM (PESH)

In the existing scheme PESH, **firstly** confusion Algorithm is applied over plain image which will shuffled the position of the pixels in plain image. The permutation technique used is based on Arnold Cat Map [2] [5] which is described as:-

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = A \begin{bmatrix} X \\ Y \end{bmatrix} \bmod N$$

$$= \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} \bmod N \qquad 1$$

The equation so obtained which will help changing the position of pixel is:-

$$X' = \bmod \left((X + (p \times Y)), N \right) \qquad 2$$

$$Y' = \bmod \left(((q \times X) + (Y \times p \times q) + Y), N \right) \qquad 3$$

Where p and q are positive integers, (x', y') is the new position of the pixel and (x, y) is the original position of the pixel. In order to get a shuffled image, Arnold cat map is applied ten times so that correlation among adjacent pixels is disturbed completely. Arnold cat map is easy to compute as it consist of a linear transformation and a mod function and hence can change the position of pixels more efficiently. The major problem of using Arnold cat map is that it is more prone to attacks for which it is applied for number of iterations.

Secondly the shuffled image so obtained is passed through diffusion process. The diffusion algorithm used is PESH which will change the data values of pixel and generate the ciphered image [6]. PESH algorithm is applied with four modes of encryption operation- ECB (Electronic Code Book) mode, CBC (Cipher Block Chaining) mode, OFB (the Output Feed Back) mode and CFB (Ciphering Feed Back) mode [7].

PESH algorithm used for encryption in existing system is described as [6] - firstly The Henon Chaotic system is converted to one dimensional map using

$$X_{i+2} = 1 - a(X_{i+1})^2 n + b\, X_i \qquad 4$$

Where a =0.3, b= 1.4(belongs to 1.07-1.4), x_0=0.01, x_1=0.02 given as a key. After this transform matrix (TM) is created using a quadratic function-

$$F(X_i) = X_i \times (2X_I + 1) \qquad 5$$

Transform matrix so obtained with the above equation is a one dimension matrix of size M*N where M is the width of the image and N is the height of the image. Next a two dimensional matrix (W) will be created of size M*N using transform matrix and the shuffled image, where M is the width and N is the height of the image.

$$W(I, J) = IM(I, J) + 2 \times TM(c) \times TM(c) \qquad 6$$

Where $i = 1, \ldots, m$ $j = 1, \ldots \ldots, n$ and $c = 1,2, \ldots \ldots m \times n$

The cipher image (IME) is formed by applying exclusive OR operation bit by bit

$$IME(I, J) = IM(I, J) \oplus W(I, J) \qquad 7$$

The existing encryption scheme (confusion and diffusion) is demonstrated in the given flow diagram [6]:-

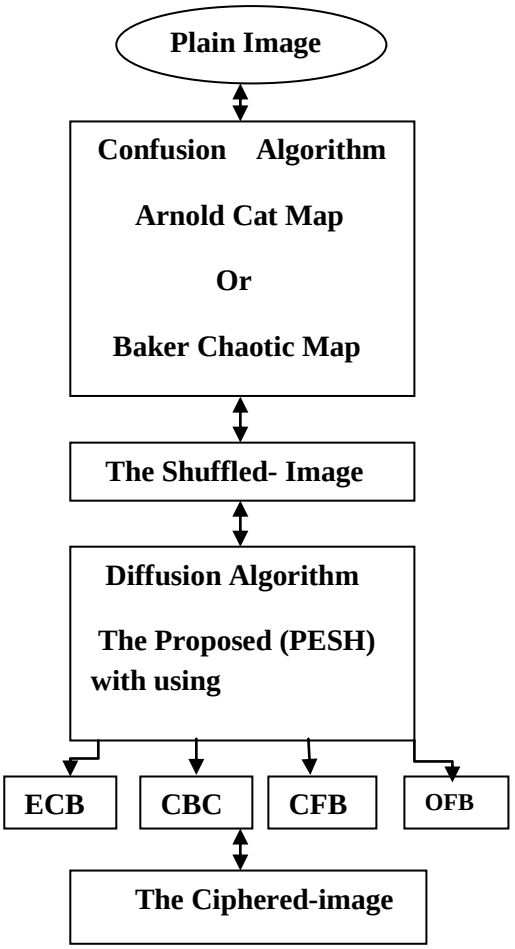


Figure1: The Diagram for illustration of encryption/Decryption of existing scheme [6]

3. PROPOSED SHUFFLE SCHEME

Based on Siamese method used in magic square generation new shuffling scheme is introduced in this section to increase the level of security of digital images. The pixels of the original image are shuffled using the steps described below. The proposed scheme is made key dependent which makes it different from the Siamese method. The new shuffled scheme is explained by taking 5*5 data matrix as shown in figure 2a.

Step1:- Move one row up and then right ( **)**

Initially we take a new data matrix (5*5) say, arr having -1 filled as a data value which will be used to scanned the position .Based on the key the row position value is decremented by 1 and the column position value is incremented by 1.suppose the key is (3,4) which indicates the starting location in new matrix. According to first round of shuffling scheme in order to move upward-right the row position value is decremented by 1 and the column position value is incremented by 1 so, the new position obtained is (2,5).

- The new position so obtained is scanned in new data matrix, **if** the location has -1 filled in it, then the position is filled from the original matrix. **Else** if the location is already filled then we place the element above the starting row location **.**The data from original matrix is

read linearly in row major order starting from 1st location to 25th location.

- Considering the boundary condition when row and column reaches its maximum value. If the row value exceeds its maximum value , reaches to 6 it is reset to 1 and if the column position reaches zero then it is reset to 5(maximum value)
- The process continues until the new data matrix is filled and scanned completely.

The new data matrix hence obtained after 1st round is shown in figure 2b and is then passed for second round of shuffling scheme.

Step2:- Move one row up and then left ( )

The same process will be followed as described in step 1 with certain changes- In second round of shuffling scheme in order to move upward-left ,based on the key value both the row position value and the column position value will be decremented by 1. To check the boundary conditions, if row and column position value exceeds its maximum value it is reset to 1. Using key (2,3) the matrix obtained after second round is shown in figure 2c.The new data matrix hence obtained is passed for third round of shuffling scheme.

Step3:- Move one row down and then right ( )

The same process will be followed as described in step1 with certain changes. In third round of shuffling scheme in order to move downward-right, based on key value both the row position value and the column position value will be incremented by 1. To check the boundary conditions, if row and column position value reaches zero it is reset to maximum value (5). Using key (4, 5) the matrix obtained after third round is shown in figure 2d. The new data matrix hence obtained is passed for fourth round of shuffling scheme

Step4:- Move one row down and then left ( )

The same process will be followed as described in step1 with certain changes. In fourth round of shuffling scheme in order to move downward-left, based on key value the row position value is incremented by 1 and the column position value will be decremented by 1. To check the boundary conditions, if row position value reaches zero it is reset to maximum value (5) and if column position value exceeds its maximum value it is reset to 1. Using key (1, 3) the matrix obtained after fourth round is figure 2e. The new data matrix hence obtained is passed for the last round of shuffling scheme

Step5:- Bit-XOR with Key based diagonal spiral positions

The data matrix obtained from fourth round is bit-XORed with key based diagonal spiral position.

First the position of data matrix is displayed in diagonal spiral manner

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

After getting diagonally spiraled positions, the starting position can be decided as per the value derived from the key.

Suppose key (i, j) is (3, 4).we find the starting position from given equation to have diagonal spiral elements.

$$X = \left(\left((i-1) \times N\right) + j\right) \qquad 8$$

Where N is the number of rows .After that bitxor operation is applied as shown-

$$\text{Array} = \text{array1} \oplus \text{array2} \qquad 9$$

Where array is a new matrix obtained after bitxor operation, array2 is the matrix obtained after step 4 and array1 is the diagonally spiraled position matrix. The two dimensional matrix obtained after bitxoring is shown figure 2f.

The new confused data matrix hence obtained is passed for diffusion by PESH algorithm.

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

2(a)

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

2(b)

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

2(c)

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

2(d)

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

2(e)

28	20	14	27	22
1	22	12	17	20
8	17	0	3	18
5	27	11	9	24
7	2	10	21	3

2(f)

Figure2: Showing Steps of New shuffling Scheme 2(a) original 5x5 data matrix 2(b) Data matrix after 1st round 2(c) Data matrix after 2nd round 2(d) Data matrix after 3rd round 2(e) Data matrix after 4th round2(f) Data matrix after 5th round

This proposed shuffling scheme is used with the PESH diffusion algorithm to get minimum correlation between the pixel values of original plain image and the ciphered image.

Here PESH is applied with single mode of Encryption operation ECB (Electronic Code Book) whereas the new shuffling scheme is applied 5 times in order to shuffle the image.

The block diagram of new shuffling scheme (confusion) and diffusion is shown below:-

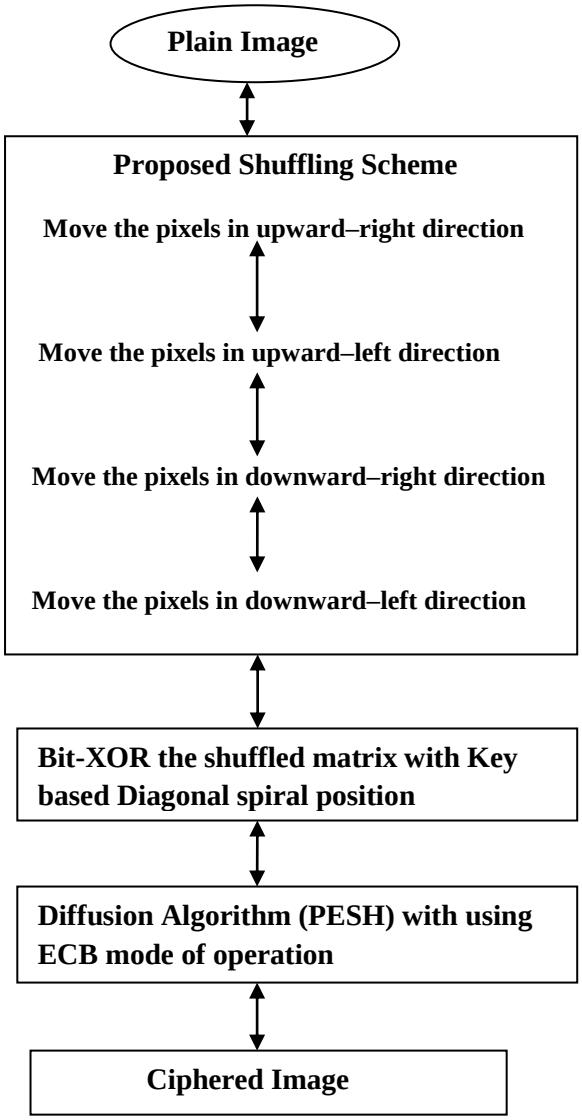


Figure3: Encryption/Decryption technique using new proposed shuffle scheme.

4. COMPARATIVE RESULTS BASED ON SECURITY ANALYSIS

In this paper security analysis is done on both the schemes existing as well as proposed .the schemes are designed and tested by MATLAB 7.10.0.499(R 2010a) version on windows 7 operating system on laptop computer with Intel(R) core(TM) 2 Duo processor, 4.00 GB RAM. The schemes are implemented on regular testing image like Lena while special emphasis will be laid on testing pure white images in order to redundancy. The strength of the scheme will be analyzed using various parameters of security analysis like correlation coefficient, differential attack parameters, histograms and others.

4.1 Statistical Analysis

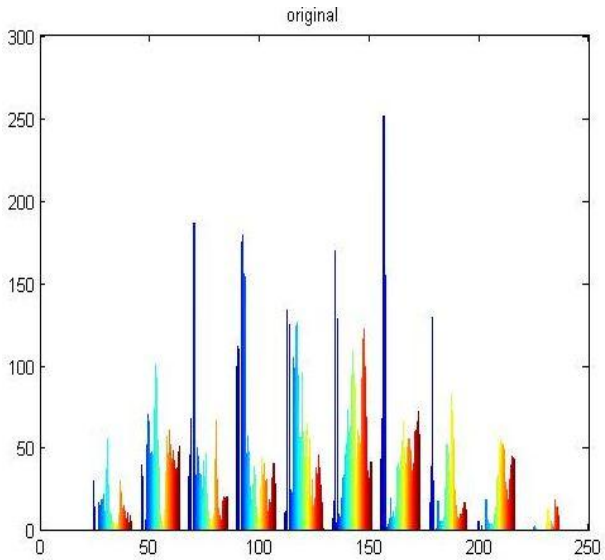
Statistical analysis is done by calculating the histogram and correlation coefficient among the pixels.

Histogram Analysis

Histogram shows the distribution of data. The flatness of the histogram shows uniform distribution and indicates the efficiency and strength of the scheme [2][3][5].

The original image (lena.jpg) with size 256*256 pixels is shown in figure 4a and its corresponding histogram is shown in figure 4b.

(a)

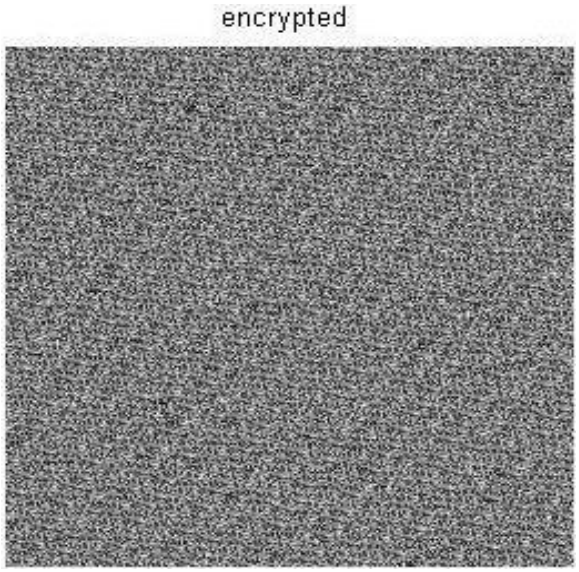


(b)

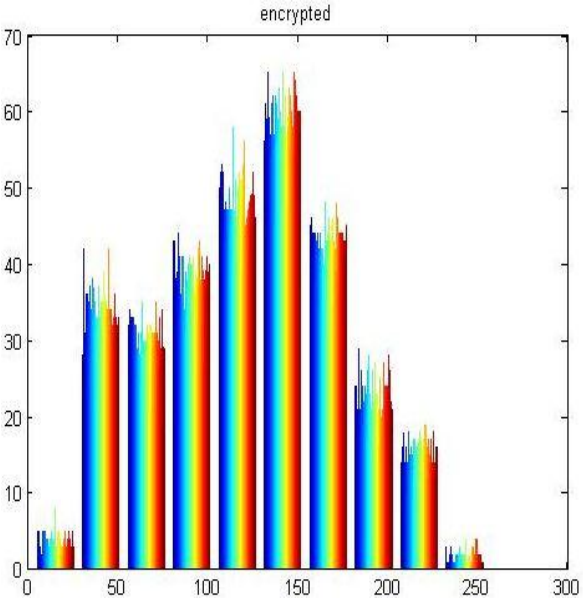
Figure4: Original-image and its histogram (a) original image (lena.jpg) (b) histogram of original image

The histogram of both the schemes with their encrypted image is shown below in figure 5 and figure 6:-

Figure5 shows Encrypted image and histogram of encrypted image produced after applying existing scheme (combination of Arnold cat map and PESH algorithm) is shown below. The histogram obtained is not accurate and its bell shaped curve depicts non uniform distribution of data which is not good from security aspects. The Arnold cat map is applied 10 times and PESH is applied once.



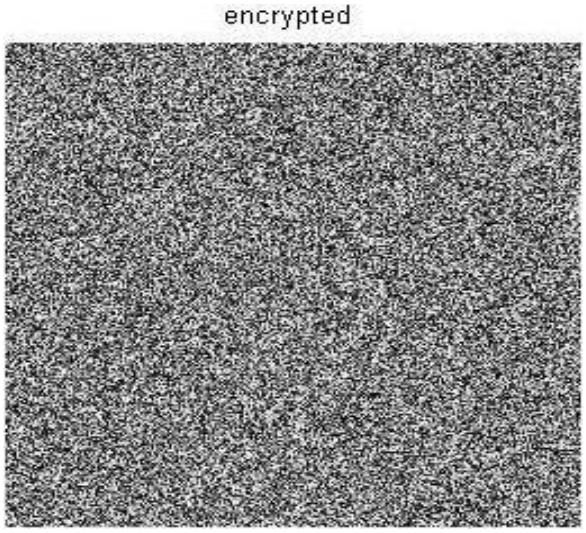
(a)



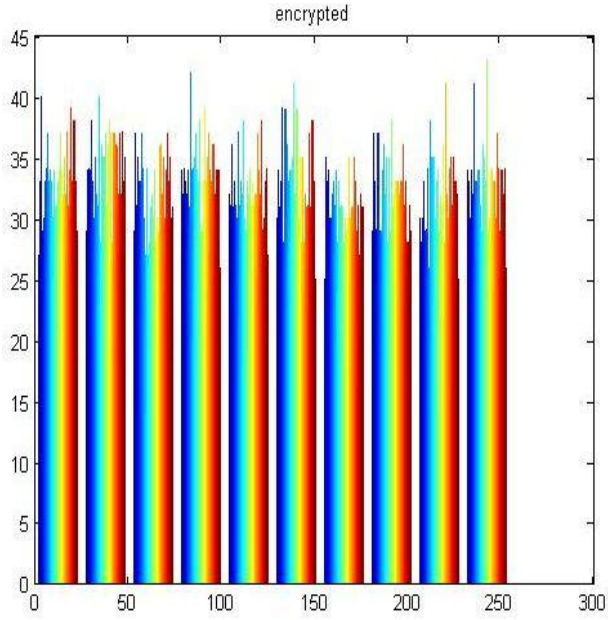
(b)

Figure5: Encrypted-image and its histogram produced after applying existing algorithm (a) Encrypted-image (lena.jpg) (b) histogram of encrypted image

Figure 6 illustrates the ciphered image and its histogram after using the combination of proposed shuffling scheme and the PESH for diffusion. The new shuffling scheme is applied 5 times and PESH is applied once. The histogram obtained appears to be flat and shows better results as compared with the histogram of existing scheme which was bell shaped and the ciphered image depicts the visual aspect of the algorithmic strength. The flatter the histogram is, the better the algorithm's performance is.



(a)



(b)

Figure6: Encrypted-image and its histogram produced after applying proposed algorithm (a) Encrypted-image (lena.jpg) (b) histogram of encrypted image

Correlation Coefficient

This factor measures the amount of deviation between the plain and encrypted image .value close to 1 show that plain image and ciphered image is highly correlated. Ideally its value should be close to zero which indicates high deviation among the pixel values of plain and encrypted image [1] [2] [3].

4.2 Differential Attack Analysis

The change produced on encrypted image by changing just one pixel value in the plain image. This change will depict the quality of encryption algorithm. The parameters used are number of pixel change rate (NPCR) and unified average change intensity (UACI) given by [1] [2] [3]:-

$$\mathbf{NPCR} = \left[\frac{\sum_{I,J} \mathbf{D(I,J)}}{\mathbf{W \times H}}\right] \times \mathbf{100}\% \qquad 10$$

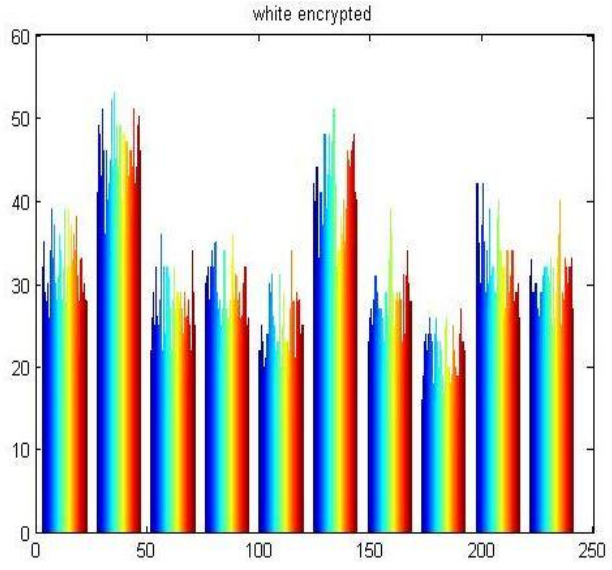
$$\mathbf{UACI} = \left[\frac{\left(\sum_{I,J} \mathbf{C_1\,(I,J) - C_2\,(I,J)}\right)}{\mathbf{(W \times H \times 255)}}\right] \times \mathbf{100}\% \qquad 11$$

Where, C_1 and C_2 are two ciphered images, W and H are the width and height of image respectively, D(I, J) is determined by $C_1(I,J)$ and $C_2(I,J)$, if $C_1(I,J) = C_2(I,J)$ then D(I,J)=0 otherwise D(I,J)= 1.

Table 1. Table showing comparative analysis

S.NO	SECURITY ANALYSIS TOOL	EXISTING SCHEME	PROPOSED SCHEME
1	**Correlation coefficient**	0.00065	0.00054
2	**NPCR value**	99.89	99.95
3	**UACI value**	0.0006	0.0075

The pure white image was used to test the efficiency of the proposed scheme .The histogram produced by using white image when new scheme was applied is shown below:-



5. CONCLUSION

The scheme proposed in this paper prime aim was to reduce redundancy .Experimental results shows that the scheme helps to remove redundancy and the histogram so obtained is flat .The proposed scheme take less time to execute and hence is efficient for light weight devices. The proposed scheme is better than the existing PESH algorithm and can be used in future by various devices using encryption.

6. REFERENCES

[1] M.A. EL-Wahed; S. Mesbah & A. Shoukry, "Efficiency and security of some image encryption algorithms", In the Proceedings of the World Congress on Engineering, 2008, 1, London, U.K.

[2] P. Maggo, Dr R.S. Chhillar, "Security of Multimedia Data: A Review Paper on various Image Security Algorithms", National Conference on Advanced Computing Technologies, Vol. 2, March 2013,pp. 852-857.

[3] 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.

[4] F. Ahmed & C.L. Resch, "Characterizing cryptographic primitives for light weight digital image encryption", Mobile Multimedia/Image Processing, Security and Application 2009, edited by Sos S. Agaian, Sabah A.Jassim, Proc. Of SPIE Vol. 7371, 73510G.

[5] I.A. Ismail; M. Amin & H. Diab, "An efficient Image Encryption Scheme Based Chaotic Logistic Maps",In the Medwell online International Journal of Soft Computing 2(2):285-291,2007 .

[6] 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

[7] El-Fishawy Nawal and M. Abu Zaid Osama, "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms", International Journal of Network Security, Vol.5, No.3, PP.241–251, Nov. 2007.

[8] M.A.B. Younes & A.Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008.

[9] Q. Zhang; Q. Wang & X. Wei, "A Novel Image Encryption Scheme Based on DNA Coding and Multi – Chaotic Maps", American Scientific Publishers Advanced Science Letters Vol.3, 447-451, 2010.

[10] D. Socek, S. Li; S.S. Magliveras & B. Furht, "Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption", IEEE/CreateNetSecureComm, Athens, Greece, pp. 406-408, September 5-9, 2005.

[11] G.N. Krishnamurthy & V. Ramaswamy, "Making AES stronger: AES with Key dependent S-box", Int. J. Comp.Sci.Network Secu., 2008, 8(9), pp.388-98.

[12] C. Li & G. Chen, "On the security of a class of Image Encryption Schemes".

[13] D. Chattopadhyay ; M.K Mandal &D. Nandi , " Symmetric Key chaotic image encryption using circle map", Indian Journal of Science and Technology Vol.4 No. 5 (May 2011) ISSN: 0974-6846.