An AES - based Robust Image Encryption Scheme

Supriyo De
Dept. of ECE and AEIE,
Saroj Mohan Institute of Technology, Guptipara,
Hooghly, West Bengal, India, Pin-712512

Jaydeb Bhaumik
Dept. of ECE,
Haldia Institute of Technology, Haldia,
Purba Medinipur, West Bengal, India, Pin-721657

ABSTRACT

The security of digital information has become a major issue during the last three decades. Encryption is one of the ways to ensure confidentiality for the digital data. Protection of multimedia data is now becoming a big challenge to create a healthy digital world. A large number of algorithms for data and image encryption are reported in the literature. Unfortunately, all traditional cryptosystems can't fulfill all the requirements of image encryption. Cryptographic weakness or high computational cost does not fulfill the real time requirement for the encryption technique. In this paper a novel approach is developed to encrypt the digital image which ensures better security with optimum cost. A linear transformation is done before encrypting an image by the Advanced Encryption Standard (AES) in ECB mode. The results show that the correlation between adjacent image elements is significantly reduced by employing the proposed scheme compared to other schemes. The histogram, correlation, entropy analysis as well as differential cryptanalysis of proposed image encryption scheme have been done to justify the strength of the proposed scheme.

General Terms

Security, Image Encryption

Keywords

Block Cipher, Advanced Encryption Standard, Linear transformation, Security analysis

1. INTRODUCTION

Image and video encryption have a huge application in various field including Internet communication, multimedia systems, medical imaging, telemedicine, confidential videoconferencing, military and defense maps and data-base, mobile computing, design of electronic circuits, technical model designing etc. Two parameters are mainly defining the effectiveness of image encryption. The first one is the speed of the encryption algorithm which important for online applications and the second one is the security of the encryption technique which is generally getting the importance in banking, defense sector. In this paper, encryption algorithm that can satisfy the requirements of these two parameters were implemented.

The Advance Encryption Standard (AES) was announced by the National Institute of Standard and Technology (NIST) in 2001 [1]-[3]. Basically, it includes three main processes, Key Expansion, Encryption and Decryption. In case of multimedia data security especially for digital image encryption by AES algorithm in ECB mode does not provide satisfactory result. For digital image there is a possibility where some positions pixel values do not have any variation. Since in ECB mode, each of same input blocks (length 128 bits) generate identical set of cipher blocks. The deficiency becomes more for those images where the color variation does not appear. In this deficiency pattern and shape of the images can be easily predicted from the cipher images.

Different techniques for image encryption have been studied in [4]. Combined encryption and compression scheme has also been reported by researchers in [5]. In [6] two direct approaches is implemented to prevent the deficiency. In first approach, the identical input difference is modified by adding different number sequences to them and the other approach is to remove the identical inputs using compression. Huang *et al.* [6] discussed limitation of AES in ECB mode for digital image encryption and proposed a modified AES for image encryption. In [7] authors proposed an algorithm based on AES key expansion in which the encryption process is a bit wise XOR operation of a set of image pixels along with the 128 bit key which changes for every set of pixels and it offers good resistance against brute force attack, key sensitivity tests and statistical cryptanalysis. Riad *et al.* [8] proposed a selective image encryption technique using hybrid chaos and block cipher. Shtewi *et al.* [9] also introduced a modified AES (MAES) for image encryption by changing ShiftRows operation of original AES. From Fig. 1(i), 1(j), 1(k) and 1(l), it is noted that scheme MAES in ECB mode also can't provide strong confidentiality for all images.

In this paper, we have proposed a new scheme called PE(Permutation followed by Encryption) to overcome the limitation of the AES and MAES. In this scheme we have introduced a permutation block before the AES block. The proposed scheme supports the parallel architecture of AES and also the complexity of permutation is very less compared to AES encryption scheme. In this work, the histogram, correlation and entropy analysis and resistance against differential attack of proposed image encryption scheme have been compared with the existing image encryption schemes. It is shown that encryption and decryption both can be done in parallel or pipelined mode. So, the proposed scheme is very much effective for multimedia application where high throughput is essential.

The rest of the paper is organized as follows. Section 2 discusses the proposed the PE algorithm for image encryption. Experimental results obtained by employing proposed scheme are elaborated in section 3. In section 4, security of proposed scheme has been evaluated. Also the scheme has been compared in terms of histogram analysis, correlation coefficient, entropy and differential cryptanalysis (Number of Pixels Change Rate and Unified Average Changing Intensity) with two existing schemes in this section and finally the paper is concluded in section 5.

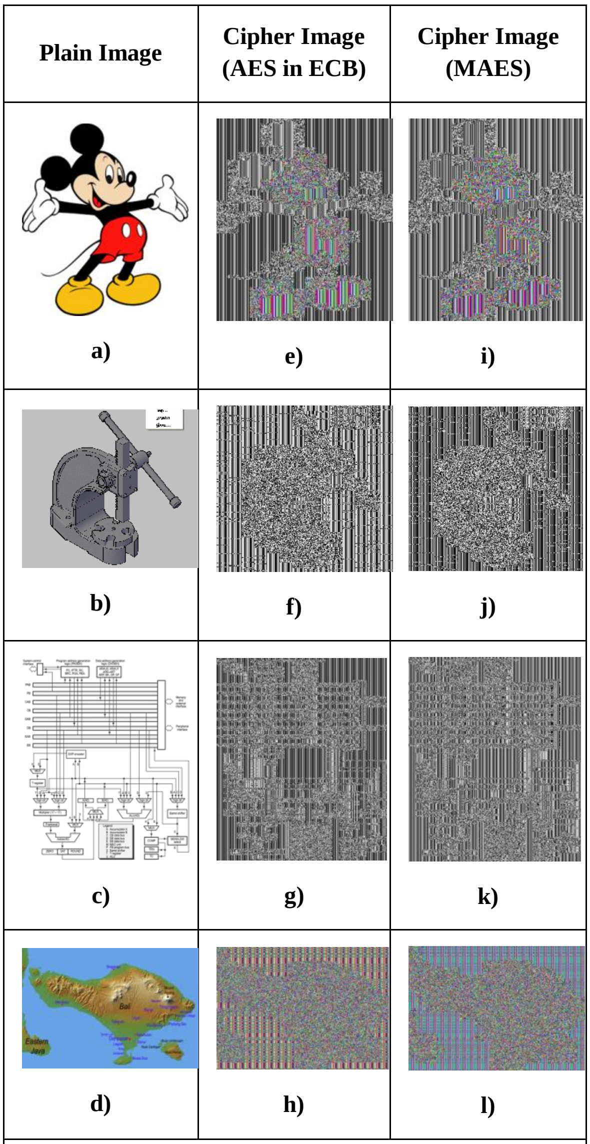


Fig 1: Cipher Image - by Applying Different Technique

2. PROPOSED SCHEME

In this section, the proposed image encryption scheme based on permutation block (PB) followed by AES encryption has been introduced.

2.1 Image Encryption

Image encryption scheme introduced PB algorithm before the AES in ECB mode. PB performs a linear transformation of the plain image. In ECB mode of AES encryption scheme, a fixed key and fixed set of inputs always produce a same set of outputs and correspondingly the cipher image carries some information about the plain image. So, before applying the AES we introduced a permutation block with minimum complexity to shuffle the pixel values of the image to improve the security of encrypted image.

2.1.1 Permutation Algorithm

Permutation block is mainly incorporated with row shifting and column shifting of the image matrix with a linear relation. The total shifting process is done N (typically 10) times to get the better result. The operation of permutation block is briefly described below where ‘X’ denotes the input matrix and ‘Y’ is the shuffled output matrix. Row shift and column shift is totally a linear operation and this also depends upon the row number and column number respectively.

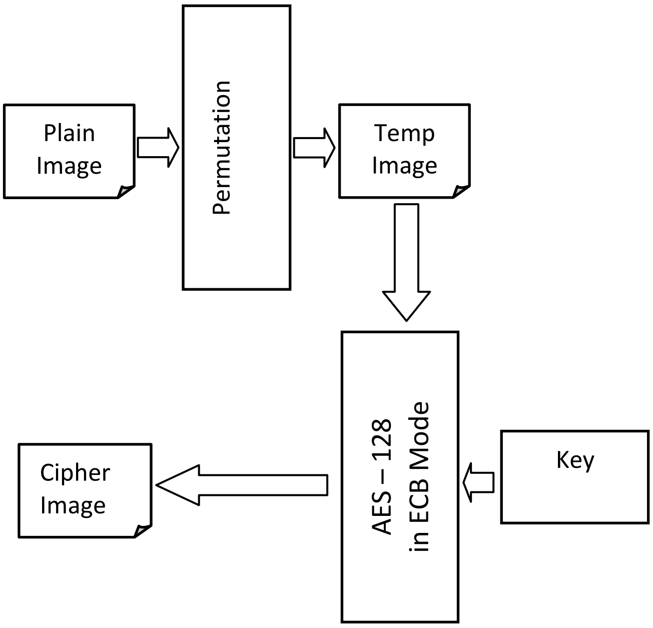
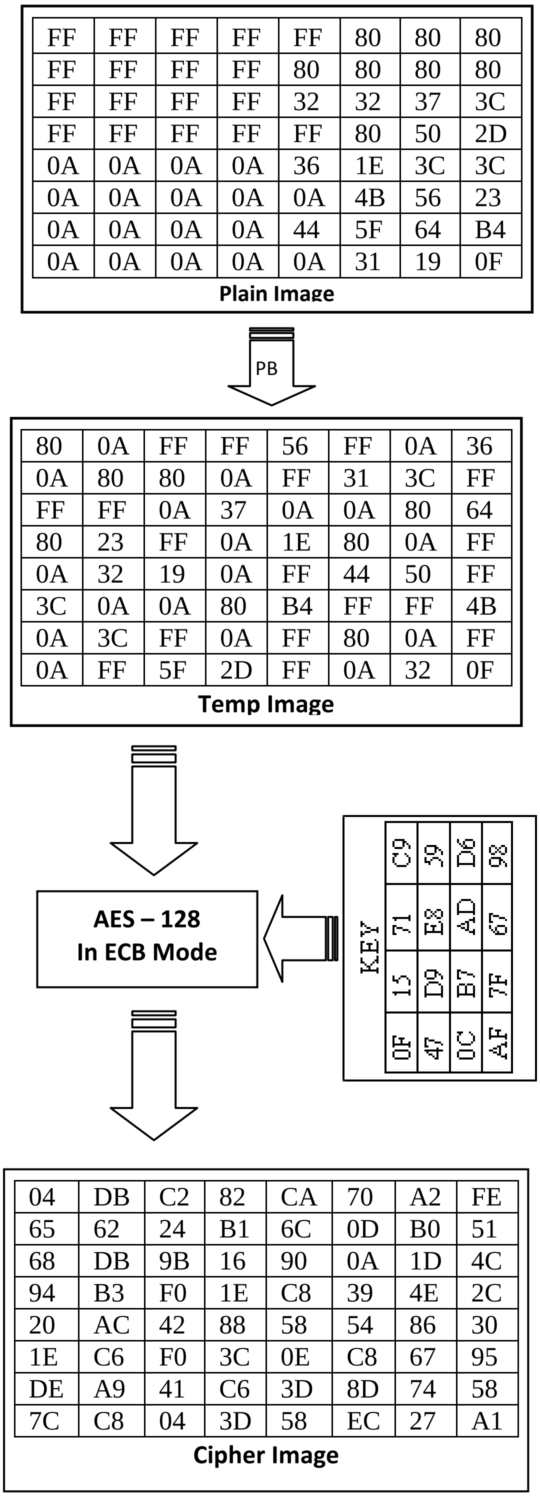


Fig 2: Block diagram of proposed image encryption scheme

```
Permutation Algorithm for each plane of colour  Image
Input:   $X_{(i)(j)}$
Where,   i=1,2,3,4 . . . . . . . R (no. of row)
           j=1,2,3,4 . . . . . . . C (no. of column)
Output: $Y_{(i)(j)}$
Where,    i=1,2,3,4 . . . . . . . R (no. of row)
            j=1,2,3,4 . . . . . . . C (no. of column)
begin
 for r =1 to N
   for i= 1 to R
     $X_{(i)(j)}$ = Circular Right Shift Row (i) of $X_{(i)(j)}$ by i bytes
   end
   for j= 1 to C
     $X_{(i)(j)}$ = Circular Upward Shift Column (j) of $X_{(i)(j)}$ by j bytes
   end
 end
 $Y_{(i)(j)}=X_{(i)(j)}$
end
```

2.1.2 Encryption

In the part of encryption AES is used in ECB mode. For AES encryption we have taken a fixed 128 bit key for a particular image. Figure 3 shows how the permutation block and AES block work together. Here 64 byte plain text is used for this example and 128 bit key for AES is shown in Fig. 3.



FF	FF	FF	FF	FF	80	80	80
FF	FF	FF	FF	80	80	80	80
FF	FF	FF	FF	32	32	37	3C
FF	FF	FF	FF	FF	80	50	2D
0A	0A	0A	0A	36	1E	3C	3C
0A	0A	0A	0A	0A	4B	56	23
0A	0A	0A	0A	44	5F	64	B4
0A	0A	0A	0A	0A	31	19	0F

Plain Image

80	0A	FF	FF	56	FF	0A	36
0A	80	80	0A	FF	31	3C	FF
FF	FF	0A	37	0A	0A	80	64
80	23	FF	0A	1E	80	0A	FF
0A	32	19	0A	FF	44	50	FF
3C	0A	0A	80	B4	FF	FF	4B
0A	3C	FF	0A	FF	80	0A	FF
0A	FF	5F	2D	FF	0A	32	0F

Temp Image

KEY

0F	15	71	C9
47	D9	E8	59
0C	B7	AD	D6
AF	7F	67	98

04	DB	C2	82	CA	70	A2	FE
65	62	24	B1	6C	0D	B0	51
68	DB	9B	16	90	0A	1D	4C
94	B3	F0	1E	C8	39	4E	2C
20	AC	42	88	58	54	86	30
1E	C6	F0	3C	0E	C8	67	95
DE	A9	41	C6	3D	8D	74	58
7C	C8	04	3D	58	EC	27	A1

Cipher Image

Fig 3: Flow of Image Encryption Scheme

2.2 Image Decryption

Image decryption process follows the reverse sequence of the image encryption. The flow starts from the AES decryption in ECB mode and then the intermediate output is just goes under the reverse permutation block algorithm i.e. instead of Circular Right Shift Row and Circular Upward Shift Column here Circular Downward Shift Column and Circular Left Shift Row is used.

3. EXPERIMENTAL RESULTS

Experiments are performed using different plain images to prove the validity of the proposed algorithm. Figures 4(e), 4(f), 4(g) and 4(h) are the output of the PE algorithm and the corresponding original images are shown in Fig. 4(a), 4(b), 4(c) and 4(d). Output of permutation block doesn't provide any security because it is linear, reversible and no secret key is associated. This intermediate output is now applied as input of AES encryption scheme to obtain the cipher image. Figures 4(i), 4(j), 4(k) and 4(l) show the cipher image output of the proposed scheme.

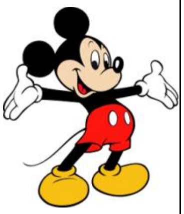
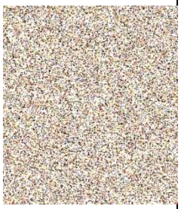
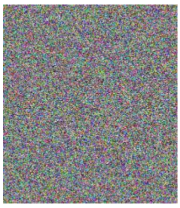
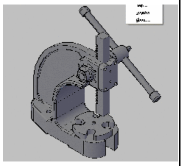
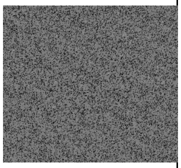
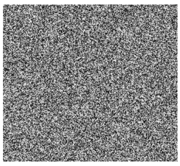
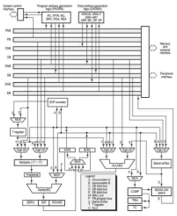
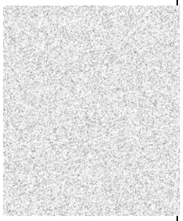
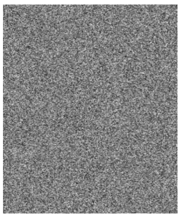
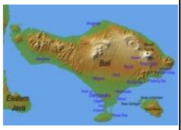
Plain Image	Temp Image	Cipher Image
 a)	 e)	 i)
 b)	 f)	 j)
 c)	 g)	 k)
 d)	 h)	 l)

Fig 4: Image Encryption Result for Proposed Scheme

4. SECURITY ANALYSIS

Entropy, histogram and correlation are the three important parameters to analyze the security of image encryption algorithm. Entropy of encrypted image possibly increases through efficient encryption algorithm. On the other hand correlation between two adjacent pixels can be reduced and uniform histogram can be obtained in the encrypted image. A good encryption technique should be robust against cryptanalytic, statistical and brute-force attacks.

4.1 Key Space Analysis

The key-space of an encryption technique is the set of possible keys that can be used to encode data using that technique. In the case of a strong encryption scheme, many keys must be tried in any brute-force attack on that technique. The proposed scheme has 2^{128} different combinations of the secret key. This long key space is sufficient for reliable practical use.

4.2 Statistical Analysis

Statistical analysis is essential to check the robustness/randomness of the cipher text obtained by the deterministic encryption scheme. Histogram and correlation of two adjacent pixels in the plain image/cipher image are analyzed to prove the effectiveness of the proposed scheme with respect to other well known encryption scheme.

4.2.1 Histogram Analysis

An image-histogram describes how the image-pixels are distributed by plotting the number of pixels at each intensity level. It is necessary for the cipher image to bear no statistical similarity. When the cipher image histogram is similar to the histogram of random image then it seems that the encryption algorithm has good performance. Figure 5 shows the histogram analysis of different plain images and cipher images. Figures 5(e), 5(f), 5(g) and 5(h) are histogram obtained by applying the AES encryption technique to the plain images and Figures 5(i), 5(j), 5(k) and 5(l) are histogram obtained by applying the MAES [9] encryption technique on the same plain images. The histogram of cipher images which are obtained by employing proposed scheme on same plain images are shown in Fig. 5(m), 5(n), 5(o) and 5(p). Histogram analysis of the proposed scheme justifies the effectiveness over MAES.

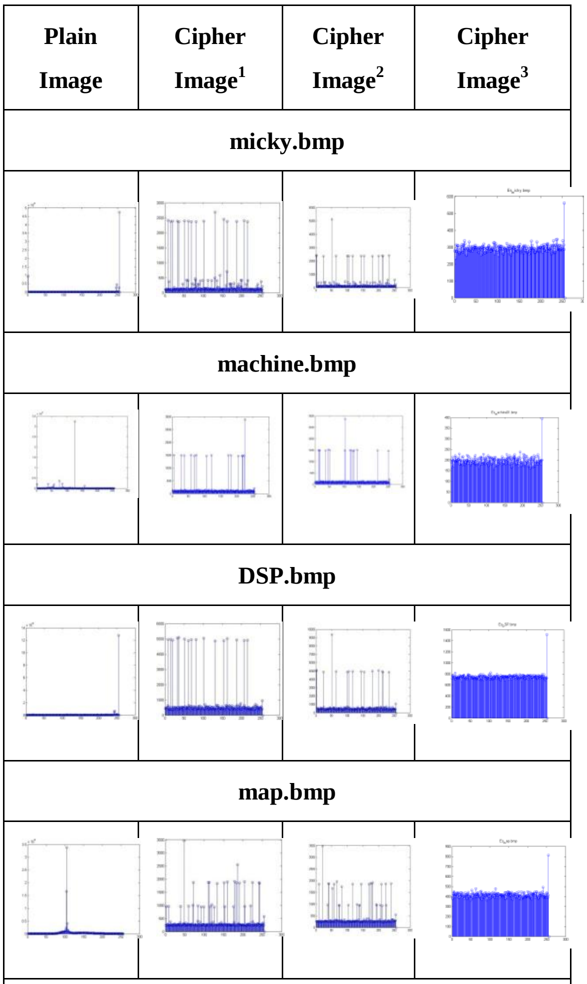
4.2.2 Correlation Analysis

The Correlation is one of the common and useful statistical tools to describe the degree of relationship between two sets of data. It is defined by the following equation.

$$r = \frac{n\sum(xy) - \sum xy \sum y}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}} \ldots.(1)$$

Where,
r: correlation value
n: the number of pairs of data
Σxy: sum of the products of paired data
Σx: sum of x data
Σy: sum of y data
Σx^2: sum of squared x data
Σy^2: sum of squared y data

We have also analyzed the correlation between two adjacent pixels for plain image / cipher image respectively. Here we have taken the possible four neighboring angels for computing the correlation. Experimental result of correlation coefficient is shown in Table 1 to justify the effectiveness of our proposed technique. It breaks the correlation of the adjacent pixel in the cipher image. Figure 6 shows the pattern of correlation for plain images and corresponding cipher images obtained by AES, MAES and proposed encryption techniques. The result shows that the proposed scheme successfully breaks the correlation in between two neighbor pixels.



Cipher Image[1]: obtained by AES

Cipher Image[2]: obtained by MAES

Cipher Image[3]: obtained by PE

Fig 5: Histogram analysis of different image

Table 1. Correlation coefficient of two adjacent pixels in the original and encrypted images

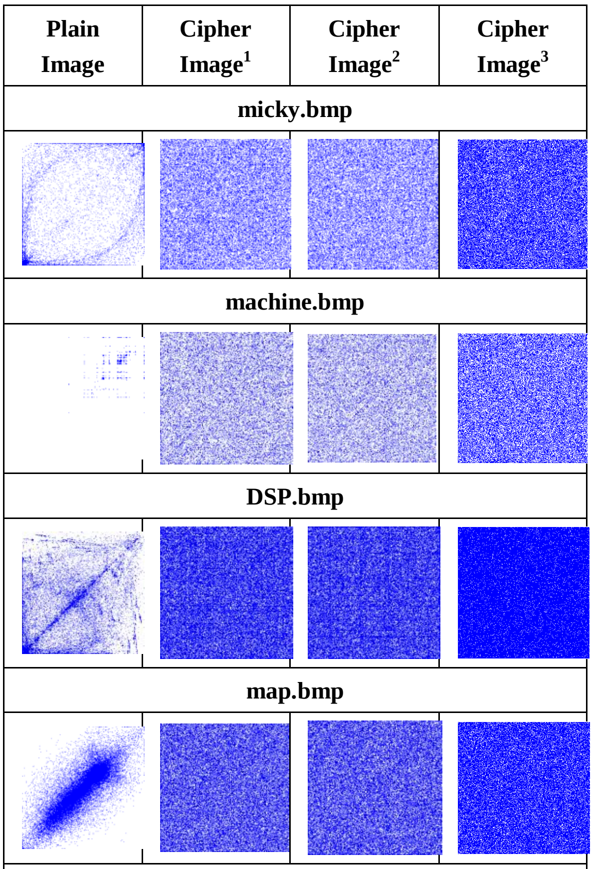
Image File Name	Direction	Plain Image	Cipher Image[1]	Cipher Image[2]	Cipher Image[3]
micky.bmp	0^0	0.9510	0.0053	-0.1045	0.0148
	45^0	0.9253	0.0153	-0.0856	0.0160
	90^0	0.9523	0.5871	0.6171	0.0097
	135^0	0.9151	0.0175	-0.0850	0.0195
Machine	0^0	0.8403	0.0973	-0.0348	0.0108
	45^0	0.8165	0.0942	-0.0145	0.0245
	90^0	0.8638	0.4634	0.4072	0.0105

	135^0	0.8463	0.0938	-0.0147	0.0274
DSP.bmp	0^0	0.8086	-0.0081	-0.0422	0.0050
	45^0	0.4458	-0.0034	-0.0358	0.0167
	90^0	0.5820	0.4663	0.4808	0.0072
	135^0	0.4452	-0.0052	-0.0376	0.0156
map.bmp	0^0	0.8533	0.0738	0.0079	0.0058
	45^0	0.8675	0.0569	0.0157	0.0167
	90^0	0.8830	0.2172	0.2365	0.0083
	135^0	0.7954	0.0566	0.0165	0.0167

Cipher Image[1]: obtained by AES

Cipher Image[2]: obtained by MAES

Cipher Image[3]: obtained by PE



Cipher Image[1]: obtained by AES

Cipher Image[2]: obtained by MAES

Cipher Image[3]: obtained by PE

Fig 6: Histogram analysis of different images

4.3 Entropy Analysis

Entropy is a measure of randomness. Higher value of entropy of encrypted image indicates the uniform distribution of pixel values which implies stronger security. The Entropy H_e of the input image and the encrypted image is calculated using following equation.

$$H_e = -\sum_{k=0}^{G-1} P(k) log_2\, (P(k)) ....(2)$$

Where,
H_e: entropy.
G: gray value of input image (0... 255).
P(k): is the probability of the occurrence of symbol k.

Table 2. Entropies of the original and encrypted images

Image File Name	Plain Image	Cipher Image[1]	Cipher Image[2]	Cipher Image[3]
micky.bmp	2.6501	6.8037	6.7483	7.9975
machine.bmp	2.3005	6.8940	6.8914	7.9959
DSP.bmp	3.2788	7.2513	7.2154	7.9992
map.bmp	5.1929	7.5168	7.5178	7.9982

Cipher Image[1]: obtained by AES
Cipher Image[2]: obtained by MAES
Cipher Image[3]: obtained by PE

Table 2 shows the entropy analysis results for different plain images and corresponding cipher images, obtained by using AES, MAES and PE scheme. Comparison of column 3, 4 and 5 of Table 2 shows that entropy of cipher images are the best in proposed scheme compared to others.

4.4 Differential Cryptanalysis

Differential cryptanalysis is a common attack against any block cipher. In image encryption, the resistance of encrypted image against differential attacks is commonly analyzed via the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) tests [10] [11].

To compute the NPCR and UACI, two cipher images are required which are obtained from the same plain image with a slight change of pixel value (usually a single pixel change).

We have obtained a reliable result of NPCR and UACI values for the proposed scheme. For calculation of NPCR and UACI, the following equations [10] [11] are used.

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% ....(3)$$

$$\mathrm{UACI} = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% .... (4)$$

Where,
C1 and C2: two ciphered image whose corresponding original images have only one-pixel difference. C1 and C2 have the same size. C1(i, j) and C2(i, j): grey-scale values of the pixels at grid (i ,j).
D(i, j): determined by C1(i, j) and C2(i, j),
if C1(i, j) = C2(i,j), then, D(i, j) = 1;

otherwise, D(i, j) = 0.
W and H: no. of columns and rows of the image pixel values.

Experimental result of NPCR and UACI are shown in Table 3 and Table 4 respectively which established the consistency of the proposed scheme.

Table 3. NPCR for encrypted images

Image File Name	NPCR		
	AES	MAES	PE
micky.bmp	96.8258	99.8565	99.6281
machine.bmp	99.6497	99.6398	99.6542
DSP.bmp	97.3970	99.7479	99.6140
map.bmp	99.7702	99.7185	99.6191

Table 4. UACI for encrypted images

Image File Name	UACI		
	AES	MAES	PE
micky.bmp	11.6858	11.0891	16.7259
machine.bmp	16.839	16.7375	16.6796
DSP.bmp	13.1187	12.2807	16.7000
map.bmp	14.8455	19.0599	16.6823

5. CONCLUSION

In this paper a simple but reliable scheme has been proposed for image encryption using a combination of permutation followed by AES based encryption employing ECB mode. In terms of statistical analysis such as entropy, correlation and histogram the proposed scheme provides better results. In this scheme, encryption and decryption modules can work in parallel or/and pipelined mode which is very much effective for multimedia data encryption. In future it can be extended to video encryption as its required high throughput.

Till date AES is secure against all existing practical attacks. Since proposed PE is based on AES so it is secure. In spite of having the knowledge of inverse permutation on cipher image the scheme does not leak any information about plain image without decryption. Therefore, the proposed PE image encryption scheme is also secure against all existing practical attack.

6. REFERENCES

[1] J. Daemen and V. Rijmen, “The Design of Rijndael- AES, The Advanced Encryption Standard,” Springer-Verlag, 2002.

[2] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," Proc. of First Advanced Encryption Standard (AES) Conference, 1998.

[3] H. Yin, H. Debiao, K. Yong, and F. Xiande, "High-speed ASIC implementation of AES supporting 128/192/256 bits," Proc. of Int. Conf. on Test and Measurement, IEEE, Vol. 1, Dec. 2009, pp. 95-98.

[4] R. Pakshwar, V. K. Trivedi, V. Richhariya, “A Survey on Different Image Encryption and Decryption Techniques,” International Journal of Computer Science and Information Technologies, Vol. 4(1), 2013, pp. 113-116.

[5] X. Li, J. Knipe, H. Cheng, “Image Compression and Encryption Using Tree Structures,” Elsevier Science - Patten Recognition Letters, 1997, pp 1253-1259.

[6] C. W. Huang, Y. H. Tu, H. C. Yeh , S. H. Liu, C. J. Chang, “Image observation on the modified ECB operations in Advanced Encryption Standard,” Proc. of Int. Conf. on Information Society (i-Society), London, Jun. 2011, pp. 264 – 269.

[7] B. Subramanyan , V.M. Chhabria, T. G. S. Babu, “Image Encryption Based on AES Key Expansion,” Emerging Applications of Information Technology (EAIT), Second International Conference, India,Feb. 2011, pp. 217 – 220.

[8] A. M. Riad, A. H. Hussein, A. A. El-Azm, “A New Selective Image Encryption Approach Using Hybrid Chaos and Block Cipher,” Proc. Of Int. Conf. on Informatics and Systems (INFOS), Cario, May. 2012, pp. 36-39.

[9] A. A. Shtewi, B. E. M. Hasan, A. E. F. A. Hegazy, “An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems,” International Journal of Computer Science and Network Security, Vol.10, Feb. 2010, pp. 226-232.

[10] Y. Wu, J. P. Noonan, S. Agaian, “NPCR and UACI Randomness Tests for Image Encryption,” Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), Apr. 2011.

[11] M. A. El-Wahed, S. Mesbah, A. Shoukry, “Efficiency and Security of Some Image Encryption Algorithms,” Proc. of the World Congress on Engineering, Vol. 1, Jul. 2008.