A Novel Approach for Image Encryption by New M Box Encryption Algorithm using Block based Transformation along with Shuffle Operation

Umashankar Pandey
M.Tech IV Sem (CSE)
TRUBA Institute of Egg & I.T
Bhopal

Manish Manoria
Director & Professor in CSE
TRUBA Institute of Egg & I.T
Bhopal

Jainendra Jain
Professor, Department of Mathematics
Sagar Institute of Research, Technology & Science, Bhopal

ABSTRACT

In the present brutal competitive world, security is prime factor to transmit confidential data over the internet. Cryptographic algorithms play very important role in providing the data security against the various attacks. The specific characteristics of image, like high transmission rate with limited bandwidth, correlation among pixels, redundancy and requirement of high storage capacity makes traditional algorithms unsuitable for image encryption. To cross these boundaries for real time applications, design of new algorithms that require less computational power while preserving a sufficient level of security is always a big challenge for researchers. This paper proposes an algorithm based on block based image transformation using perfect shuffle operation followed by new encryption algorithm. In this paper we compare the generated results with available algorithms like AES, RC6 and BFS on the basis of two parameters entropy and correlation.

Keywords

Network Security, Image Encryption, Image Entropy, Image Correlation, Confusion and Diffusion.

1. INTRODUCTION

Due to vast improvement in the fields of computation and network technology, image cryptography got the limelight among the researchers community. Image cryptography has so many applications in the field of internet communication, multimedia systems, medical imaging and more importantly in the defense sector. Because of inherent differences in text data and image data, traditional cryptosystems are not the appropriate choice due to two reasons - first is the size of data and second is the correlation between adjacent points. As the traditional algorithms need more time to encrypt the image data and don’t have appropriate mechanism for controlling the correlation property, the output cipher image may be easily predicated by the intruders. This paper focuses on to minimize the prediction ability of intruders while optimizing the encryption -decryption time. The main idea behind the present work is that an image can be viewed as an arrangement of blocks, pixels and bits. In order to minimize the high correlation among pixels and increase the entropy value, this paper introduces a transformation algorithm which divides the image into blocks and shuffles their positions before they are passed to the encryption algorithm. The variable secret key encryption algorithm (symmetric) is used to encrypt the transformed image. This encryption process decreases the mutual information among the encrypted image pixels resulting in the increased entropy value. The rest of the paper is organized as follows: Section II gives a background about the current image encryption schemes. In Section III, the description of the proposed block-based transformation algorithm is presented. Section IV presents the experimental results and discussion, along with the comparison of proposed algorithm with other systems. Finally, section V concludes the paper.

2. LITRATURE SURVEY

Encryption algorithms can be categorized into two groups - Symmetric (private) key and Asymmetric (public) keys encryption algorithms. In Symmetric key encryption or secret key encryption, only one key is used to encrypt and decrypt the data. The key should be distributed before transmission between entities. Strength of Symmetric key encryption algorithms depends on the size of key used. For the same algorithm, encryption using longer key is harder to break than the one using smaller key. Examples of symmetric key encryption algorithms include DES, 3DES, RC2, RC6, AES, Blowfish among others. DES uses one 64-bit key, Triple DES (3DES) uses three 64-bit keys, RC2 uses one 64-bit key, AES uses various (128,192,256) bit key, Blowfish uses various (32-448) bit key with default key size of 128 bit while RC6 uses various (128,192,256) bit key [1, 2, 3, 4, 5, 6, 7, 8]. Key transportation between communication parties using public networks and key management are two issues in symmetric key cryptography. Even Diffie Hellman Key Exchange Algorithm [8] suffers from man in middle attack.

Asymmetric key encryption or public key encryption algorithms are used to solve above mentioned both issues. In Asymmetric key encryption two keys are used - private key and public key. Public key, known to everyone, is used for encryption and the private key, known only to the user is used for decryption (for example RSA and Digital Signatures). Thus there is no need for distributing the keys prior to transmission. Asymmetric encryption techniques are almost 100 to 10000 times slower than Symmetric ones, as they require more computational processing time [1]. The most common classification of encryption techniques is shown in Fig. 1. Brief description of the most common encryption techniques is given as below:

DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It uses 64 bit key with 64 bit block size. Since inception, many attacks and methods have recorded the weaknesses of DES, which have made it an insecure block cipher [2], [3].

3DES: It is an improved version of DES applied on 64 bit block size with 192 bit key. 3DES uses the encryption method similar to the one used in the original DES but is applied thrice to increase the encryption level and the average safe time. Major drawback of 3DES is its encrypting/decryption time as compared to others cipher methods [2].

RC2: It is a block cipher which uses 64-bits block size with a variable key size ranging from 8 to128 bits. RC2 was said to be unbreakable by its inventor Ronald L. Rivest, but some serious drawbacks were noticed by the researcher's community and were rectified in its higher versions [2].

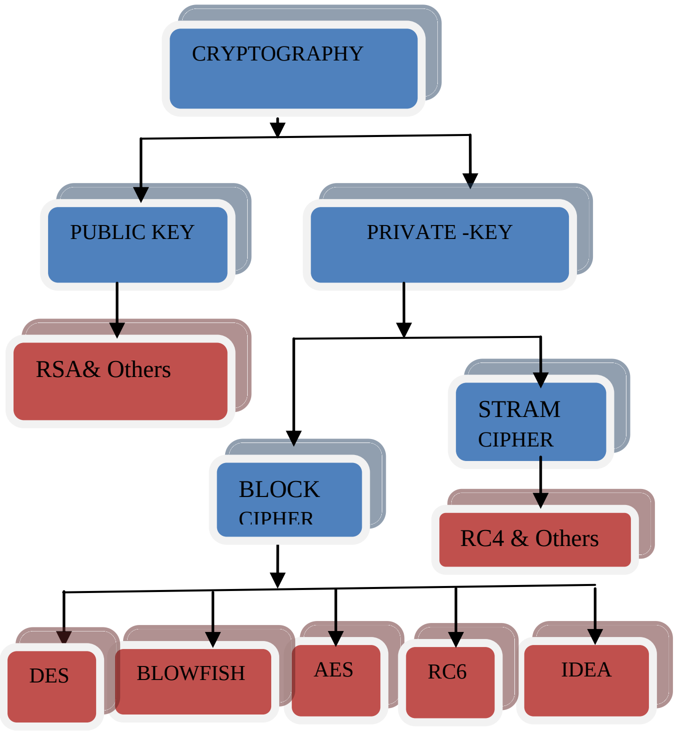


Fig 1: Overview of the field of traditional cryptosystems

Blowfish*:* It is block cipher with block size of 64-bit and takes a variable length key, ranging from 32 bits to 448 bits; default being 128 bits. It is unpatented and license free. Blowfish is a successor of two fish [4].

AES*:* It is a block cipher .It has variable key length of 128, 192, or 256 bits; default being 256 bits. It encrypts data blocks of 128 bits. Number on rounds (10, 12 and 14) used in this algorithm depend upon size of key. AES encryption is fast and flexible and it can be implemented on various platforms especially in small devices [14]. Also, AES has been carefully tested for many security applications [2], [9].

RC6*:* It is block cipher derived from RC5. It was designed to meet the requirements of the Advanced Encryption Standard competition. RC6 has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. RC6 has gained great reputation in very short time and it has been applied successfully in modern applications.

In this section, a study of various research papers based on image encryption/decryption techniques and performance parameters which can play an important role to improve the efficiency and security of algorithm is presented. In [10] author presents comparative study of three block cipher (RC6, MRC6, and Rijndael) algorithms. In this paper authors have encrypted different types of Bitmap images with each of the above three encryption algorithms and measured the maximum deviation between the original and the encrypted images, the correlation coefficient between the encrypted and the original images, the difference between the pixel value of the original image and its corresponding pixel value of the encrypted one, the encryption time and the throughput. These factors were applied on the three encryption algorithms to evaluate both: images containing many high frequency components and images containing very large areas of single colors, as examples of binary images.

In [11], authors have introduced a block-based transformation algorithm based on the combination of image transformation combined with a well known encryption and decryption algorithm, Blowfish. Here the original image was divided into blocks which were rearranged into a transformed image using the above mentioned transformation algorithm and then the transformed image was encrypted using the Blowfish algorithm. The results showed that the correlation between image elements was significantly decreased by using this technique. The results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

In [12], authors have presented another image encryption algorithm based on chaotic encryption, DES and a combination of image encryption algorithm. According to researchers the new encryption scheme realizes the digital image encryption through chaos and improved DES. The authors in their encryption scheme have used the Logistic chaos sequencer to make the pseudo-random sequence, carried on the RGB with this sequence to the image chaotically and then made double time encryptions with improved DES. Theoretical analysis and simulation indicated that this plan had the high starting value sensitivity and enjoyed high security and the encryption speed. In addition it also kept the neighboring RGB relevance close to zero. The algorithm can be used in the actual image encryption.

In [13], authors have presented simulation results based on the parameters like visual testing, key space analysis, histogram analysis, information entropy, encryption quality, correlation analysis, differential analysis, sensitivity analysis and performance analysis. Salsa20, the method used in the paper for protecting the distribution of digital images in an efficient and secure way.

In [14], author has presented a novel and robust chaos-based cryptosystem for secure transmitted images and four other versions. Here author has proposed a block encryption/decryption algorithm where they have shuffled the image pixel position by 2D chaotic map, followed by substitution (confusion) and permutation (diffusion) operations on every block, with multiple rounds, combined using two perturbed chaotic PWLCM maps. The perturbing orbit technique improves the statistical properties of encrypted images. The obtained error propagation in various standard cipher block modes demonstrates that the author's cryptosystem is suitable to transmit cipher data over a corrupted digital channel. Finally, author has tried to prove that his cryptosystem has a high security level on the basis of many tests.

In [15], author has presented a new digital image scrambling encryption algorithm based on chaotic sequence. In this algorithm he has utilized the good features of chaotic sequence related to cryptographic properties, such as pseudo-random, sensitivity to initial conditions and aperiodicity. Basically this algorithm uses logistic mapping to the confusion of the location of pixels in a digital image.

A new image encryption scheme based on high dimensional compound chaotic systems is presented in [16]. Here authors' crypto system utilizes a 2D Logistic chaotic map to shuffle the pixel matrix of the plain image. After that they have combined a strong nonlinear coupling structure with hyper-chaos and different ways of encryption are chosen according to different areas to make gray-level transformation.

In [17], authors apply high level confusion and diffusion properties in the developed algorithm by them. In this regard they have proposed a hybrid approach for partial image encryption. The proposed hybrid approach involves rearranging the mapping image according to SCAN patterns and selecting a pixel value of rearranged mapping image based on the mapping function. The main purpose of proposed technique is to convert the pixel value of original image into row and column values of mapping image.

In [18], author presents an algorithm based on AES Key Expansion in which the encryption process is a bit wise exclusive OR operation of a set of image pixels along with the 128 bit key which changes for every set of pixels . In this paper the keys to be used are generated independently at the sender and receiver side based on AES Key Expansion process. Hence the initial key alone is shared rather than sharing the whole set of keys.

Another paper [19] proposes a novel confusion and diffusion algorithm for image encryption based on logistic map and cheat image. Here the author has chosen the initial condition and control parameter of logistic map as the secret key. The cheat image selected from the most common images in public network, together with the chaotic matrices generated by logistic maps, is employed both in encryption and decryption processes to encrypt and recover the plain image. One cheat image can be used to encrypt a great number of plain images if the cheat image does not attract the attention of the attackers. The computer experiments prove that the proposed image encryption algorithm is robust and secure enough to be used in practical communication.

3. PROPOSED WORK

In this section we present a model of proposed image encryption and decryption algorithm based on chaotic map. Proposed model is divided into four parts. First part is input part where different types of jpeg or jpg images are selected as input. In second part key is selected which will be used in encryption/decryption process. Third part describes the proposed algorithm where an image encryption/decryption based on chaotic map is designed. The results are discussed in the fourth part, where we test our proposed algorithm based on selected parameters.

3.1 Proposed Algorithm

```
1.  Select an Image.
2.  Calculate number of pixels (N) from selected image.
3.  Calculate Horizontal Pixel Block (HPB) = Image Width/10.
4.  Calculate Vertical Pixel Block (VPB) = Image Height/10
5.  Divide no of pixels into two equal parts.
6.  Pixels block should be equal
7.  If No. of pixels block is even then
8.  Go to step no. 10 ,Otherwise
9.  Add one pixel (8 bits) of 0 bits
10. Perform perfect logical XOR Operation using
     Shuffle Network between pixel block as shown in
     the following figure:
```

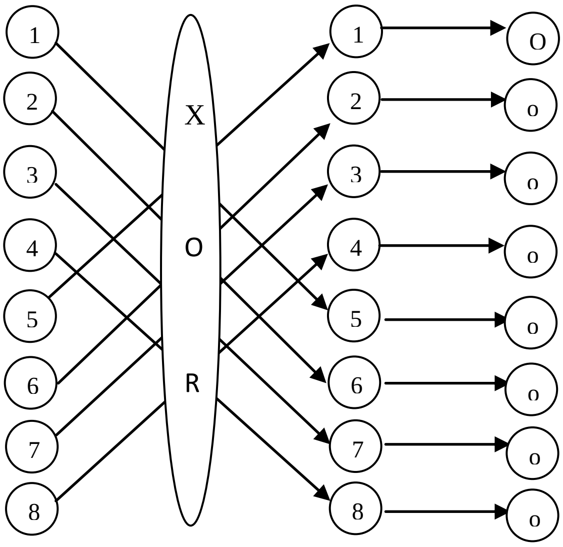


Fig 2 :Shuffle operation

```
11. HPB >VPB Then Set Value = 1
    Else
    Set Value = 2
11. For i= 1 to N pixels.
12. If Value = 1 then
13. Rearrange horizontal pixel block
            $Pixel\ Block_i = (Pixel\ Block_i + i) \bmod N$
    Else If value = 2 then
    Rearrange vertical pixel block
    $Pixel\ Block_i = (Pixel\ Block_i + i) \bmod N$
    End for Loop
14. Finally the new pixel block position is prepared.
15. Using random function
1.  Select one pixel block randomly.
2.  Select first 128 bits ,
3.  if it is not 128bits then
4.  Go to step no. (1)
    Else if it is last one and no of bit is less than 128 bit then
    Padding of 0 bit is done to make it as 128.
16. Input a key value of 128 bits.
17. Perform logical operation between Key value and
    image value (128 bit).
18. Perform M-Box operation.
```

19. Repeat process no 16 - 19 till all pixels of images processed.
20. Rearrange all pixels into image form.
21. Resulted image is cipher image.
22. Exit

Steps of M-Box Algorithm

1. Pass 128 bits value as an input in the form of key value.
2. Divide Key (k) into two parts K12 and K21 Separately of 64 bits each.
3. Select K12→ 64 bits & divided into 8-8 bits blocks. Total 8 blocks will be generated. Similarly select K21→ 64 bits & divided into 8-8 bits blocks. Total 8 blocks will be generated.
4. Apply Mix (K12, K21).
5. After Mixing of K12 and K21 with each other total 64 bits will be generated. This will become output of M-Box function.
6. **Exit.**

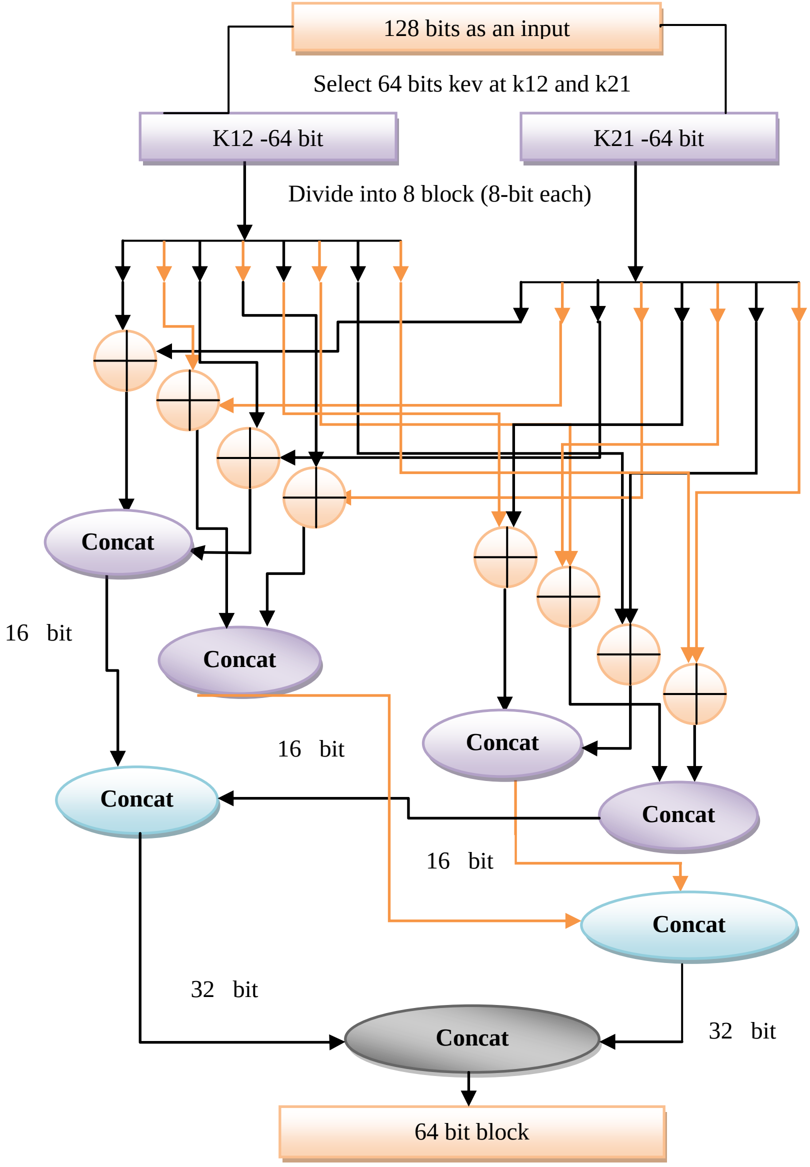
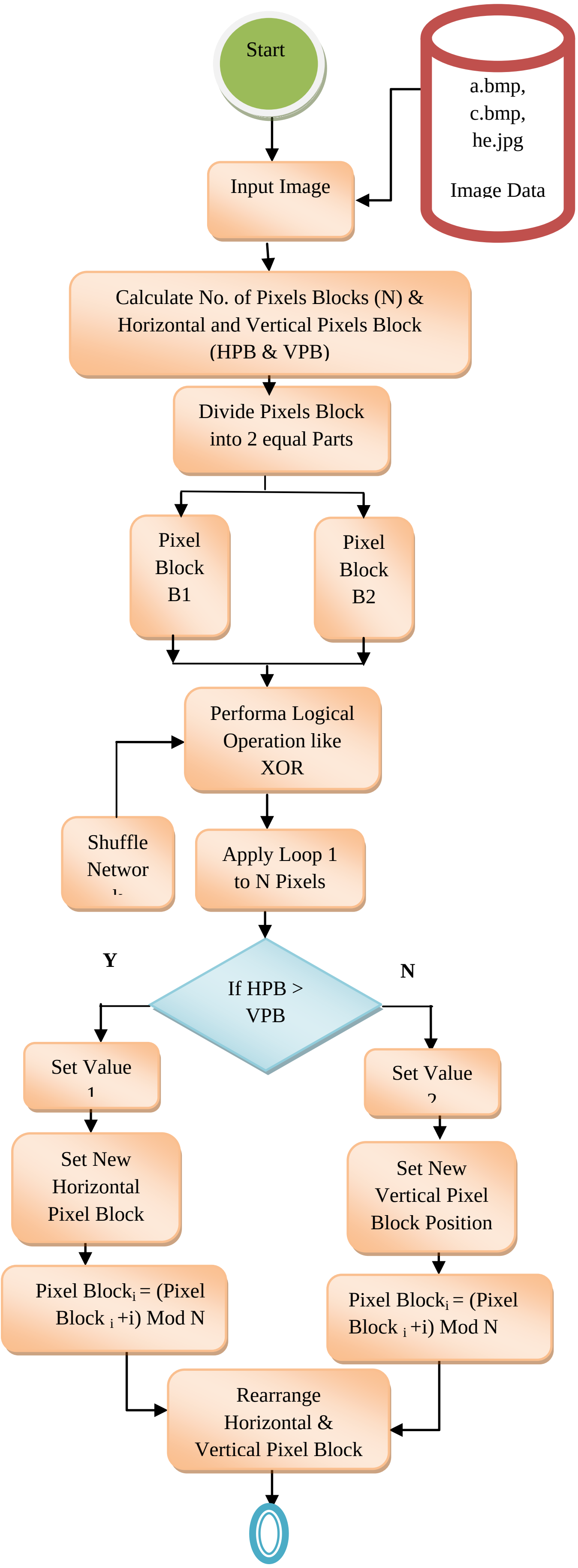


Fig 3: M-Box operation


Start
a.bmp,
c.bmp,
he.jpg
Image Data
Input Image
Calculate No. of Pixels Blocks (N) & Horizontal and Vertical Pixels Block (HPB & VPB)
Divide Pixels Block into 2 equal Parts
Pixel Block B1
Pixel Block B2
Performa Logical Operation like XOR
Shuffle Network
Apply Loop 1 to N Pixels
Y
N
If HPB > VPB
Set Value 1
Set Value 2
Set New Horizontal Pixel Block
Set New Vertical Pixel Block Position
Pixel Block_i = (Pixel Block_i +i) Mod N
Pixel Block_i = (Pixel Block_i +i) Mod N
Rearrange Horizontal & Vertical Pixel Block

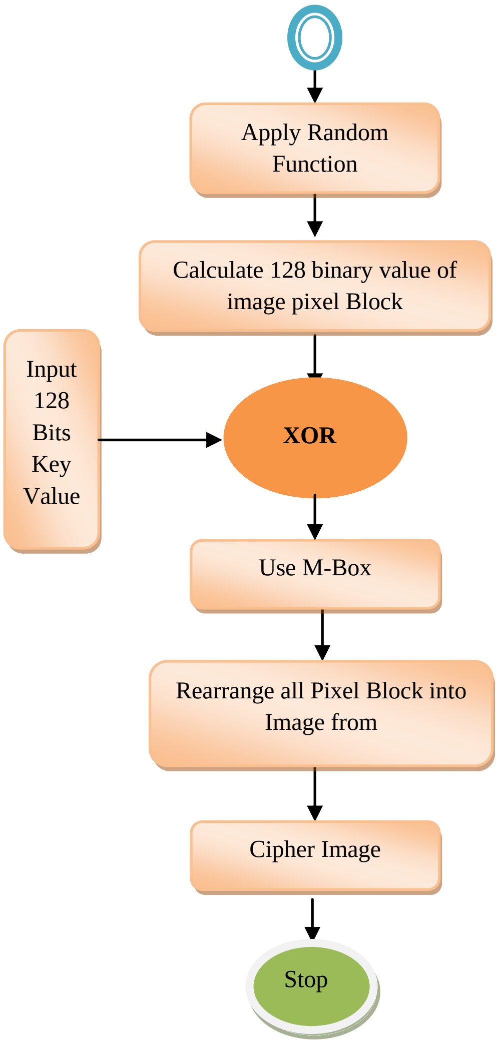

Apply Random Function
Calculate 128 binary value of image pixel Block
Input 128 Bits Key Value
XOR
Use M-Box
Rearrange all Pixel Block into Image from
Cipher Image
Stop

Fig 4: Flow Chart of Proposed Algorithm

To judge our proposed work we have compared BFS, AES and RC6 with our proposed Algorithm (PA) using the parameters[20] like Encryption time, Decryption time, Entropy of cipher image, PUP (Percentage of Unchanged Points), Histogram analysis and correlation coefficient between adjacent pixels (horizontal, vertical and diagonal).
In the following analysis, P = $(p_{i,j})_{MXN}$ expresses the original image with the size of *MXN* , p_{ij} is the gray value of the image pixel *(i,j)*, *C=*$(C_{i,j})_{MXN}$ is the cipher image obtain by encrypting P.

A. Information Entropy Analysis

Information entropy [20][24] is defined to express the degree of uncertainties in the system. The entropy *H* (*x*) of a message source *x* can be calculated as:

$$H(X)=\sum_{i=1}^{n} p(x_i)I(x_i)......................(1)$$

$$H(X)=\sum_{i=1}^{n} p(x_i)\log_b \frac{1}{p(x_i)}...........(2)$$

$$H(X)=-\sum_{i=1}^{n} p(x_i)\log_b p(x_i).........(3)$$

Where p (x_i) represents the probability of symbol x_i and the entropy is expressed in bits. Here *b* is the base of the logarithm used. Common values of *b* are 2, Euler's number e, and 10, and the unit of entropy is bit for *b* = 2, nat for *b* = e, and dit (or digit) for *b* = 10 [12].

C. The percentage of unchanged points

Definition 1: The percentage of the unchanged points of all the pixels in Image P, called the percentage of unchanged points[20][24], expressed by *PUP* (P, C).

$$PUP(P,C)=\frac{\sum_{i=1}^{M}\sum_{i=1}^{N} f(i,j)}{MN}\times 100\%................(4)$$

Where

$$F(i,j)\ =1\ , if\ g_{ij}=c_{ij}$$
$$F(i,j)=0\ , \text{otherwise},$$

C. Correlation of two adjacent pixels

To test the correlation of image P (size of MXN) horizontally, vertically and diagonally, we calculate the correlation coefficient [20][24]of a sequence of adjacent pixels by using the formulas (5), (6), (7), (8),(9) and (10).

$$\operatorname{cov}_{Hor}(P)=\frac{\sum_{i=1}^{M}\sum_{i=1}^{N-1}[p(i,j)-E(P)][P(i,j+1)-E(P)]}{MXN}......(5)$$

$$\operatorname{cov}_{Var}(P)=\frac{\sum_{i=1}^{N}\sum_{j=1}^{M-1}[P(i,j)-E(P)][P(i,j+1)-E(P)]}{MXN}......(6)$$

$$\operatorname{cov}_{Dag}(P)=\frac{\sum_{i=1}^{M-1}\sum_{i=1}^{N-1}[P(i,j)-E(P)][P(i,j+1)-E(P)]}{MXN}.....(7)$$

$$R_{Hor}(P)=\frac{\operatorname{cov}_{Hor}(p)}{D(P)}, R_{Var}(P)=\frac{\operatorname{cov}_{Var}(p)}{D(P)}, R_{Dag}(P)=\frac{\operatorname{cov}_{Dag}(p)}{D(P)}.(8)$$

where

$$E(P)=\frac{\sum_{i=1}^{M}\sum_{i=1}^{N} p(i,j)}{MXN}.................................(9)$$

$$D(P)=\frac{\sum_{i=1}^{M}\sum_{i=1}^{N}[p(i,j)-E(P(i,j)]^2}{MXN}..........(10)$$

D. Histogram analysis:

The desired parameter to prevent the leakage of information to intruders is statistical dissimilarities between encrypted and original images. By use of histogram analysis[20] of image, we exactly visualize the similarities between cipher and original image. Fig. 5 shows the histogram analysis on test image

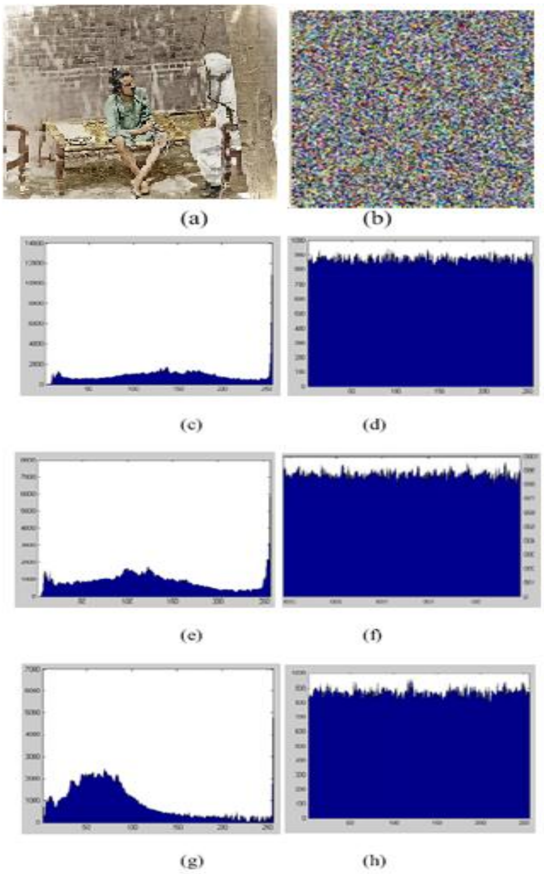


Fig 5: Histogram analysis: Frame (a) shows plain image. Frames (c), (e) and (g) respectively, show the histograms of red, green and blue channels of the plain image shown in figure (a). Frame (b) show the encrypted image of the plain image. Frames (d), (f) and (h) shows the histograms of red, green and blue channels of encrypted image shown in figure (b).

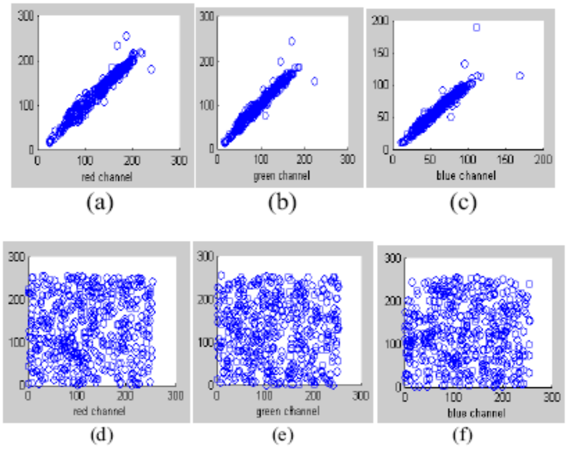


Fig 6: Correlation of two adjacent pixels. Frame (a), (b) and (c) show the distribution of two horizontally, vertically and diagonally adjacent pixels in plain image. Frame (d),(e) and (f) show the distribution of two horizontally vertically and diagonally adjacent pixels in cipher image.

4. RESULTS & DISCUSSION

Following results were achieved while applying the proposed algorithm on the test images. Simulations were carried out on machine with configuration Intel (R) core(TM) 2 Duo Processor, CPU T5550 1.83GHz and 2 GB of RAM.
Here PA stands for Proposed Algorithm.

“Table .1” Entropy of cipher text

File name	BFS	AES	RC6	PA
image01	9	3	3	3
image02	12	4	4	4
image03	15	5	5	5
image04	18	6	6	6
image05	21	7	7	7

Table2. Encryption Time in seconds

File Name	BFS	AES	RC6	PA
image01	916167.1	164447.6	2956401	14782006
image02	2532082	399819.2	2242314	8008265
image03	1469703	201324.9	3767323	10297348
image04	1456919	353547.8	3120106	9840335
image05	2715179	321298.8	5616181	14688473

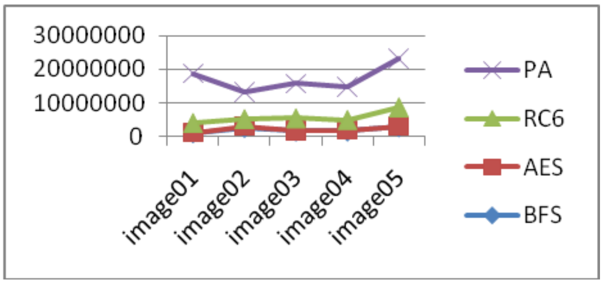


Fig.7: Comparison of Algorithms by Entropy of Cipher Image.

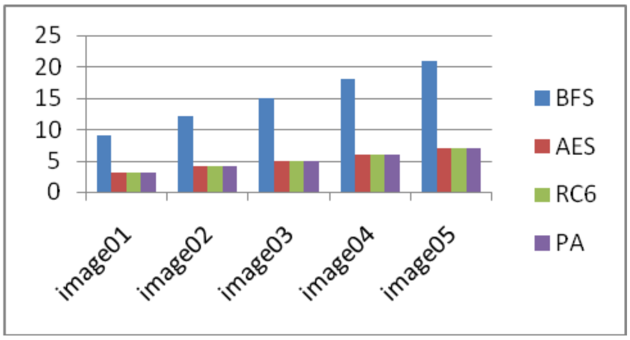


Fig 8: Comparison of Algorithms by Entropy of Cipher image.

The present work is based on the following points:

1. The encryption system should be computationally secure.
2. Encryption and decryption should be fast enough, not to degrade system performance. The algorithm for encryption and decryption must be simple enough to be done by user in personal computer.
3. The security mechanism should be flexible.
4. There should not be a large expansion of encrypted image Data.

As shown in table1 entropy by our proposed algorithm is highest among BFS, AES and RC6. Thus proposed algorithm has an advantage over others while the encryption and decryption time of proposed algorithm is optimal. Figure 6 represents the uniform distribution of adjacent pixels in cipher image as compared to plain text. Similarly it is clear from figure 5 that the cipher image obtained using the proposed algorithm is far different from the original image. As 128 bit key is used to encrypt the image, it is infeasible to breaks by brute force attacks.

5. CONCLUSION

In this paper the both diffusion and confusion operations are performed and taking the advantages of chaotic properties, a modified chaotic encryption scheme for images has been proposed. The encryption procedure employed block based image transformation using shuffle exchange operation to shuffle the pixels of image and M box for chaotic confusion. Experimental results of the proposed technique showed a direct relationship between number of blocks and entropy. When compared to commonly used algorithms, the proposed algorithm resulted in the best performance - highest entropy with the moderate encryption time.

6. REFERENCES

[1] D. Coppersmith, “The data encryption standard(DES) and its strength against attacks,” IBM Journal of Research and Development, pp. 243 -250, May1994.

[2]J. Daemen, and V. Rijmen, “Rijndael: The advanced encryption standard,” Dr. Dobb’s Journal, pp. 137-139, Mar. 2001.

[3]N. E. Fishawy, “Quality of encryption measurement of bitmap images with RC6, MRC6, and rijndael block cipher algorithms,” International Journal of Network Security, pp. 241-251, Nov. 2007.

[4] Hardjono, Security In Wireless LANS And MANS, Artech House Publishers, 2005.

[5] K. Naik, “Software implementation strategies for power-conscious systems,” Mobile Networks and Applications, vol. 6, pp. 291-305, 2001.

[6] P. Ruangchaijatupon, and P. Krishnamurthy, “En- cryption and power consumption in wireless LANs-N,” The Third IEEE Workshop on Wireless LANs, pp. 148-152, Newton, Massachusetts, Sep. 27-28,2001.

[7]B. Schneier, The Blowfish Encryption Algorithm, Retrieved Oct. 25, 2008. (http://www.schneier.com/blowfish.html).

[8] W. Stallings, Cryptography and Network Security, Prentice Hall, pp. 58-309, 4th Ed, 2005.

[9] S. Z. S. Idrus, and S. A. Aljunid, “Performance analysis of encryption algorithms text length size on web browsers,” IJCSNS International Journal of Computer Science and Network Security, vol. 8, no.1, pp.20-25, Jan. 2008.

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

[11] Mohammad Ali Bani Younes and Aman Jantan “Image Encryption Using Block-Based Transformation Algorithm” IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03 Advance online publication: 19 February 2008.

[12] ZHANG Yun-peng, ZHAI Zheng-jun, LIU Wei, NIE Xuan, CAO Shui-ping and DAI Wei-di “Digital Image Encryption Algorithm Based on Chaos and Improved DES” published in Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2009.

[13] Alireza Jolfaei and Abdolrasoul Mirghadri “Survey: Image Encryption Using Salsa20” published in IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 5, September 2010 ISSN (Online): 1694-0814.

[14] Abir AWAD “A New Chaos-Based Cryptosystem for Secure Transmitted Images” published in IEEE TRANSACTIONS ON Computers 2011.

[15] Wenping Guo “A New Digital Image Scrambling Encryption Algorithm Based on Chaotic Sequence” published in IEEE Conferences 2011.

[16] Ling Li, Weinan Wang and Jinjie Li “A Novel Image Encryption Algorithm Based on High-dimensional Compound Chaotic Systems” published in IEEE Conferences 2011.

[17] Panduranga H T and Naveen kumar S K “ Hybrid Approach to Transmit a Secrete Image” published in IEEE Conferences 2011

[18] B.Subramanyan, Vivek.M.Chhabria and T.G.Sankar babu”Image Encryption Based On AES Key Expansion” published in Second IEEE International Conference on Emerging Applications of Information Technology 2011 .

[19] Zhang Yong “Image Encryption with Logistic Map and Cheat Image” published in IEEE Conferences 2011.

[20] Qian Li and Yang Wang “The Performance Analysis of Image Encryption Algorithm Based on Chaotic System” published in IEEE International Conference on Electronic & Mechanical Engineering and Information Technology 12-14 august 2011.

[21]Schneider, T.D, Information theory primer with an appendix on logarithms, National Cancer Institute, 14 April 2007.

[22] Paul A.J, P. Mythili and K. Paulose Jacob”Matrix based Cryptographic Procedure for Efficient Image Encryption” published in IEEE Conferences 2011.

[23] Sun Xin, Yi Kaixiang, Sun Youxian.New Image Encryption Algorithm Based on Chaos System [J]. Journal of Computer-AidedDesign & Computer Graphics, 2002, 14 (2): 136-139.

[24]Wikipedia (www.wikipedia.org).