A New Chaos Based Medical Image Encryption Scheme

Sakib Mostafa, Masud An Nur Islam Fahim, A. B. M. Aowlad Hossain
Khulna University of Engineering & Technology Khulna-9203, Bangladesh
sakibmostafa11@gmail.com, mostofa21fahim@gmail.com, aowlad0403@ece.kuet.ac.bd

***Abstract*— Image encryption has great importance in transmitting images securely for numerous applications taking the advantages of modern communication networks. Due to the era of modern technology medicine sector has updated in dramatic way such as the concept of telemedicine, more specifically the tele radiology services, has raised a great deal of concerns in the security of medical images transmitted over open networks. In order to meet the necessary challenge, a new chaos based encryption scheme is proposed with emphasis on stronger security with variable control parameter facility in a simplistic way. Thorough experimental tests are carried out and the obtained results have shown satisfactory performance which means proposed scheme provides an effective way for online secure medical image transmission over public networks.**

Keywords*— Chaotic encryption; logistic map; pixel position permutation; ciphered image.

I. INTRODUCTION

Communication networks are growing rapidly in today's world and working as the pathway of sharing over trillion bits of information every day in the form of text, image, and video data. Secured transmission of information through communication media is very crucial. Due to the recent advancement in digital image processing and communications facilities, transmission of images has been increased dramatically for various applications.

Different encryption schemes have been developed in order to make the data to be unintelligible other than the intended recipient. Data encryption standard, advanced security standard, RSA, is the widely used existing data encryption algorithms, but they are mainly employed in text or binary data. These encryption standards when applied to images found to be less efficient, because images have larger volume, higher redundancy, higher correlation among pixels compared to text data. Different image encryption techniques have been proposed like as stenography, chaos based encryption, and SCAN based encryption [1]-[4]. Stenography based encryption is based on hiding the original image into another image; also it could be done by hiding image into another types of multimedia files. Chaos based image encryption is based on rearranging image according to the non-linear behavior of different types chaotic equations such Logistic map, Arnold Cat map, Henon map, Standard map. SCAN based encryption works with several patterns which are meant to coordinating the pixels into versatile ways according to SCAN language. This language also provides compressing sensing in particular case also.

Chaotic functions related features like diffusion, confusion and dependence on keys have used to encrypt digital image [5]. However, some flaws have been observed in the chaos based crypto system [6]-[9]. The common flaws of these algorithms are: (i) the control parameters for permutation are fixed in all permutation–diffusion rounds; (ii) in the diffusion stage, the keystream extracted from the chaotic orbit only depends on the key [10]. Scrambling using bit level permutation has been done in some study but this does not sufficient degree of encryption because each bit of any pixel can fall into any other bit position with the equal probability [10]-[12]. Prodessor et al. proposed a scheme which is easy to implement but got less cryptographic strength and less encryption ratio [13]. Bendett et al. proposed a scheme which is XOR based, fast in response but provide less cryptographic security [14]. S. Rao et al. presented a work with strong security, fast but insufficient encryption ratio [15]. Li et al. proposed a technique with formidable security but not practical enough to implement [16].

We plan to develop an image encryption scheme with emphasis on strong security, simple to implement and fast in response. A chaos based logistic map is considered to encrypt pixel value and pixel position of the image. Chaos based algorithm shows fragility due to constant control parameter. Random pixel position may provide an important sequence to the attacker also. And attacker retrieves the whole image or at least portion of it from this sequence by statistical attack. That's why we have maintained our pixel shuffling algorithm in such a way that could cure this problem. Also another angle for looking at this work is by looking at the output. This step by step work provides a new scheme is suitable enough to provide a complete unknown look which makes it different from the rest of the work. If we look at the previous work at this sector, we can see an output with complex random pattern or masked distribution of pixels. Unlike others, this work has introduced a new way to represent the image which is completely dark and it is impossible to make any guess by looking at it or make an impact by applying statistical attack.

This paper is organized as follows. The methodology section describes the ins and outs of our encryption and decryption proposal. The security issues are analyzed in the security analysis section. This section consists of differential attack analysis, key space analysis, histogram analysis, and pixel value correlation analysis. Finally the findings of this study are discussed and conclusion has been drawn.

978-1-5386-1023-7/17/$31.00 ©2017 IEEE

II. METHODOLOGY

Our proposed image encryption scheme has two major functioning steps: pixel value encryption and pixel position encryption. Pixel value encryption is used for hiding the original pixel value in order to prevent unwanted authorization. This is done by XOR operation, frequency domain base analysis and spatial domain based analysis. For pixel value encryption, we generate similar number of random pixels compared to original image. Another set of pixels from random pixels is generated by shifting the first set and XOR operation is performed between them to produce secret key to use it to encrypt the image primarily. The primary ciphered image is then subtracted by a pseudo image which is created alongside the original image based on prime pixels for final pixel value encryption.

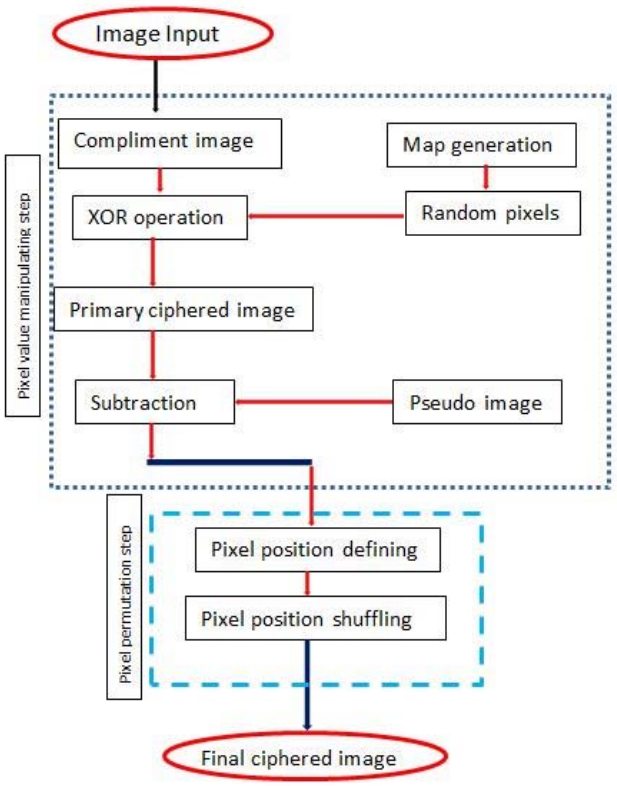

Fig. 1. Flowchart of proposed scheme

The pixel position encryption techniques usually rearrange the pixel position using matrix transformation or SCAN language. In proposed scheme, we shift the pixel position in such a way that least amount correlation is maintained between consecutive pixels with less computation. The flowchart of proposed work is shown in Fig. 1.

A. Value Encryption Technique

The steps of the pixel value encryption technique are described below:

1. Firstly the original input image p(M×N) is converted into its complimented version p.

2. The chaotic logistic map is formed generating random values to achieve the goal of image encryption using the equation below:

$$X_{n+1} = \mu X_n[1 - X_n];$$

Where X_{n+1} is the sequence of the chaotic chain and μ is the controlling parameter which is ranging as [0,4] and X(n) is the just the initial value within range of X_n =[0,1].

Now for selecting the initial value we will use skew tent map. The skew tent map is as follows:

$$X_{n+1} = \frac{X_n}{p}, \text{ if } X_n \in [0, p]$$

Or,

$$X_{n+1} = \frac{(1 - X_n)}{1 - p}, \text{ if } X_n \in (p,1]$$

Here P ∈ [0, .99]. Using this we will determine the value of initial parameter X_n. This parameter is dependent on previous value; that's why this method is been chosen because in later several values have been implemented in order find effect of correlation and keyspace analysis.

3. From the logistic map generating values will be M×N in number. And this map is then converted into pixel intensity like values by multiplying with 255.This sequence will be count as S1.

4. Then each element of set S1 converted into binary and applying 2-bit shifting operation a second set S2 is generated.

5. Finally, the key set is obtained executing of XOR operation between S1 and S2.

6. This key stream will be used to encrypt the pixels of the images

7. A pseudo image is then generated which is consists of nearest prime pixels comparing with the primary encrypted image. Pseudo image is another key.

8. Substitution operation between primary encrypted image and pseudo image is been performed.

In this value manipulation method bit shifting has done in order to doping the values of logistic map and then XOR have done in order to encrypt the pixel value which is more likely a conventional fashion.

B. Pixel Position Encryption Technique

After manipulating the pixels value, pixel position encryption next emphasis of our proposed scheme. Though, numerous amount of algorithm is available to do this operation, its efficiency depends on its computational complexity. For pixel position encryption, we plan to reorganize the pixel positions introducing least correlation

between neighboring pixels emphasizing on less complexity. The strategy is that a fixed number of pixels are taken as 1D segment keeping their order and being continued to cover the entire image. In this study, the segment length is considered as 10. Then the segments are reorganized to encrypt the pixel position as follows:

1. Defining pixel positions P_k where *k*=0 to9
2. Find C= mod (A, B); Where A= M×N, B=10.
3. Find E=$\frac{D}{B}$; D = (A-C).
4. Update the pixel position as P_j (i+1) =B+ P_j (i);
5. Where, i = 0 to E;
a. j = 0 to 9;
6. If P_j (i+1) >M×N; operation will be stop.
7. Now converting the image into 1D array **A** and segment it into 10 sub 1D arrays with size of 1×(E/10) , assume they are $A_0[], A_1[], A_2[], A_3[], A_4[], A_5[], A_6[], A_7[], A_8[], A_9[]$.
8. Now we will rearrange the segments into the parent array to encrypt its pixel position as: A [$A_1[], A_9[], A_2[], A_8[], A_3[], A_7[], A_4[], A_6[], A_5[], A_0[]$]; Where, $A[p_i, p_{(k+10)}, p_{(k+20)}]$.

C. Decryption Technique

To decrypt the image pixel position first, the received final ciphered image is converted into an array of pixel data which were encrypted. This parent array will be segmented into 10 arrays according to encryption algorithm as: B [$B_0[], B_1[], B_2[], B_3[], B_4[], B_5[], B_6[], B_7[], B_8[], B_9[]$]. Every first pixel of each segment will be taken from them and will be saved in another set of temporary segments. This procedure will be continuing sequentially and it's obvious that each temporary cluster will be full of E elements. Then these temporary cluster set will be convert into a parent array of pixels. This could be shown as: $T_0[p_0, p_1, p_2, \ldots\ldots\ldots p_{(M\times N)}]$. This array is the image where each pixel value is encrypted and they maintain same pixel position compared to the original image.

The above parent array will be needed to decrypt image with respect to pixel value. This is done by the XOR operation between the secret key and the pixel value of encrypted image.

III. RESULT SNALYSIS AND DISCUSSION

We have used the popular Skull and Brain images to test the algorithm. The original images along with cipher images and the reconstructed images are shown in Fig. 2. An image encryption scheme is said to be good if the algorithm is sensitive to its secret key i.e. the change of a single bit in algorithm should produce a new cipher image. For analyzing the key sensitivity part, the control parameters are modified. Originally μ=0.212 was achieved from skew tent map but later 0.221, 0.911, 0.496 was defined as the set value for testing. Resultant images of Fig. 2 are significantly different from each other not only visually but also in inheriting values. Clearly it is quite difficult to analyze them by simply observing and that's why respective correlation analysis has been performed in order to ensure the authenticity of the key sensitivity. Fig. 3 shows the image analysis for key sensitivity where we have used variable control parameters.

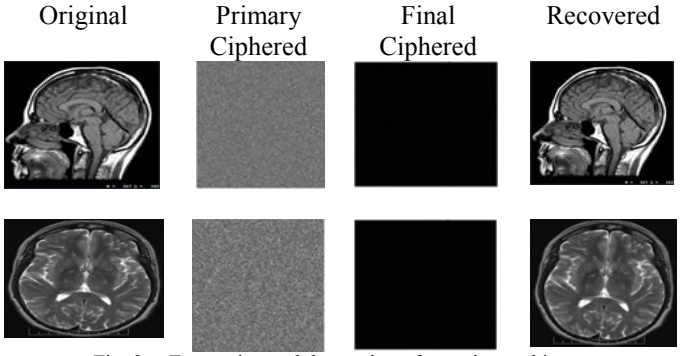

Fig. 2. Encryption and decryption of experimental images.

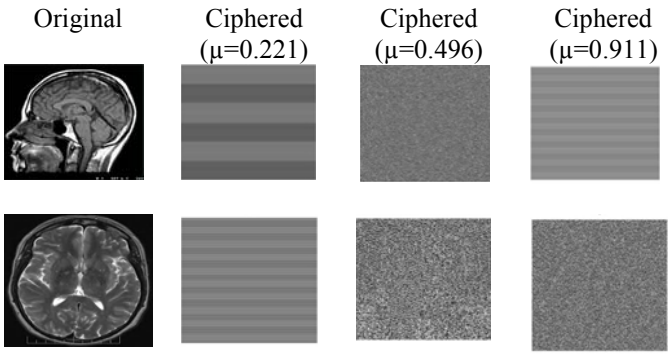

Fig. 3. Encryption using different control parameters for primary steps.

A. Keyspace Analysis

An image encryption scheme is considered to be strong enough to resist the brute force attack if it inherits the key length more than 2100. In our proposed scheme, it has been observed that same image with different control parameter value has shown 99.1% of value degradation from each other. For changing one or all of controlling parameter the obtained encrypted figures are totally different from the previous value. Therefore, the encryption is significantly sensitivity to its key. We have performed several analyses for the original image using variable control parameter and our obtained result is individual for each set of parameters. This ensures the key sensitivity of our presented scheme. Since we have used 128 bits encryption scheme, our total key space is equal to 3.4208×1038×1032×(M×N)256. As the attacker needs to run this amount of operations, breaking is practically infeasible [17].

TABLE I. KEY SPACE OF DIFFERENT ENCRYPTION SCHEME

Encryption Schemes	Key space
Guan et al.[3]	10^{42}
Chen et al.[7]	2^{138}
Anusudha et al.[19]	2^{120}
Proposed	$3.4208\times10^{38}\times10^{32}\times(M\times N)^{256}$

B. *Statistical Analysis*

Claude Elwood Shannon stated that it is possible to solve different kind of ciphers by statistical analysis [18] and it was clear in his suggestion that we can use confusion and diffusion in order to deceive the power attacker based on statistical analysis. This analysis has been performed on the image for demonstrating the superiority of encrypted image. This is shown by analyzing a test upon the histograms of the enciphered images and on the correlations of adjacent pixels in the ciphered image.

Fig. 4 and 5 shows the histogram of the original image and the ciphered image of skull and brain respectively and they are different from each other as expected.

Histogram of original image Histogram of ciphered image

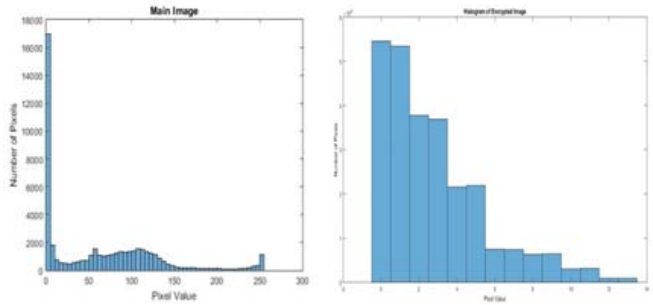

Fig. 4. Histogram of original and ciphered image of Skull

Histogram of original image Histogram of ciphered image

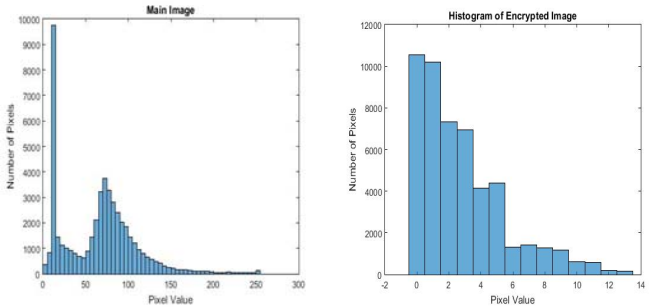

Fig. 5. Histogram of original and ciphered image of Brain.

A useful metric to assess the encryption quality of any image cryptosystem is the correlation coefficient between pixels at the same indices in the plain and the cipher images. For this we have to perform the following formula:

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \quad (1)$$

Where x and y are grey-scale values of two adjacent pixels in the image and cov(x,y)= E(x-E(x))(y-E(y)). And for variance $D(X) = 1/N \sum_{i=1}^{N} (x_i - E(x))^2$.

We have calculated the horizontal, vertical, and diagonal correlation considering the pixel positions (x, y) in respective directions. Table II show the correlation coefficients for different images for the proposed algorithm. The range of correlation value is between -1 to +1. 1 or nearer values means strong linearity in the relationship and -1 or nearer value indicates strong distant relationship between the pixels. For original image the correlation coefficients are nearly 1 for both skull and brain image. It has been noticeably observed that, in the case of ciphered image values are far away from 1 even in maximum case it is negative value which is desired for enhanced security against the brute force attack or differential attack. As the correlation is going down for ciphered image, the proposed scheme can ensure strong encryption.

TABLE II. CORRELATION COEFFICIENTS FOR DIFFERENT IMAGES

Images/Direction	Skull		Brain	
	Original	Ciphered	Original	Ciphered
Horizontal	0.9703	-0.00078	0.8455	0.0002
Vertical	0.988	-0.00196	0.8142	0.0001
Diagonal	0.963	0.0026	0.9465	0.0002

C. *Correlation Analysis*

We have plotted the pixel values on location (x, y) vs. (x,y+1) to compare the correlation between pixel positions of original and ciphered images. From the graphical analysis, it is clear that pixels are way distant in the ciphered image comparing to the original image for Fig. 6 and 7.

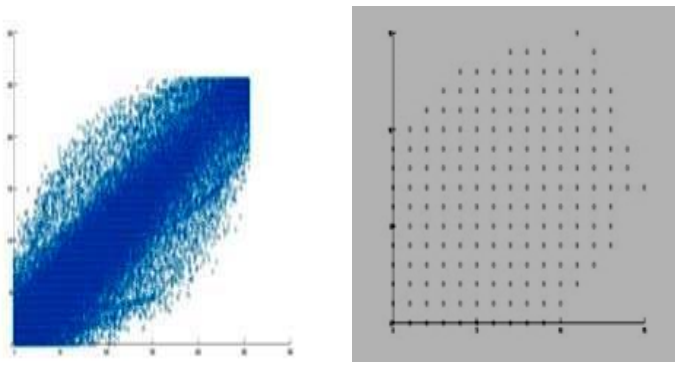

Fig. 6. Pixel value location on (x, y) vs (x, y+1) of original and ciphered images for Skull image.

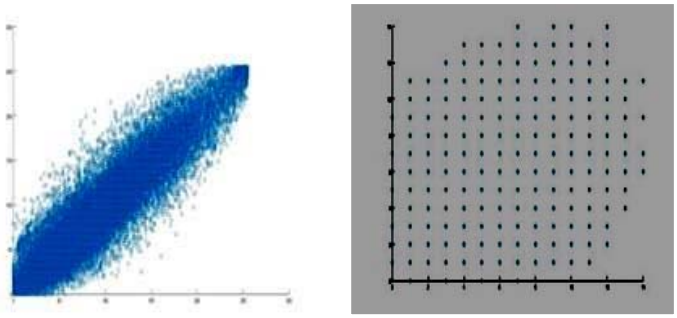

Fig. 7. Pixel value location on (x, y) vs (x, y+1) of original and ciphered images for Brain image.

D. Differential Attack Analysis

Aim of this type attack is to find out the secret key which has been used to encrypt the image. An encryption scheme how much strong against this type of attack can be measured by performing NPCR which stands for Number of Pixel Change Ratio. NPCR used to perform the test for finding out pixel changing influence over the encrypted image [19]. The NPCR is defined as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\ \% \qquad (2)$$

Where the D is a binary matrix with size M×N and its element value will be 1 only where the pixel of original image is not matched with the corresponding pixel of ciphered image. NPCR measures percentage pixel difference in two images. UACI is defined as follows:

$$UACI = \frac{1}{M \times N}[\sum_{i,j} \frac{c_1(i,j) - c_2(i.j)}{255}] \times 100\,\% \qquad (3)$$

Table II shows the calculated NPCR and UACI for both Skull and brain images. As our algorithm encrypt each pixel separately NPCR are as high as 99.99% for both the images. Also the UACI are close to 0 which is desirable.

Table III shows the calculated NPCR for both Skull and brain images.

TABLE III. CALCULATED NPCR FOR ENCRYPTED IMAGES

IMAGES	UACI	NPCR
Skull	99.99%	4.87×10^{-7}
Brain	99.99%	2.49×10^{-7}

E. Time vs content size Analysis

One of the remarkable features of this study is its dealing with the computation time in comprehensive manner. Due to its functioning capacity, it deals with the image by considering it as a set of numbers and then computes the necessary information and point to be noted that, for this purpose we have used an average machine with core-i5 processor and 4 GB ram. Now, the algorithm definitely publish different amount of time for different set of images but none of them exceeds not more than 14 seconds even for a 1024x1024 image. Following graphical representation will be sufficient for representing the summary of the time vs size relationship.

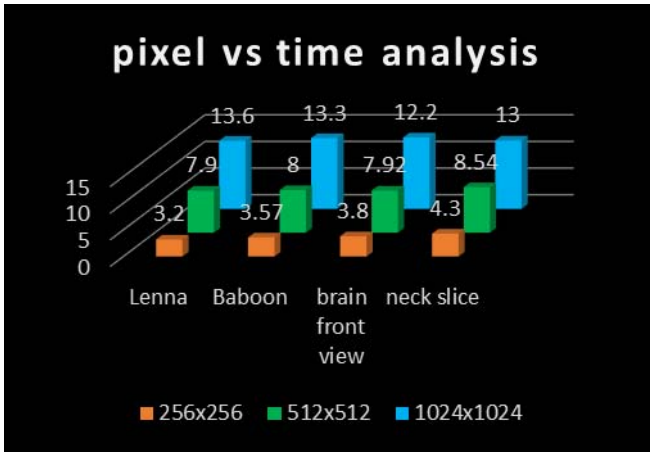

Fig. 8. Pixel value location on (x, y) vs (x, y+1) of original and ciphered images for Brain image.

IV. CONCLUSION

In this paper, a logistic map based image encryption scheme has been presented. The algorithm uses variable control in order to produce the secret key. Also pixel permutation has been done in such a way that minimum distance between each pixel is 10. After performing several tests it shows good response comparing to other complex algorithms based on similar chaotic maps. We have founded that algorithm provides stronger security as well as key sensitivity and presence of randomness comparing to other two dimensional chaotic maps. The algorithm is simple enough for practical implementation keeping satisfactory robustness.

REFERENCES

[1] D. R. Bull and D. W. Redmil, "Optimization of image coding algorithms and architectures using genetic algorithms ," IEEE Trans. on Industrial Electronics, vol. 43, pp. 549-558, 1996

[2] N. A. Flayh and S. I. Ahson, "Wavelet based image encryption," in Proceedings of 9th International Conference on Signal Processing, pp. 797-800, 2008.

[3] Z. H. Guan, F. J. Huang, and W. J. Guan, "Chaos-based image encryption algorithm," Physics Letters A, vol. 346, pp. 153-157, 2005.

[4] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, vol. 24, pp. 926-934, 2006.

[5] X. M. Li and Lin Dai, "A Novel Approach for Double Image Encryption" in Proceedings of IEEE Region 10 Conference, pp. 697-701, 2010.

[6] A. Meghdad; M. B Parmida, and M. H. Hesam,"Chaos-Based Medical Image Encryption Using Symmetric Cryptography," in Proceedings of International Conference on Information and Communication Technologies: From Theory to Applications, 2008.

[7] G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat Maps,” Chaos, Solitons & Fractals, vol. 21, pp. 749–761, July 2004.

[8] R. Rhouma and B. Safy “Cryptanalysis of a new image encryption algorithm based on hyper-chaos” Physics Letters A, vol. 372, pp. 5973-5978, 2008.

[9] L. Wang, Q. Ye and Y.Q. Xiao, "An image encryption scheme based on cross chaotic map", in Proceedings of Congress on Image and Signal Processing, pp. 22-26, 2008.

[10] G. Ye “Image scrambling encryption algorithm of pixel bit based on chaos map,” Pattern Recognition Letters, vol. 31, no. 5, pp. 347-354, 2010.

[11] C. Fu and Z. Zhu.“A chaotic image encryption scheme based on circular bit shift method.” in Proceedings of 9th International Conference for Young Computer Scientists, pp. 3057 –3061.

[12] C. A. O. G-.hui, H. Kai, Y. He, and E. Xu; “Algorithm of image encryption based on permutation information entropy,” in Proceedings of Computer Science & Information Tech, vol. 53, pp. 102.

[13] M. Podesser, H. P. Schmidt, and A. Uhl, “Selective Bit plane Encryption for Secure Transmission of Image Data in Mobile Environments,” in Proceedings of the 5th Nordic Signal Processing Symposium, 2002.

[14] M. V. Droogenbroeck and R. Benedett, “Techniques for selective encryption of uncompressed and compressed images”, in Proceedings of Advanced Concepts for Intelligent Vision Systems, pp. 90-97, 2002.

[15] Y. V. S. Rao, A. Mitra, and S. R. M. Prasanna, “A Partial Image Encryption Method with Pseudo Random Sequences”, in Proceedings of International Conference on Information System Security, pp. 315-325, 2006.

[16] H. Cheng and X. Li, “Partial Encryption of Compressed Images and Videos,” IEEE Transaction on Signal Processing, vol. 48, vo. 8, pp. 2439-2451, 2000.

[17] E.-Samie, H. Ahmed, F. Elashry, O. S. Faragallah, and S. A. Alshebeili. Image Encryption: A Communication Based Perspective, CRC Press, 2013.

[18] C. E. Shannon, “A mathematical theory of communication,” Bell System Technical Journal, vol. 27, pp. 379–423, 1948.

[19] M. R. Saranya, A. K Mohan, K Anusudha, “A hybrid algorithm for enhanced image security using chaos and DNA theory,” in Proceedings of Computer Communication and Informatics, 2012.