Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique

Nidhi Sethi
Assistant Professor
Dehradun Institute of Technology
Dehradun-248001
nidhipankaj.sethi102@gmail.com

Sandip Vijay
Professor & Head (ECE)
Dehradun Institute of Technology
Dehradun-248001
vijaysandip@gmail.com

Abstract
Several traditional encryption schemes have been analysed and based on the literature survey, it has been found that chaotic sequences are very much useful to create randomness. In this paper, a new encryption scheme has been proposed with two phases. In the first phase the input image is transformed using a new transformation technique whereas in the second phase .Chirikov Standard Map is used for pixel shuffling and modified Logistic Map is used for diffusion. Chirikov standard map , decor relate the strong relationship among adjacent pixels hence employed to shuffle the pixel positions of the plain image. The modified logistic map is used for generating the random sequence which is completed the purpose of changing pixel values. Various images and standard lena image is used to demonstrate the validity of the proposed algorithm. The results of experiments show that the proposed algorithm for image cryptosystems provides a no correlation between the original image and cipher image. The scheme is key sensitive and shows impressive resistance against brute force attack and statistical attack.

Keywords
Image encryption, , Chirikov Standard Map,1D Logistic Map

1. Introduction

There are many existing encryption algorithms which are secure and take less time in execution. But most of the algorithms have used I D or 2 D chaotic sequences to complicate the encryption process, since the chaotic sequence greatly depends on the initial condition.

Image transforms are very important in digital processing they allow to accomplish less with more. For example the Fourier Transform may be used to effectively compute convolutions of images1 or the Discrete Cosine Transform may be used to significantly decrease space occupied by images without noticeable quality loss. So ,a new transform has been introduced in the proposed scheme. In the second stage modified logistic map is used to to exhibit the chaotic behaviour . The modified logistic map is a polynomial mapping (equivalently, recurrence relation) of degree 2, often seen as an archetypal example of how complex, chaotic behaviour can arise from very simple non-linear dynamical equations.

Here in this proposed work in which the plain image is first subjected to a new transformation technique .In second stage the transformed image is shuffled using chirikov map. The chirikov maps aims at shuffling of the pixels randomly. The shuffled image is divided into

blocks. After this division the blocked image is XORed with the random chaotic sequence. Finally the shuffled image's pixel intensity is changed using logistic mapping. The proposed algorithm is tested for several images and the results are given in the experimental results section.

2. Literature Review

Information security is the hot topic of research for decades to deal the prevailing security requirements. Traditional encryption schemes such as DES,,T-Des , AES are not suited to build the cryptosystem for digital images , this is due to the inherent features of the images and high redundancy. P.Raviraj et.al [1] have proposed a new modified haar wavelet transform which have improved the PSNR and MSE results. J. M. Blackedge et al. [2] have proposed a multilevel blocks scrambling is employed to scramble the blocks of coefficients which requires high computation. The control parameters of the scrambling are randomly generated from the secret key dependent. The key stream used to encrypt the scrambled image is extracted from the chaotic map and plain image.

Musher Ahmed et.al[5] have used the combination of Arnold cat map with 1 D logistic map and 2 D logistic map. Ahmed T[9] propose a novel Steganographic method for hiding information within the spatial domain of the gray scale image. The proposed approach works by dividing the cover into blocks of equal sizes and then embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel.

W Puech et al. [10] have explained and reviewed the security, performance and reliability issues , in respect to the combination of various chaos based symmetric key cryptosystems. Logistic, Henon , Tent , Cubic and Cheyshev mappings have been used for the enhancement of the key space. Chengqing Li et al. [11] , have reviewed four chaos based image encryption schemes were proposed .Essentially, the four schemes can be classified as one class , which composed of two basic parts :permutation and diffusion of pixel value with ciphertext feedback function. Hence many security problems were found like the schemes are not sensitive to change of plain-image, the schemes are not sensitive to change of secret key,there exist a serious flaws of diffusion function, the schemes can be broken with no more than $[\log_l(MN)+3]$ chosen images when iteration number is equal to one, where MN is dimension of image. Chong Fu et.al [15] have used , Chirikov standard map , to decor relate the strong relationship among adjacent pixels hence employed to shuffle the pixel positions of the plain image. After the decor relating the pixels , the pixel values are modified sequentially to confuse the relationship between cipher image and plain image.

3. Encryption using the Haar Wavelet transform and Logistic Map

The proposed image encryption algorithm has two major steps: Transformation and Encryption. Firstly, the transformation has been done using Modified Fast Haar Wavelet transform. The transformation calculates the average and difference of adjacent pixels and also dividing the average and difference by sqrt(2).The same operation is applied both for row and column alternatively. The number of iterations is **three** in this case.

By applying the Haar wavelet transform we can represent the image in terms of a low-resolution image and a set of detail coefficients The detail coefficients are used in reconstruction of the image. Then the transformed image is diffused using Chirikov map. To achieve better decor relation among the adjacent pixels , a block based image shuffling scheme is proposed using crossover techniques of genetic algorithm. Then the pixel values of the shuffled image are encrypted by applying a 1 D Logistic map. The control parameters are chosen by the users which are the secret keys. Here number of keys are 5.

4. Encryption using the Modified Fast Haar Wavelet transform and Logistic Map

The proposed image encryption algorithm also has two major steps: Transformation and Encryption. Firstly, the transformation has been done using Haar Wavelet transform. The transformation calculates the average and difference of four adjacent pixels and also dividing the average and difference by 4.The same operation is applied both for row and column alternatively. The numbers of iterations are **three** in this case.

By applying the Modified Fast Haar wavelet transform we can represent the image in terms of a low-resolution image and a set of detail coefficients The detail coefficients are used in reconstruction of the image. Then the transformed image is diffused using Chirikov map. To achieve better decor relation among the adjacent pixels , a block based image shuffling scheme is proposed using crossover techniques of genetic algorithm. Then the pixel values of the shuffled image are encrypted by applying a 1 D Logistic map. The control parameters are chosen by the users which are the secret keys. Here number of keys are 5.

5. Proposed Algorithm

5.1 New Transformation

To calculate the new transform of an array of *n* samples:

1. Find the average of each consecutive pair of samples. (*n*/2 averages)
2. Find the difference of each consecutive pair of samples. (*n*/2 differences)
3. Fill the first half of the array with averages.
4. Fill the second half of the array with differences.
5. Repeat the alternatively for row and for column.
6. Repeat the above steps for reduced averaged part.
   (The array length should be a power of two)

5.2 Chirikov Map

Chirikov Map is an invertible area preserving chaotic map for two canonical dynamical variables (x,y). It is described by the equation:

$$X_{n+1=}(X_n + Y_n) \bmod N \ldots\ldots (1)$$

$$Y_{n+1=}(Y_n + K\sin 2\pi X_{n+1}/N) \bmod N \ldots\ldots (2)$$

K is dimensionless parameter that influences the degree of chaos. The value of K can be used as a secret key for confusion , N XN is the size of the image. Because of the simple mathematical operation , it is very efficient to shuffle the pixels of the plain image using this map.

5.3 Modified Logistic Map

The 1D logistic map is discrete time analogue of population growth model. It is a non-linear chaotic discrete system that shows random behavior. The equation of modified logistic map is below:

$$X_{n+1}=\lambda\ X_n(1-\ X_n)*X_n\hat{}2 \ldots\ldots\ldots\ldots (3)$$

Where X_n is the intial value which is used as a secret key in this algorithm , λ is the control parameter which affects the randomness and n is the number of rounds .As the value of the λ increases the randomness(number of periods) increases .λ lies in the range [3,4].The sequence formed by the 1D logistic map is used for diffusion in the encryption process.

The proposed image encryption algorithm has three major steps. Firstly , the image is transformed using new technique , which has shown better results than Haar wavelet transform and modified fast haar wavelet transform .Secondly, the correlation among the adjacent pixels is disturbed completely as the image data have strong correlations among adjacent pixels. For image security and secrecy, one has to disturb this correlation. This correlation has been disturbed by Chirikov Standard map. The control parameters of chirikov map are the control parameters of confusion. After changing the pixel position, a block based image shuffling scheme is used . Then the pixel values of the shuffled image are encrypted by employing a modified 1 D Logistic map. The control parameters of modified logistic map are the control parameters of permutation. The shuffling effect obtained after a number of iterations depends on these parameters. In the algorithm, these control parameters are randomly generated through the chaotic sequences obtained from modified 1D Logistic map and Chirikov standard map.

Extraction, Decompression and Decryption : Using the above algorithm in reverse order , the original image can be retrieved .

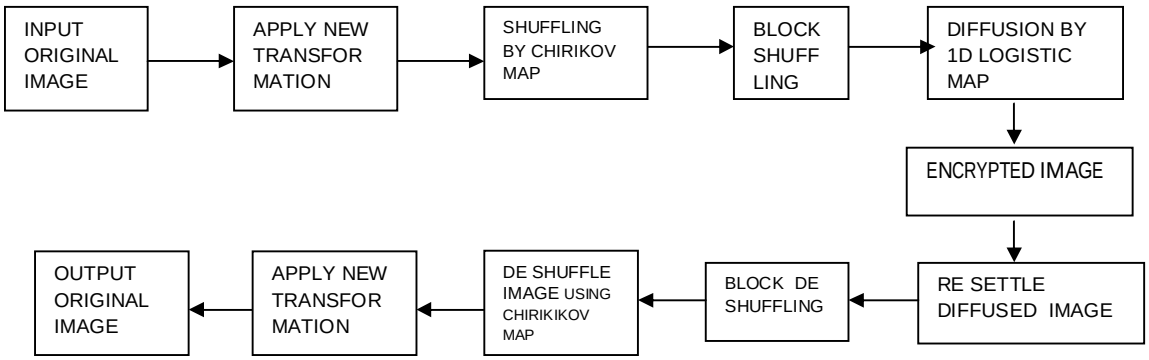

Fig 1: Block Diagram of the proposed algorithm

6. RESULTS AND ANALYSIS

We can see from the results table that by changing the transform and modifying the 1 D Logistic map there is considerable changes in the results. The change result are towards better side since PSNR is reduced and MSE is increased It was found for lena image that PSNR is 22.8% and 4.3% lower than the two methods respectively .It is said that lower is the PSNR better is the encryption scheme. Similarly the MSE is also 60% and 9% higher than both the methods respectively..

We can see that for the image BK there is not much difference in the values, because the image was high contrast , whereas the image of Lena and baba has better changes due to the smooth color contrast .

Total number of Keys: 05;

Key1: A unique number used as initial vector for Chirikov mapping **Key2**: A unique number for number of iterations the map will shuffle. **Key 3**: Fed to random number generator for further **Key 4:** Initial parameter for logistic mapping ; **Key 4**: lemda:(3<key3<4)

7. Experimental Results

The proposed algorithm is compared with Haar wavelet transform and Modified fast haar wavelet transform. The comparative study is shown for the image of Lena in the Table 1. We can see the results are better than the previous transformations as they are compared on the basis of PSNR, MSE ,MAE, correlation among pixels and entropy. The Table 2 shows the results of proposed algorithm for image of baba.

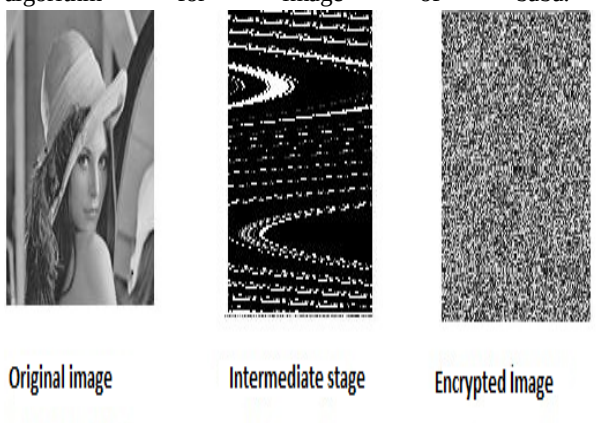

Fig:2 Image after and before encryption

7.1 Key Analysis:

7.1.1 Key Sensitivity **:**A good cryptosystem should be sensitive to a small change in secret keys i.e. a small change in secret keys in decryption process may results into a completely different output image. Our proposed encryption algorithm is sensitive to a very small change in the secret keys. If we change a little ($10^{-14)}$ in any of the initial conditions then the decrypted image is completely different and in un-understandable form

7.1.2 Key Space : Key space is the total number of different keys that can be used in the cryptographic system .A cryptographic system should be sensitive to all secret keys. There are total four initial conditions , 2 of Chirikov map and two of logistic map used in the algorithm .All these four intial conditions are used as secret keys of encryption and decryption. In this situation, the precision of each key is 10^{-14}, the key space size is $(10^{14)8}$ i.e. 10^{112}, which is extensively large enough to resist the exhaustive attack.

7.2 Statistical Analysis:

Many attacks can be done which are based on the statistical analysis .Statistical analysis has been performed on the test images to demonstrate the bad correlation among the pixels of the encrypted images. The following test have been performed like PSNR , MSE , MAE ,information entropy and Correlation coefficient. The results shown below shows that there is negligible correlation between pixels of the encrypted image in comparison to original image.

7.2.1 Mean Squared Error is the average squared difference between original input image and a encrypted image. It is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total number of pixel .

7.2.2 Peak Signal-to-Noise Ratio is the ratio between the original image and the encrypted image. PSNR is calculated in decibels. The higher the PSNR, the closer the encrypted image is to the original. In general, a higher PSNR value should correlate to a higher quality image. For good encryption scheme the PSNR should be as low as possible.

7.2.3 MAE is the Mean absolute error. It is used to measure how close predictions are to the eventual outcomes. The larger the value of MAE better is the image security.

7.2.4 Correlation Coefficient Analysis: To estimate the encryption quality of the proposed encryption algorithm , the correlation is used .For highly correlated image the correlation coefficients are almost 1 and for encrypted images the correlation coefficients is almost 0.

7.2.5 Information Entropy:Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon [14]. Information entropy is defined to express the degree of uncertainties in the system. It is well known that the entropy $H(m)$ of a message source m can be calculated as:

$$H(s)=-SUM(p(s_i)\log_2 p(s_i))$$

Table 1: Results for the image of Lena

	New transformation	M.FHWT	HWT
PSNR	46.9425	51.237	69.7082
MSE	1.3147	0.4888	0.007
Entrropy(O)	0.8634	0.8634	0.8634
Entrropy(E)	7.9882	7.9872	7.9891
Correlation	-0.00027	0.003	-0.00173
MAE	126.81	79.4894	53.67

Table 2: Results for the image of Baba

	New transformation	M.FHWT	HWT
PSNR	46.896	50.093	46.759
MSE	1.3287	0.6	1.3712
Entrropy(O)	1.291	1.291	1.291
Entrropy(E)	7.9896	7.9897	7.9888
Correlation	-0.0164	-0.0082	0.0063
MAE	127.5	83.5197	129.2

Table 3: Results for the image of BK

	New transformation	M.FHWT	HWT
PSNR	46.999	48.9612	46.683
MSE	1.3214	0.825	1.399
Entrropy(O)	1.314	1.314	1.314
Entrropy(E)	7.9874	7.9882	7.9878
Correlation	0.0026	0.008	0.007
MAE	127.261	95.96	129.17

8. CONCLUSION

A new chaotic digital image encryption scheme using five secret keys of 144-bit size is proposed. Proposed algorithm has two phases one to transform the plain image and other ro actually encrypt the transformed image which incorporate both pixel substitution as well as pixel permutation process .In the substitution process, sub-block pixels value is modified which depends on used secret key and random sequence generated by modified logistic map. In permutation process, pixels position is reshuffled within sub-image by using key.

The proposed algorithm is compared with two methods first the combination haar wavelet transformed with logistic mapping and second is the combination fast haar wavelet transform with logistic mapping and tested on the standard lena image and other images. It was found for lena image that PSNR is 22.8% lower 4.3% lower than the two methods respectively .It is said that lower is the PSNR better is the encryption scheme. Similarly the MSE is also 60% and 9% higher than both the methods respectively. The other results are also depicted in the table 1. Thus , we concluded that the algorithm is resistant to statistical attacks and brute force attack. The resistance to chosen plain text and chosen cipher text is still under process.

9. REFERENCES

[1] P Raviraj and M.Y. Sanavullah, (2007) "The modified 2D-Haar Wavelet Transformation in image compression" Middle East Journal of Scientific Research, Vol: 2 , Issue: 2,pp 73-78,ISSN 1990-9233.

[2] Jonathan M.Blackedge,Musheer Ahmed ,Omar Farooq(2010) "Chaiotic image encryption algorithm based on frequency domain scrambling" ,School of Electrical Engineering systems Articles,Dublin Institute of Technology.

[3] G. K. Kharate, A. A. Ghatol and P.P.Rege, (2005) "Image Compression Using Wavelet Packet Tree", ICGST-GVIP Journal, Volume Issue (7).

[4] David F. Walnut, ,(2002) "Wavelet Analysis", Birkhauser, ISBN-0- 8176-3962-4.

[5] Musheer Ahmed, M.shamsher Alam(2009) **"**A new algorithm of encryption and decryption of images using chaotic mapping**"** International Journal on computer science and engineering,vol.2(1), pp46-50.

[6] J.Fridrich(1998) **"S**ymmetric ciphers based on two-dimensional chaotic maps" International Journal of Bifurcation and Chaos.vol.8, ,1259-1284.

[7] **L**inhua Zhang, Xiaofeng liao , Xuebing Wang(2005) "An image encryption approach based on chaotic maps" chaos solitons and fractals,vol.24 ,759-765.

[8] **S**higuo lian , Jinsheng sun, Zhiquan wang(2005) **"**A block cipher based on a suitable use of the chaotic standard map"chaos solitons and fractals,vol.26, ,117-129.

[9] Ahmed T A1-Taani and Abdullah M.AL-Issa (2009) "A Novel Steganographic Method For Gray-Level Images". World Academy Of Science Engineering and Technology,.

[10] Puech, W. and Rodrigues, J. M. (2004.) A New Crypto-Watermarking Method for Medical Images Safe Transfer. In The 12th European Signal Processing Conference, pp. 1481-1484.

[11] Chengqing Li, (2008)"On the security of a class of Image Encryption Scheme", IEEE International Symposium on Circuit & System , ISCAS, Department of Electronics Engineering, University of Hong Kong , pg 3290-3293

[12] S. K. Muttoo1, Sushil Kumar(2008) **"**Data Hiding in JPEG Images**"** BVICAM'S International Journal of Information Technology Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi.

[13] Microslav Dobsicek, (2004)"Modern Stegnography" 8th International Student Conference on Electrical Engineering FEE CTU.

[14] C.E. Shannon, (1949)"Communication Theory of Secrecy Systems," *Bell Syst Tech J*, vol. 28, , pp. 656–715.

[15] Chong Fu, Jun-jie Chen,Hao Zou, Wei-hong Meng, Yong-feng Zhan, and Ya-wen Yu(2012), "A chaos-based digital image encryption scheme with an improved diffusion strategy" (C) 2012 OSA, Vol. 20, No. 3 / OPTICS EXPRESS 2363.