A New Image Encryption Method using Chirikov and Logistic Map

Nidhi Sethi
Assistant Professor
Dehradun Institute of Technology
Dehradun-248001

ABSTRACT
In this paper, we have proposed a new method to develop secure image-encryption techniques using a Chirikov Standard Map and Logistic Map . In this technique, a Chirikov standard map is used to shuffle the pixels of the image and hence creating the confusion. The 1D logistic map is further used to create diffusion in the image. Various test images are 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 highly key sensitive and shows good 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.

Here in this proposed work the combination of Logistic map and chirikov map have been used.The input image is subjected to chirikov mapping which aims at shuffling of the pixels.The shuffled image is then again shuffled by blocks shuffling.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. LITREATURE 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. 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.

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 following security problems were found: 1) the schemes are not sensitive to change of plain-image; 2) the schemes are not sensitive to change of secret key; 3) there exist a serious flaws of diffusion function; 4) 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.

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

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

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

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.

2.2 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 logistic map is below:

$$X_{n+1}=\lambda\ X_n(1-\ X_n)$$

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.

3. PROPOSED ALGORITHM

The proposed image encryption algorithm has two major steps. Firstly, 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 logistic 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 1 D Logistic map. The control parameters of 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 1D Logistic map and Chirikov standard map.

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

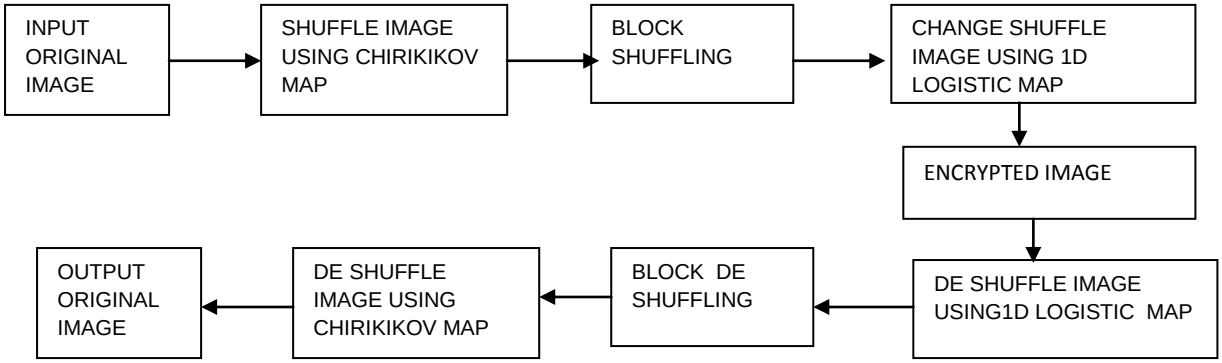

Fig 1: Block Diagram of the proposed algorithm

4. RESULTS AND DISCUSSION

In this proposed work the combination of Chirikov map and 1D Logistic map has been used. To demonstrate the efficiency of the algorithm ,the results of various tested images is shown below. It is found that this new scheme has a satisfactory security level with low computational complexity ,and hence fast ,which proves to be a good candidate for real-time secure image transmission.

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)

4.1 Experimental Results

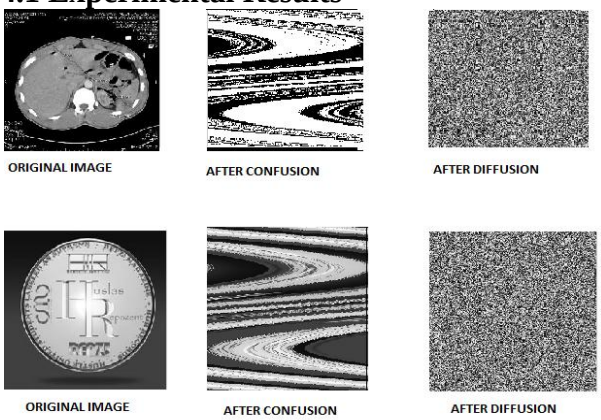

Fig:2 Image after and before encryption

4.2 Key Analysis:

4.1.1 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

4.1.2 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.

4.3 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.

4.3.1 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 .

4.3.2 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.

4.3.3 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.

4.3.4 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.

4.3.5 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 of PSNR , MSE and MAE

S.NO	*Name of the Image*	*Number of keys*	*PSNR*	*MSE*	MAE
1	Lena	5	51.375	0.4737	73.2982
2	Baba	5	50.156	0.6272	82.7033
3	Brain	5	42.6	3.5679	99.8053
4	HR	5	44.0785	2.542	89.0576

Table 2: Results of Correlation

S.NO	Name of the image	Size	CORR
1	Baba	128*128	0.0044
2	Lena	128*128	-0.0067
3	Brain	256*256	0.0043
4	HR	240*240	-0.0027

Table: 3 Result of Entropy

S.NO	Name of the image	Size	Plain Image	Cipher Image
1	Baba	128*128	0.0001	7.9889
2	Lena	128*128	0.0001	7.9879
3	Brain	256*256	0.96088	7.9962
4	HR	240*240	0.0002	7.9969

5. CONCLUSION

The reported paper aimed at developing an secure algorithm for image encryption. The encryption algorithm use two concepts i.e confusion and diffusion which is also called substitution and permutation among the pixels of the gray scale image. To perform the confusion in the plain-image's pixels, a chirikov map is used and finally ID logistic map is used to perform the diffusion. Four different size images have been used for test and the results are mentioned above .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.

6. 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.