Chaos Image Encryption using Pixel shuffling

Manjunath Prasad[1] and K.L.Sudha[2]

[1.]M.Tech (DEC) student, DSCE, Bangalore,
manjunath.dubey@yahoo.com
[2.]Prof, Dept of ECE, DSCE, Bangalore.
klsudha1@rediffmail.com

***Abstract**: The advent of wireless communications, both inside and outside the home-office environment has led to an increased demand for effective encryption systems. The beauty of encryption technology comes out in more pronounced way when there is no absolute relation between cipher and original data and it is possible to rebuild the original image in much easier way. As chaotic systems are known to be more random and non-predictable, they can be made utilized in achieving the encryption. The transposition technology of encryption systems requires scrambleness behaviour in order to achieve the encryption of the data. This scrambleness behaviour can be derived from the randomness property of chaos which can be better utilized in the techniques like transposition system. In wireless communication systems, bandwidth utilization is an important criterion. In order to use encryption system in wireless communication; key space plays an important role for the efficient utilization of the bandwidth. In this paper we present a chaos-based encryption algorithm for images. This algorithm is based on pixel scrambling where in the randomness of the chaos is made utilized to scramble the position of the data. The position of the data is scrambled in the order of randomness of the elements obtained from the chaotic map and again rearranged back to their original position in decryption process. The same algoritm is tested with two different maps and performance analysis is done to select best suited map for encription.*

***Key words:** chaos, Encryption systems, Transposition technique.*

1. Introduction

The amazing developments in the field of network communications during the past years have created a great requirement for secure image transmission over the Internet. Internet is a public network and is not so secure for the transmission of confidential images. To meet this challenge, cryptographic techniques need to be applied. Cryptography is the science of protecting the privacy of information during communication, under hostile conditions. In recent days, Chaos based methods are used for image Encryption. Chaos word has been derived from the Greek, which refers to unpredictability and it is defined as a study of nonlinear dynamic system. Chaos theory is a mathematical physics which was developed by Edward Lopez. Chaos is suitable for image encryption, as it is closely related to some dynamics of its own characteristics. The behaviour of the chaos system, under certain conditions, presents phenomena which are characterized by sensitivities to initial conditions and system parameters. Through the sensitivities, the system responses act to be random. The main advantages of the chaotic encryption approach include: high flexibility in the encryption system design, good privacy due to both nonstandard approach and vast number of variants of chaotic systems, large, complex and numerous possible encryption keys and simpler design.[1] The digital image processing methodology is classified into two categories- pixel value substitution and pixel location scrambling. The first one concentrates on changing the pixel value so that others cannot read the original pixel information in the digital image.

D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, pp. 169–179, 2011.
 DOI: 10.5121/csit.2011.1217

The other one concentrates on changing the pixel position for the purpose of encryption. However, both of these methods can be easily decrypted by some ways. Use of key which act like an initial condition in the chaos encryption system is an important parameter for key space, the larger the key space, more immunity towards brute-force attack but bandwidth is also an important criteria when it comes to use of wireless communication.

A large number of applications in real systems, both man-made and natural, are being investigated using this novel approach of nonlinear dynamics. Many chaos based encryption methods have been presented and discussed in the last two decades. An elaborated survey has been done about chaotic cryptography in paper [2]. In paper [3] authors have used Henon map to achieve encryption of grey image. In this algorithm, first, the Arnold cat map is used to shuffle the positions of the image pixels and then the shuffled-image is encrypted based on Henon's chaotic system pixel by pixel. Paper [4] suggests a new approach to image encryption based on hyperchaotic map in order to meet the requirements of the secure image transfer. The ergodic matrix of one hyperchaotic sequence is used to permute image, the form of which is decided by a chaotic logistic map, the other hyperchaotic sequence is used to diffuse permuted image. Hybrid Image Encryption Using Multi-Chaos-System is proposed in [5] where in three maps are used for shuffling the R,G,B matrix separately and another map for Bit-Chaotic-rearrangement. Four different chaotic maps are used in order to achieve encryption of colour image. Paper [6] presents a novel image scrambling method using Poker shuffle, which is controlled dynamically by chaotic system. Papers [7-15] give various ways of using chaos for cryptography.

In this paper we have proposed a new algorithm which utilizes the single map against the four maps used in [5]. We used Henon map and Lorentz map for pixel shuffling and measured correlation coefficient and key sensitivity for finding best suited map for this algorithm. The key space will become less with single map utilization and hence better suited for applications like wireless communication. At the same time it gives better secrecy and a key which is difficult to decypher by an unintended user.

2. Proposed Encryption Algorithm

Consider an image (Io) with dimension M×N×P, Where, P represents color combination (3 for a color image); M, N represents rows and column of intensity level. Separate R,G, B matrix of Image and convert each R,G,B matrix into single array (1×mn). For example, Lena image which is one of the common image used for image processing algorithms has a dimension of 225× 225× 3 and after separation of R,G,B and converting it in to single array vectors, we get 3 vectors of dimension 1× 50625.

For encryption we first generate elements from chaos map equal to the dimension of 3×M×N matrix. In our example of Lena image 225×225×3=151875 elements are generated with Henon map. The Henon map can be generated using the equation given below which is iterated for n=1 to 151875 times to generate the required elements.

x(n+1)=1-a*x(n)^2+y(n); y(n+1)=b*x(n);

We used the following values for the constants 'a' and 'b' to get a random sequence.

a=1.76, b=0.1 and y(n)=1

The same procedure is repeated with Lorentz map. Following equations describes Lorentz map.

X(1)=s*(y(i-1,2)-y(i-1,1));

X(2)=r*y(i-1,1)-y(i-1,2)-y(i-1,1)*y(i-1,3);

X(3)=y(i-1,1)*y(i-1,2)-b*y(i-1,3);

y(i,:)=y(i-1,:)+h*X;

For this map, we used the following values for the constants 's','y','h', 'b'and 'r' to get a random sequence.

s=10,b=3,r=30,h=0.01 and y=[0.1,0.1,0.1]

The table below shows elements generated from Henon map taking iteration for 'n' from 1 to 27. (27 elements are taken as an example to explain the encryption process where as actual number of elements generated for Lena image is 151875)

Table.1 27 Elements generated from Henon map

0.819	0.912	1.234	0.486	0.298	0.421	0.581	1.456	1.834
0.412	2.814	3.453	2.166	1.281	1.481	0.893	0.921	0.110
0.234	0.822	1.625	1.435	1.893	1.205	0.891	0.717	0.625

Here care should be taken to see that the generated elements are unique; there shouldn't be any repetition. Now divide the generated elements into three blocks of each equal to M×N. In our example of Lena image each block is of dimension 1×50625.

Table.2 below shows how the obtained elements from the previous steps are divided into three separate arrays each of 9 elements for the total of 27 elements.

Table.2 Division of elements into 3 rows to represent RGB values

0.819	0.912	1.234	0.486	0.298	0.421	0.581	0.456	1.834

0.412	2.814	3.453	2.166	1.281	1.481	0.893	0.921	0.110

0.234	0.822	1.625	1.435	1.893	1.205	0.891	0.717	0.625

Now sort the elements of each block in ascending or descending order and compare the mis-order between the original and sorted elements of each block and tabulate the index change. We have got three series of index change values in according to three blocks. For example consider the first array from the previous table. Index the elements as shown in fig1 (a). Arrange the elements in decreasing order and tabulation of the displacement in the index is noted by comparing the elements before and after sorting as in fig1 (b). This procedure is repeated for all the three colours. Now according to the obtained index, we change the intensity position to get encrypted image.

In the fig (2) column 1 represents intensity value of image, column 2 represents the tabulated index value obtained from the previous step and column 3 represents the arranged intensity value according to column 2.

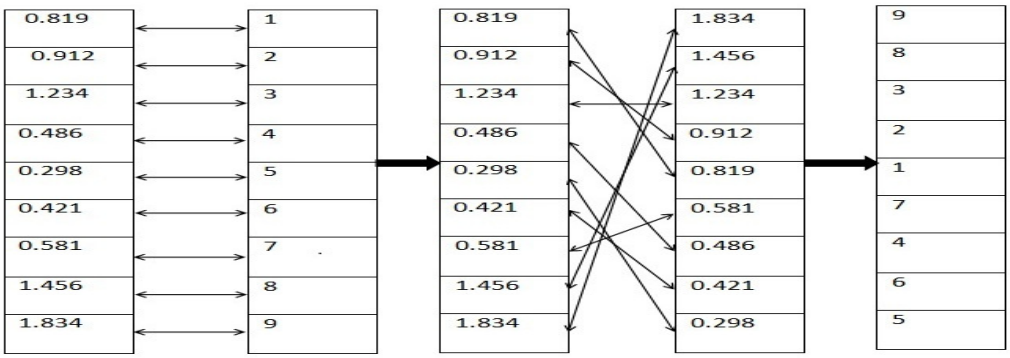


Fig 1(a) Fig 1(b)

Fig(1) Arranging elements in decreasing order and tabulation of the displacement in the index

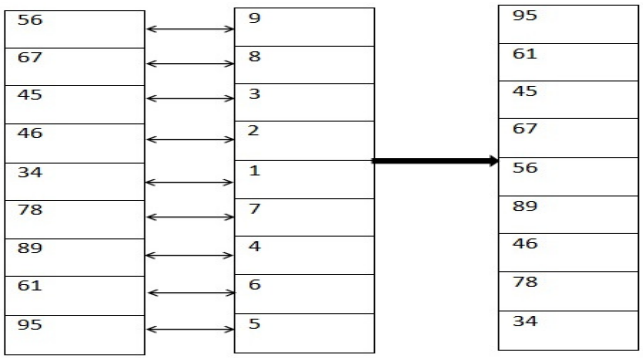


Fig (2) Ordering of pixel values

In our example of Lena image, similar process is done for 50625 pixels and encrypted image is obtained. Decryption is done by the reverse process followed for encryption. In fig 3(b) column 1 represents the sequence of received elements; column 2 represents sorted index elements obtained from the encryption process and column 3 represents resorted index elements. At the receiving point, the same random sequence is generated with Henon map to obtain back he sorted index elements as in fig 3(a) and original pixel values are obtained back as in Fig 3(b)

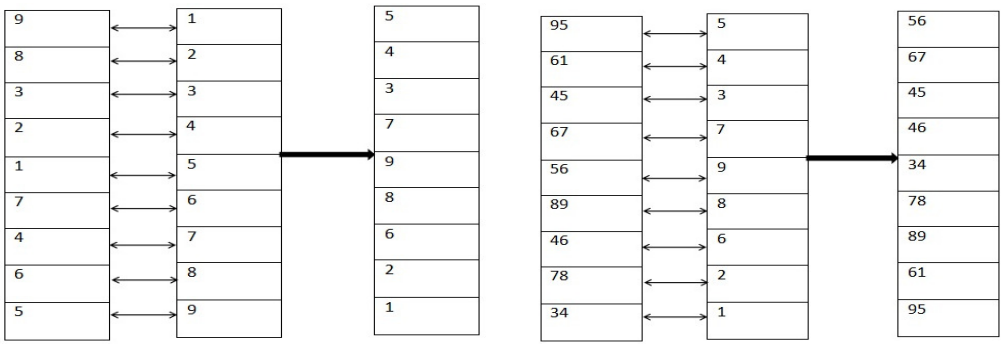


Fig 3(a) Fig 3(b)

Fig (3) Decryption process

3. Experimental results

Two colour images are taken for testing the proposed pixel scrambling algorithm. The first one is a medical image "*Brain* (201×251×3)". Fig. 4(a) shows the original map, pixel scrambled encryption map and their RGB-level and Fig4(b) encrypted "*Brain image(201×251×3)*" with RGB plot.

As seen from the figures, the intensity value of the original Brain image is distributed or scrambled in the encrypted image and its RGB plot. This distribution is due to the randomness obtained from the elements of the Henon map. The obtained image from the process of encryption is subjected to decryption algorithm where in the pixel values are rearranged back to its original position resulting into the intensity plot which is same as the original image intensity plot as shown in Fig 4(c)

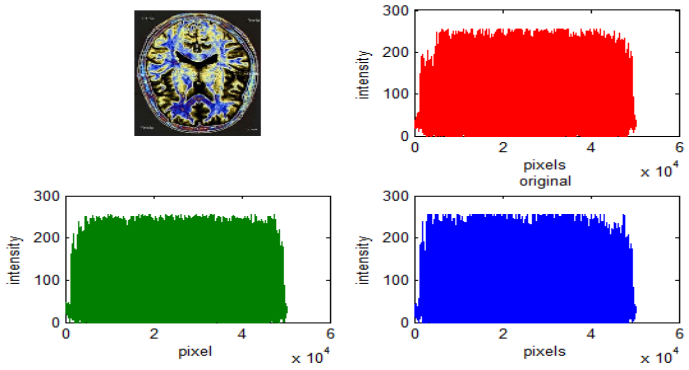


Fig4(a) Image and RGB intensity levels

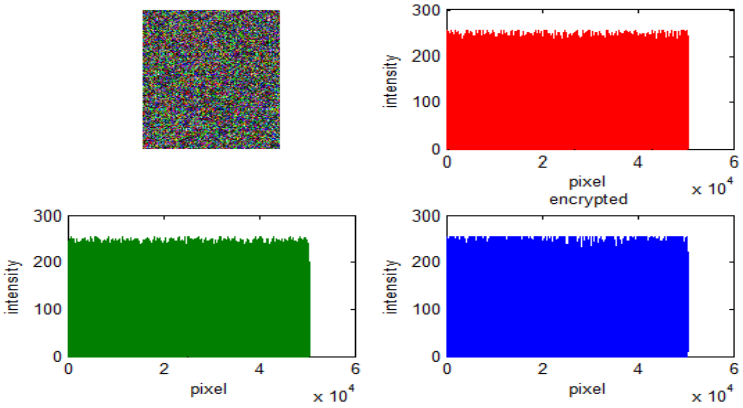
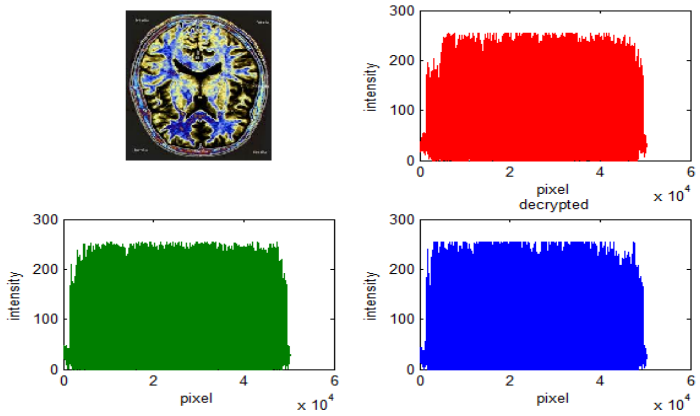


Fig4(b) Scrambled Image and RGB intensity levels



Fig(4c) Decrypted Image and RGB intensity levels

Another image taken to test the algorithm is Lena image (225×225×3). Fig 5(a), 5(b) and 5(c) show the original image, pixel scrambled encrypted image and decrypted image with their RGB-levels.

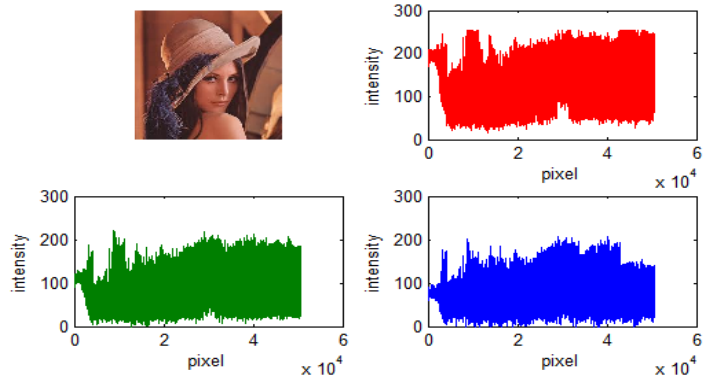


Fig5(a)Lena image and RGB intensity plots

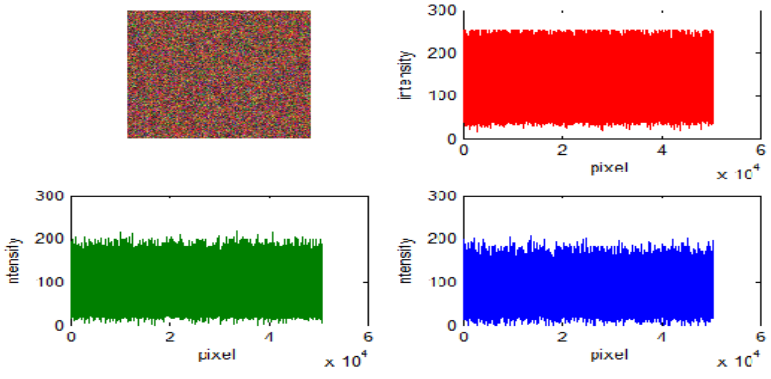


Fig5(b) Encrypted image and RGB intensity plots after encryption

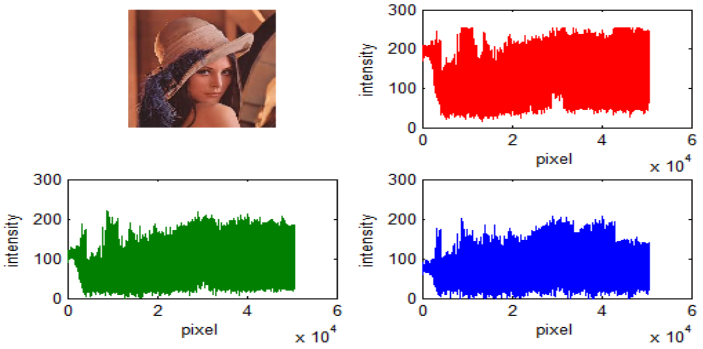


Fig5(c) decrypted image and RGB intensity plots after decryption

All results are obtained from the simulation of encryption algorithm in Matlab Simulator for Henon map. A similar type of encryption and decryption process is performed with Lorenze map also to compare the two results.

4. Performance Analysis

To measure the performance of the encryption algorithm, we have calculated the correlation coefficient. If correlation coefficient is nearer to zero for an encrypted image, then algorithm is said to be better. To prove that decryption is possible only with one key, key sensitivity is calculated.

4.1 Correlation Coefficient

Correlation coefficient 'r' is the measure of extent and direction of linear combination of two random variables. If two variables are closely related, the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, two variables are not related. The coefficient *r* can be calculated by the following formula

$$r = \frac{\sum_i (Xi - Xm)(Yi - Ym)}{\sqrt{\sum_i (Xi - Xm)2}\sqrt{\sum_i (Yi - Ym)2}}$$

Where

- Xi - pixel intensity of original image
- Xm- mean value of original image intensity
- Yi- pixel intensity of encrypted image
- Ym - mean value of encrypted image intensity

The correlation values are calculated for original and encripted images with Henon and Lorenze maps and shown in the table 3 and 4. It clearly shows that the correlation co-efficient values are very near to zero with both the maps. But values obtained from Henon map are slightly lesser compared to Lorentz map.

With this we can conclude that , for this encryption algorithm Henon map have a slight upper hand compared to Lorentz map. But for both the pictures the correlation co-efficient are very low and near to Zero. This proves that the algorithm leads to a more secured encryption process.

Table 3. Correlation coefficient with Henonmap

Image	R(correlation)	G(correlation)	B(correlation)	total(correlation)
Brain.jpg	2.5042e-006	3.3799e-006	3.7928e-006	3.2256e-006
	9.3529e-007	8.3087e-007	8.3523e-007	8.6710e-007

Table 4. Correlation coefficient with Lorentz map

Image	R(correlation)	G(correlation)	B(correlation)	total(correlation)
Brain.jpg	9.2416e-007	8.4546e-007	8.4187e-007	8.7050e-007
Lena.jpg	1.327e-005	8.7905e-006	7.7947e-006	9.9475e-006

4.2 Key Sensitivity

A good Encryption algorithm should be very much sensitive to the key. A slight variation in the key should result in totally different image in the rebuilding process at the destination end.

Fig6 (a) original image

Fig6 (b) decrypted image using actual key (a=1.80000)

Fig6(c) decrypted image with slightly different key(a=1.80001)

Fig(6) Decryption with Henon map

In this algorithm, the initial condition assumed to generate the chaotic map acts as the key. We tried to decript the encripted image with one iniial condition, using another initial condition which differ by a very small value. Obtained results are shown in fig(6)

.

The above results are shown for Henon map with initial conditions ‘a’=1.80000 (original key) and slightly different value 1.80001. From the obtained result it is clear that a slight variation, say 0.0001 results in totally different image as shown in Fig 6(c).

The same experiment was carried using Lorentz map. Slight variation in initial condition ‘b’=2.8 to 3.0 of Lorentz map results in different decrypted images as shown in Fig7(c)

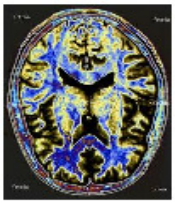


Fig7(a) original image

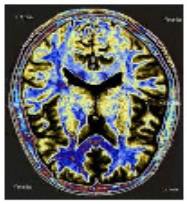


Fig7 (b) decrypted image using actual key (b=2.8)

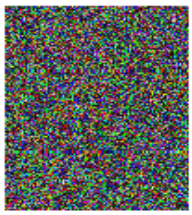


Fig7(c) decrypted image with slightly different key(b=3.0)

Fig (7) Decryption with Lorentz map

In our algorithm we have used single Henon map/Lorentz map, thus key space is less in comparison to the paper [5]. There they have used 3 chaos maps in order to achieve encryption which uses a keyspace 3 times that of our algorithm. Memory requirement is less in this algorithm and hence better suited for the applications like wireless communication.

5. Conclusion

This paper describes about a novel image encryption technique using the concept of non-linear dynamic system (chaos). The chaos system is highly sensitive to initial values and parameters of the system. The proposed method utilizes the randomness of the chaos maps in order to encrypt the image. In this algorithm the pixel position is changed according to the randomness of the chaotic elements, which is derived by comparing sorted and unsorted chaotic elements generated from chaos map. This algorithm completely removes the outlines of the encrypted images, blurs the distribution characteristics of RGB-level matrices.

We have calculated the correlation coefficient '*r*' to test the distribution of elements of the encrypted image. We tried the same algorithm with two maps in order to test the suitability of the map for this algorithm. With the results we can conclude that both maps are suited for encryption. Also with both maps, results are better compared to the result obtained in paper [5]. The obtained values clearly signify the importance of this algorithm in the application of image encryption, especially for wireless communication because single map is used in this algorithm, which leads to efficient utilization of bandwidth. As only one initial condition value has to be sent, number of bits to be transmitted is 1/3rd of that required in paper [5], which is an important factor for wireless communication.. The key sensitivity test proves the calibre of the algorithm when it is subjected to wrong key.

Acknowledgement: The work described in this paper is supported by the ISRO (RESPOND Grant NO. ISRO/RES/3/609/10-11).

References

[1] Victor Grigoras1 , Carmen Grigoras "Chaos Encryption Method Based on Large Signal Modulation in Additive Nonlinear Discrete-Time Systems" Proc. of the 5th WSEAS Int. Conf. on Non-Linear Analysis, Non-Linear Systems and Chaos, Bucharest, Romania, October 16-18, 2006.

[2] Mintu Philip, Asha Das "Survey: Image Encryption using Chaotic Cryptography Schemes" *IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011.*

[3] E. N. Lorenz, " Deterministic nonperiodic flow," J.Atmospheric Sci. 20 (1963) 130.

[4] Chen Wei-bin; Zhang Xin; "Image encryption algorithm based on Henon chaotic system" Image Analysis and Signal Processing, 2009. IASP 2009. International Conference, Publication Year: 2009 , Page(s): 94 – 97.

[5] Nien, H.H.; Huang, W.T.; Hung, C.M.; Chen, S.C.; Wu, S.Y.; Huang, C.K.; Hsu, Y.H.; "Hybrid image encryption using multi-chaos-system" Information, Communications and Signal Processing, 2009. ICICS 2009. 7th International Conference on digital identifier Publication Year: 2009 , Page(s): 1 – 5.

[6] Xiaomin Wang; Jiashu Zhang; " An image scrambling encryption using chaos-controlled Poker shuffle operation" Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on Publication Year: 2008, Page(s):1- 6.

[7] Murali, K.; Haiyang Yu; Varadan, V.; Leung, H.; "Secure communication using a chaos based signal encryption scheme" Consumer Electronics, IEEE Transactions on Volume: 47 , Issue: 4, Publication Year: 2001 , Page(s): 709 – 714.

[8] Li Chuanmu; Hong Lianxi; "A New Image Encryption Scheme based on Hyperchaotic Sequences" Anti-counterfeiting, Security, Identification, 2007 IEEE International Workshop , Publication Year: 2007 , Page(s): 237 – 240.

[9] Deergha Rao, K.; Gangadhar, Ch.; "Modified Chaotic Key-Based Algorithm for Image Encryption and its VLSI Realization" Digital Signal Processing, 2007 15th International Conference, Publication Year: 2007 , Page(s): 439 – 442.

[10] Koduru, S.C.; Chandrasekaran, V.; "Integrated Confusion-Diffusion Mechanisms for Chaos Based Image Encryption" Computer and Information. Technology Workshops, 2008. CIT Workshops 2008. IEEE 8th International Conference, Publication Year: 2008 , Page(s): 260 – 263.

[11] De Wang; Yuan-Biao Zhang; "Image Encryption Algorithm Based on S-boxes Substitution and Chaos Random Sequence" Computer Modelling and Simulation, 2009. ICCMS '09. International Conference , Publication Year: 2009 , Page(s): 110 – 113.

[12] Weihua Zhu; Ying Shen; "Encryption algorithms using chaos and CAT methodology" Anti-Counterfeiting Security and Identification in Communication (ASID), 2010 International Conference , Publication Year: 2010 , Page(s): 20 – 23.

[13] Qiang Wang; Qun Ding; Zhong Zhang; Lina Ding; "Digital Image Encryption Research Based on DWT and Chaos" Natural Computation, 2008. ICNC '08. Fourth International Conference Volume: 5 Publication Year: 2008 , Page(s): 494 – 498.

[14] Zhang Yun-peng; Liu Wei; Cao Shui-ping; Zhai Zheng-jun; Nie Xuan; Dai Wei-di; "Digital image encryption algorithm based on chaos and improved DES Systems", Man and Cybernetics, 2009. SMC 2009. IEEE International Conference Publication Year: 2009 , Page(s): 474 – 479.

[15] Usama, M.; Khan, M.K.; "Classical and chaotic encryption techniques for the security of satellite images" Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium Publication Year: 2008 , Page(s): 1 – 6.

[16] Yupu Dong; Jiasheng Liu; Canyan Zhu; Yiming Wang; "*Image encryption algorithm based on chaotic mapping"* Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on Volume: 1 'Publication Year: 2010 , Page(s): 289 – 291.

[17] Kwok-Wo Wong, Ching-Hung Yuen; "Performing Compression and Encryption Simultaneously using Chaotic Map".

Authors

Manjunath Prasad, received his B.E(ECE) from AIET , Gulbarga and presently pursuing his M.Tech (DEC) in DSCE, Bangalore. His areas of interest are Digital communication, Digital image processing and embedded design.

Email-Id:- manjunath.dubey@yahoo.com

Dr K L Sudha, received her B.E(ECE) from Mysore university in 1988, M.E (electronics) from Bangalore University in 1992.She got her PhD from Osmania university in 2009. She has 15 years of teaching experience and presently working as professor in DSCE, Bangalore. She has published more than 12 research papers in journals and conferences. Her areas of interest are wireless communication and information theory.

Email-Id:- klsudha1@rediffmail.com