A Comparative Study of Image Encryption Methods Using Coupled Map and Non-Linear Chaotic Algorithm

Vinayak Jadhav, Shilpa K

Abstract- With the rapid development of computer network and multimedia technology, the security of digital image information has become a major concern. For image data with privacy and national security should be transmitted in a secret way, image encryption technology has drawn more and more attention. In this project two digital image encryption methods based on the chaotic systems are used for the high level security and the key space, Non-linear Chaotic Algorithm (NCA) and a novel algorithm based on mixture of chaotic maps or coupled map, NCA uses the power functions and tangent functions instead of linear function to increase the key space and high level security. In novel algorithm based on mixture of chaotic maps or coupled map, a typical coupled map was mixed with a one-dimensional chaotic map and used for high degree security image encryption while its speed is acceptable, and also it has large key space than the NCA map. By experimental results the mixture of chaotic system or coupled map is robust than the NCA map.

Key words: Image encryption, chaotic system, Logistic map, NCA map, Coupled map. NPCR, UACI

1. INTRODUCTION

With the rapid development of multimedia technology and Internet, digital images and other multimedia are more commonly and frequently transmitted in the public communication network. Therefore, the security of image data attracts more and more attention, and image encryption technology becomes an important issue of cryptography.

Image Encryption is a process of converting an image from readable to unreadable form or it is the process of encoding images (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can read it. Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the Internet and through wireless networks. Traditional image encryption algorithm such as data encryption standard (DES) has the weakness of low-level efficiency when the image is large. The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. After Matthews proposed the chaotic encryption algorithm in 1989, there is an increasing researches of image encryption technology are based on chaotic systems. Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, no periodicity and topological transitivity, etc. Therefore, chaotic cryptosystems have more useful and practical applications.

One-dimensional chaotic system with the advantages of high-level efficiency and simplicity, such as Logistic map, has been widely used now. But their weakness, such as small key space and weak security, Logistic map is defined as $x_{n+1} = \lambda^* x_n * (1 - x_n)$, where λ € (0, 4), n = 0,1 . . . The parameter k and initial value x_0 may represent the key. The Logistic map has small key space and weak security. To overcome small key space and weak security coupled map and NCA algorithms are introduced. A new nonlinear chaotic algorithm (NCA), that chaotic encryption systems can be easily attacked and, in order to improve security, they suggested the adoption of non-linear functions, limited in time and space, to change the key continuously. A coupled map is a dynamical system that models the behaviour of non-linear systems (especially partial differential equations). They are predominantly used to qualitatively study the chaotic dynamics of spatially extended systems.This includes the dynamics of spatiotemporal chaos where the number of effective degrees of freedom diverge as the size of the system increases.

2. LITERATURE REVIEW

Wenping Guo presented *a* digital image scrambling encryption algorithm based on chaotic sequence. The algorithm utilizes the good features of chaotic sequence related to cryptographic properties, such as pseudo-random, sensitivity to initial conditions and aperiodicity. This algorithm use logistic mapping to confusion the location of the pixels in a digital image. Result shows that this scrambling encryption has good scrambling performance [1].

Shashank Shekhar et. al, described an efficient method for encryption of digital images using an adaptive algorithm. In this paper the image is used was segregated into significant and non significant blocks. For making the level of security different for different blocks, total and partial encryption has been utilized for the significant and non significant blocks respectively. Spatial as well as transform domain for the significant and non significant respectively are used in this proposed method. A comparative study between the conventional approaches of spatial and transform domain for the encryption of the image with the proposed encryption algorithm reveals the superior performance of this algorithm [2].

A hash based image encryption algorithm presented by **Abbas Cheddad et. al.** This paper describes a novel way of encrypting digital images with password protection using 1D SHA-2 algorithm coupled with a compound forward transform. A spatial mask is generated from the frequency domain by taking advantage of the conjugate symmetry of the complex imagery part of the Fourier Transform. This mask is then XORed with the bit stream of the original image. Exclusive OR (XOR), a logical symmetric operation, that yields 0 if both binary pixels are zero or if both are ones and 1 otherwise. This can be verified simply by modulus (pixel1, pixel2, 2). Finally, confusion is applied based on the displacement of the cipher's pixels in accordance with a reference mask. Both security and performance aspects of the proposed method are analyzed, which prove that the method is efficient and secure from a cryptographic point of view. One of the merits of such an algorithm is to force a continuous tone payload, a steganographic term to map onto a balanced bits distribution sequence [3].

Alireza Jolfaei et. al, approaches a novel image encryption scheme is proposed based on combination of pixel shuffling and W7. Due to sensitivity to initial conditions, chaotic maps have a good potential for designing dynamic permutation map. So a chaotic Henon map is used to generate permutation matrix. An external secrete key is used to derive the initial conditions for the chaotic map and W7 secrete key. Pixel shuffling is performed via vertical and horizontal permutation. Shuffling is used to expand diffusion in the image and dissipate the high correlation among image pixels. In order to evaluate performance, the proposed algorithm was measured through a series of tests. It is highly key sensitive and shows poor resistance against brute-force and statistical attacks [4].

The plain image is first decomposed into 8X8 size blocks based on shuffling of image is carried out using 2D catmap. Further the control parameters of shuffling are randomly generated by employing 2D coupled logistic. After that the shuffled image is encrypted using chaotic sequence generated by one dimensional logistic map [5]**.**

Nidhi Sethi et. al, proposed a new method to develop secure image-encryption techniques using a logistics- based encryption algorithm. In this technique, a Haar wavelet transform was used to decompose the image and decorrelate its pixels into averaging and differencing components. The logistic based image encryption algorithm produces a cipher of the test image that has good diffusion and confusion properties. The remaining components are compressed using a wavelet transform [6].

The image encryption is based on Henon chaotic maps in order to meet the requirements to secure the image transfer. It contains several parameters of chaos system, it is sensible to the original value and the unpredictable. Based on the key sensitivity and statistical analysis tests the Henon map provides an efficient and secures the image. The distribution of grey values of the encrypted image has a random like behaviour [7].

The system is used for encrypting the digital image data to secure image transmission. A secure communication scheme based on logistic map chaotic sequences with a non linear function proposed. Encryption and decryption keys are obtained by the logistic map which is one dimensional map that generates the secrete key which is the input for the non-linear function. Receiver can get the original information using received information and identical key. The result of the computer simulation shows that the transmitted image can be reliably recovered by using the proposed scheme even under the noisy channel [8].

The encryption plan combines the sequence generated by one-dimensional and two dimensional logistic chaotic maps to scramble the image, with scrambling algorithm being simple, easy to implement. The algorithm perform an easy operation on the chaotic sequence generated, making it able to act as the subscript of the image pixel matrix. The image will then scramble according to the subscript determined by the sequence. Due to the random likeness of the chaotic sequence, the pixels obtained according to this method during the scrambling will also be random. Higher dimensional chaotic system will be used to diffuse the pixels of the scrambled image and the sequence will be selected according to the conditions [9].

G. Alvarez et. al, suggested a paper on crypt analyzing a non-linear chaotic algorithm for image encryption. In this paper describes the security weakness of some proposed algorithm based on logistic like new chaotic map. This paper shows that the chaotic map distribution is far from ideal, thus making it a bad candidate as a pseudo random stream generator. As consequences the images encrypted with this algorithm are shown to be breakable through different attacks of variable complexity [10].

A chaotic map based cryptography technique confusion and diffusion applied on a spectral domain on discrete cosine transform (DCT) coefficients and hence the encryption is achieved fast without applying the large number of confusion and diffusion cycle as spatially domain is needed. The random number generator and Gaussian distributor are used to create diffusion template [11].

The NPCR (Number of pixel changing rate) and UACI (Unified average Changed intensity) are two common parameters used to evaluate the strength of algorithms of image encryption with respect to differential attacks. A high NPCR and UACI score is usually interpreted as a high resistance to the differential attacks. It is not clear how high NPCR/UACI is such that the image cipher indeed has a high security level. They approach this problem by establishing a mathematical model for ideally encrypted images and then derive the variance and expectations of UACI and NPCR and experimental results using the NPCR and UACI randomness tests show that many existing image encryption methods are actually not as good as they are purported, although some methods do pass these randomness tests [12].

3. METHODOLOGY

3.1 NON LINEAR CHAOTIC ALGORITHM

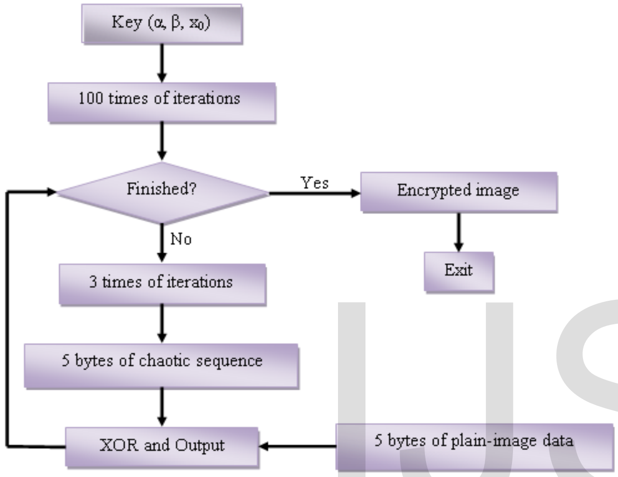

Fig.1: Non-linear Chaotic Algorithm

The encryption steps are as follows.

- Set encryption key for the plain image, including initial parameters α, β and x_0.
- Do 100 times of chaotic iteration as formula 4.3, and obtain the decimal fraction x_{100}.
- If the encryption work is finished, and then the image is encrypted, otherwise do three times of chaotic iteration and as a result, a decimal fraction, such as x_{103} will be generated, which is a double value and we choose its first 15 significant digits.
- After that divide the 15 digits into five integers with each integer consisting of three digits, for each integer, do mod 256 operation and another 5 bytes of data will be generated.
- Do XOR operation using the 5 bytes of data with 5 bytes of image data (grey value or colour RGB value). Output the calculation result to the object image and go to 3rd step.
- Pass the encrypted image through public communication channel.
- Then pass the encryption key through secure communication channel.
- End the encryption process.

The first 100 times of the chaotic iteration curve are abnegated in order to avoid the harmful effect of the transitional procedure. Here to improve system security pseudo random numbers discontinuously used as shown in flow chart. One was selected after two abnegated points.

The decryption algorithm is similar to the encryption algorithm but receiving encryption key and operating with the encrypted image.

3.2 COUPLED MAP

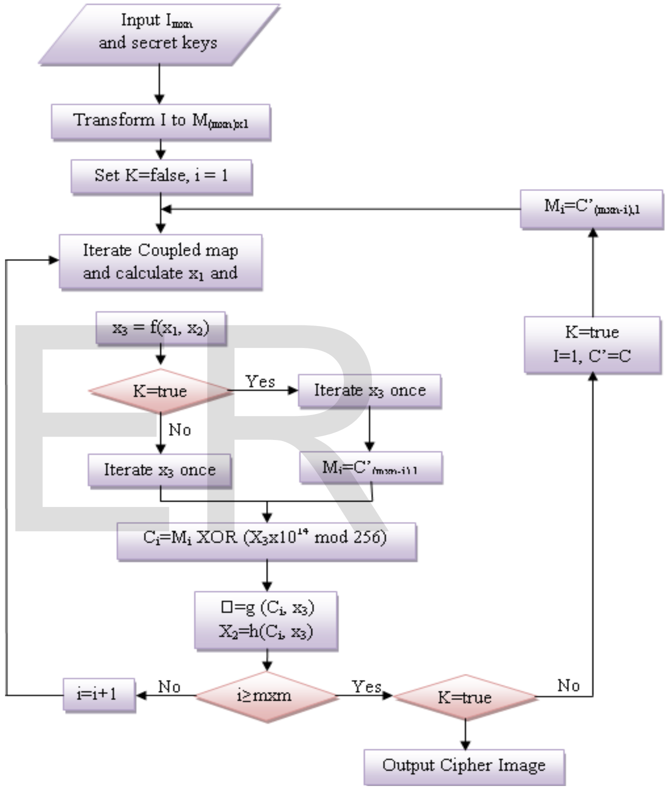

Fig.2: Coupled Map Algorithm

Following are the steps for the coupled map algorithm based on the mixture of chaotic maps.

- An image I_{mxn} is transformed into matrix $M_{(mxn)x1}$.
- The matrix $M_{(mxn)x1}$ is encrypted using results of iteration of chaotic coupled map and the third map.
- Using the initial condition and control parameters of the coupled map, the coupled map is iterated and then using a function of new $\tilde{x}_1(n+1)$ and $\tilde{x}_2(n+1)$ initial condition for the third map is made.
- Then the third map is iterated once and C_i is generated using the following equation.

$$C_i = M_i XOR(\tilde{x}_3(n+1) \times 10^{14} mod\ 256$$

- Then initial condition of $\tilde{x}_2(n+1)$ and coupling parameter (ϵ) are generated using a function of Ci and $\tilde{x}_3(n+1)$. This process continues up to M_{mxn}.
- Then M_{mxn} is set equal to C_{mxn} and the whole process is repeated for the new M from the last element to the first one and new matrix C is the output as the cipher text or image.

The decryption procedure is similar to that of encryption process illustrated above with reverse of cipher text as input instead of plain text in the encryption procedure. Since both decryption and encryption procedures have similar structure, they have essentially the same algorithmic complexity and time.

4. RESULT

4.1 Results of nca image encryption method for colour image

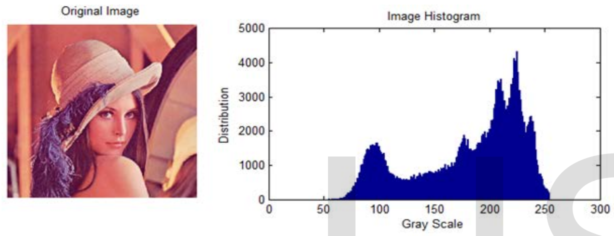

Fig.3: Input image (512X512) and its histogram

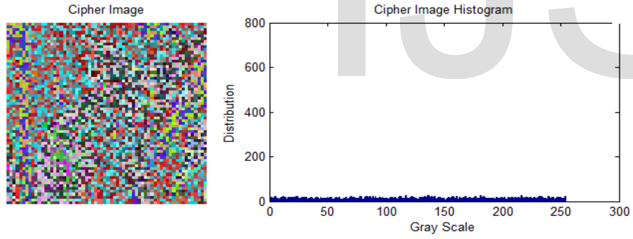

Fig.4: Encrypted Image and its Histogram

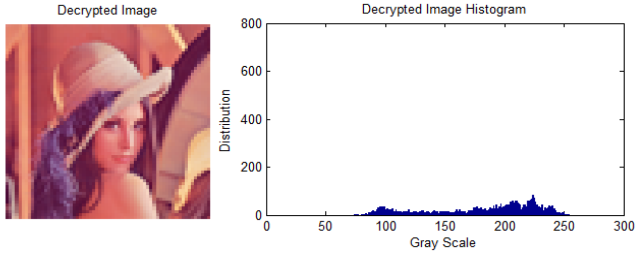

Fig.5: Decrypted image and its histogram with correct key

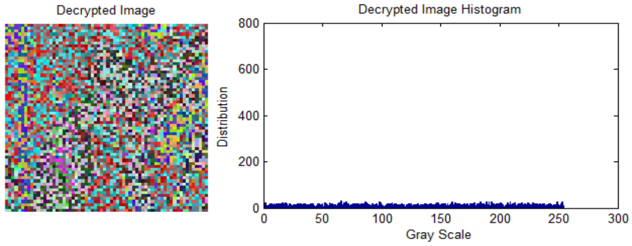

Fig.6: Decrypted image and its Histogram with incorrect key

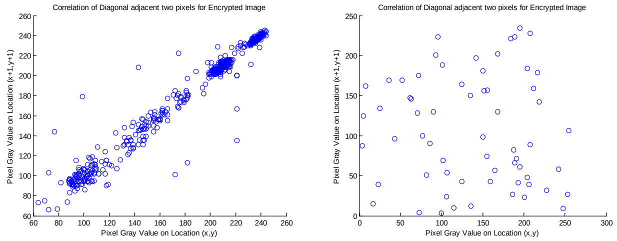

Fig.7: Correlation of two diagonally adjacent pixels in original and cipher image

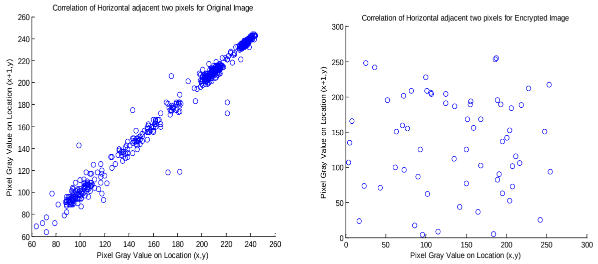

Fig.8: Correlation of two horizontally adjacent pixels in Original and cipher image

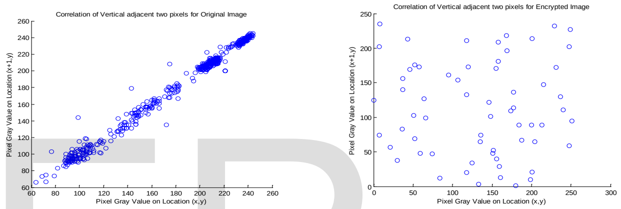

Fig.9: Correlation of two vertically adjacent pixels in Original and cipher image

The correlation of two adjacent pixels with key α= 1.41, β=5, x_0=0.3 as shown in below table.

Table 1: Correlation of two pixels of original and cipher image with key α= 1.41, β=5, x_0=0.3

CORRELATION COFFICIENTS	PLAIN IMAGE	CIPHERED IMAGE
HORIZONTAL	0.93618	0.1348
VERTICAL	0.84466	0.16698
DIGONAL	0.79089	0.15852

The NPCR and UACI differ for different initial parameters. As the higher NPCR and UACI it will become more resistant to the differential attacks. The NPCR and UACI for the colour Lena image as shown in table 2, for different initial parameter. Hence it is the key sensitive.

Table 2: NPCR and UACI for different initial parameters.

IMAGE	NPCR	UACI
LENAGRAY.BMP FOR A= 1.41, B=5, X_0=0.3	97.6563	32.9512
LENAGRAY.BMP FOR A= 1.5, B=39, X_0=0.8	99.9512	34.0787

The entropy, MSE and PSNR values for the initial parameters α= 1.41, β=5, x_0=0.3 is given in the below table.

Table 3: Entropy, MSE and PSNR values

ENTROPY	MSE	PSNR
8.7591	0.0019116	27.186

4.2 Results of coupled map image encryption method for colour image

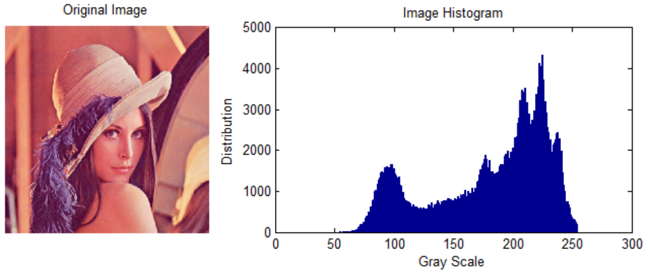

Fig.10: Original image and its histogram

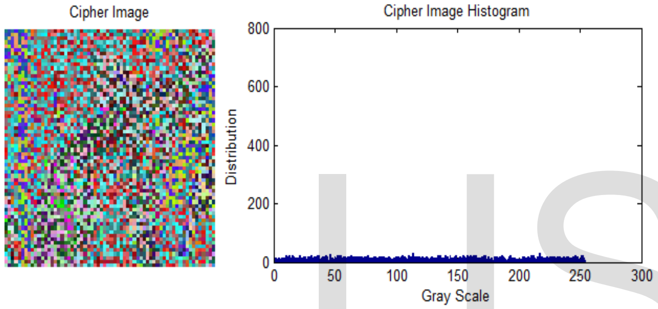

Fig11: Cipher image and its histogram

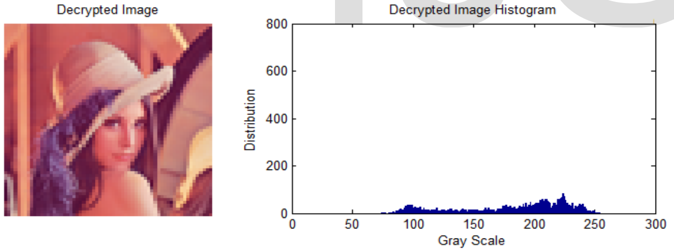

Fig.12: Decrypted image and its histogram with correct key

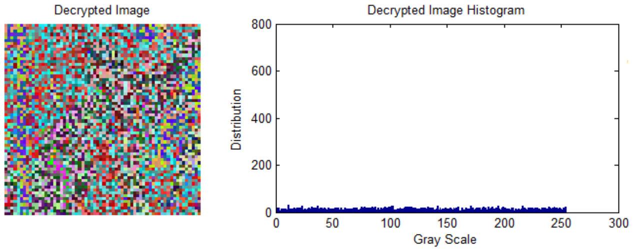

Fig.13: Decrypted image and its histogram with wrong key.

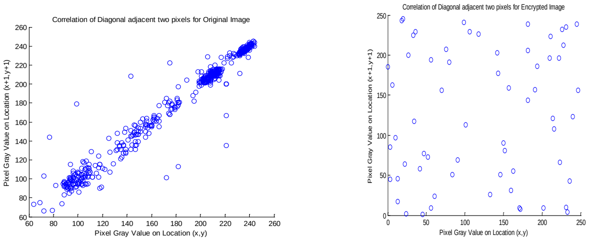

Fig.14: Correlation of two diagonally adjacent pixels in Original and cipher image

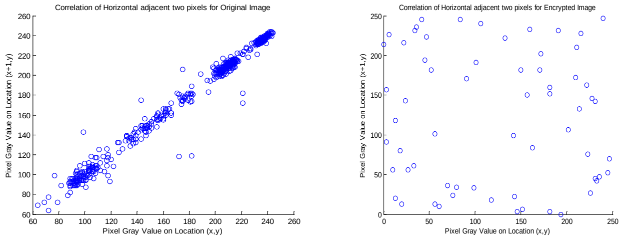

Fig.15: Correlation of two horizontally adjacent pixels in Original and cipher image

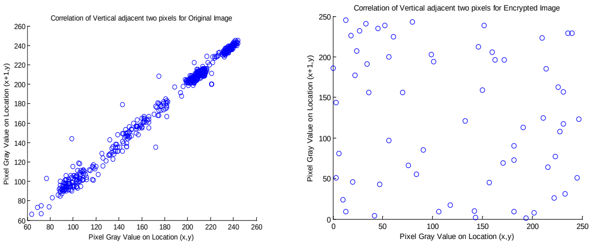

Fig.16: Correlation of two vertically adjacent pixels in Original and cipher image

The correlation of two adjacent pixels with key α_1=1.2, α_2=1.4, α_3=3 as shown in below table.

Table 4: Correlation coefficients for original and encrypted image

CORRELATION COFFICIENTS	PLAIN IMAGE	CIPHERED IMAGE
HORIZONTAL	0.93618	0.16881
VERTICAL	0.84465	0.14152
DIGONAL	0.79089	0.16881

The NPCR and UACI differ for different initial parameters. As the higher NPCR and UACI it will become more resistant to the differential attacks. The NPCR and UACI for the colour Lena image as shown in table 5, for different initial parameter. Hence it is the key sensitive.

Table 5: NPCR and UACI for initial parameters

IMAGE	NPCR	UACI
LENAGRAY.BMP FOR A_1= 1.2, A_2 =1.4, A_3 =3	97.9492	33.002
LENAGRAY.BMP FOR A_1= 1, A_2 =2, A_3 =5	97.583	32.4806

Table 5 shows the experimental entropy, MSE, PSNR values for the initial values for the key α_1= 1.2, α_2 =1.4, α_3 =3

Table 6: Entropy, MSE and PSNR values

ENTROPY	MSE	PSNR
8.7678	0.00050999	32.9244

5. CONCLUSION

The experimental results show that the mixture of chaotic system using coupled map algorithm is more robust than the nonlinear chaotic algorithm. The mixture of chaotic maps using coupled map method has the advantages like large key space i.e. over than 2^{260}, where in non-linear chaotic map is 10^{45}. Both the algorithms can endure severe attacks such as statistical attacks and brute-force attack but the coupled map algorithm provides high level security than the NCA map.

ACKNOWLEDGMENT

We wish to thank Mrs Bhagyashree Pandurangi for guiding us. And also we would like thanks to our organization AGMRCET Varur for supporting to publish.

REFERENCES

[1] Wenping Guo,"A new Digital Image Scrambling Encryption Based on Chaotic Sequence".

[2] Shashank Shekhar, Harshita Srivatsav and Kishore Dutta, "An Efficient Encryption Algorithm for Digital Images". International Journal of Computer and Electrical Engineering, Vol.4, No.3, June 2012.

[3] Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt, "A hash-based image encryption algorithm School of Computing and Intelligent Systems".

[4] Alirefza Jolfaei and Abdolarasoul Mirghadri, "An Image Encryption Approach using Chaos and Stream Cipher", Journal of Theoretical and Applied Information Technology.

[5] Musheer Ahmad and M. Shamsher Alam, "A new Algorithm of Encryption and Decryption of Images Using Chaotic mapping". International Journal on Computer Science and Engineering, Vol.2(1), 2009, PP 46-50.

[6] Nidhi Sethi and Deepika Sharma, "A novel method of image encryption using Logistic Mapping". International Journal of Computer Science Engineering (IJCSE).

[7] Xin Zhang and Weibin Chen, "A New Chaotic Algorithm for Image Encryption based on Henon Map".

[9] H. Ogras and M. Turk, "Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function", World Academy of Science, Engineering and Technology 2012.

[10] G. Alvarez and Shujun Li, "Cryptanalyzing a nonlinear Chaotic Algorithm (NCA) for image encryption". Communications in nonlinear Science and Numerical Simulations vol. 14, no. 11, 2009. PP 3743-3749.

[11] Shoaib Ansari, Neelesh Gupta and Sudhir Agrawal, " An Image Encryption Approach Using Chaotic Map in Frequency Domain", International Journal of Emerging Technology and Advanced Engineering. ISSN 2250-2459, Volume 2, Issue 8, August 2012

[14] Yue Wu, P. Noonan and Sos Agaian, "NPCR and UACI Randomness Tests for Image Encryption", Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011.