Image Encryption Using Chaotic Maps: A Survey

Priya R Sankpal
Dept. of TCE
BNMIT
BANGALORE, INDIA
Priya.bnmit@gmail.com

P. A. Vijaya
Dept. of ECE
BNMIT
BANGALORE, INDIA
pavmkv@gmail.com

Abstract— **As the exchange of data over the open networks and Internet is rapidly growing, security of the data becomes a major concern. One possible solution to this problem is to encrypt the data. The data can be text, image, audio, video etc.. In today's world most of the multimedia applications involve images. Earlier image encryption techniques like AES,DES,RSA etc. exhibit low levels of security and also weak anti attack ability. This problem was overcome by using chaos based cryptography. The chaotic systems are very sensitive to initial conditions and control parameters which make them suitable for image encryption. Many works have been done in the field of chaos based image encryption. In this survey paper an attempt has been made to review the aspects and approaches of the design used for image encryption.**

Keywords — **Image, cryptography, chaotic maps, encryption, security, analysis.**

I. Introduction

As the data exchange in electronic way is rapidly increasing, it is also equally important to protect the confidentiality of data from unauthorized access. The breaches in security affect user's privacy and reputation. The data exchanged can be text, image, audio, video etc. Each type of data has its own features different techniques are used to protect confidential image data from unauthorized access. Hence encryption of data is done to confirm security in open networks such as the internet where the multimedia applications are ever growing. Cryptography is the study of techniques for secure communication in the presence of an adversary. It deals with problems like encryption, authentication, and key distribution to name a few. Image encryption is a technique that provides security to images by converting the original image into an image which is difficult to understand. Applications of image encryption can extended to military communication, multimedia systems, medical science, telemedicine, internet communication etc. Generally images are different from textual data. The idea for encryption of image is to consider a 2D image as a 1D data stream and this stream is encrypted with any textual based cryptosystem. This approach is called nave approach [1]. For text, small bit rate audio, image and video files that can be sent over a fast dedicated channel, this approach is suitable. Unfortunately these encryption algorithms may not satisfy for different image data types like JPEG, PNG, BMP, etc... i.e. Traditional cryptosystems can be used to encrypt images, but it is not a good idea as image size is always much greater than the textual data. Also the decrypted text should be equal to the original text, whereas this requirement is not necessary for image data. An image when decrypted contains small distortion and is usually acceptable because of the characteristic of human perception.

II. IMAGE ENCRYPTION TECHNIQUES

Image encryption techniques can be divided into two groups based on the approach used to construct the encryption scheme: chaos based methods and non chaos based methods. Image encryption can also be classified according to the percentage of the data that is encrypted as full encryption and partial encryption. Several reviews have been published on image and video encryption including selective methods, thereby providing a fairly complete overview of the techniques developed till date [2] – [5].

III. CHAOS THEORY FOR CRYPTOGRAPHY

A chaotic dynamical system is a deterministic system that exhibits seemingly random behavior as a result of its sensitive dependence on its initial conditions and can never be specified with infinite precision. The chaotic system behavior is unpredictable; thereby it resembles noise. The close relationship between cryptography and chaos makes a chaos based cryptographic algorithm a natural candidate for secure communication and cryptography. Cryptographic algorithms and chaotic maps have similar properties such as sensitivity to changes in the initial conditions and control parameters, pseudorandom behavior and unstable periodic orbits with long periods. The basic principle of image encryption using chaos is based on the ability of some dynamic systems to produce sequence of numbers that are random in nature. Messages are encrypted using these sequences [5]. Because of the pseudorandom behavior, the output of the system seems random in the attacker's view whereas it appears as defined in the receiver's view and decryption is possible [6]. An important difference between cryptography and chaos maps is that encryption transformations are defined on finite sets whereas chaos maps have meaning only for real numbers [5]. Each chaos map has parameters that are equivalent to encryption key in cryptography. The similarities and differences between these two are listed as shown in Table I.

978-0-7695-5100-5/13 $31.00 © 2013 IEEE
DOI 10.1109/ICSIP.2014.80

Table 1. Similarities and differences between chaos and cryptography

There are two ways to apply a chaos map in a cipher system:

1. Generate pseudorandom key stream using chaotic systems
2. Use the plain text or the secret key(s) as the initial conditions and control parameters

Chaotic Systems	Cryptography Algorithms
Phase space : Set of real numbers	Phase space : Finite Set of integer numbers
Iterations	Rounds
Parameters	Key
Sensitivity to initial conditions and control parameters	Diffusion

Finally apply some iteration on chaotic systems to obtain cipher text. The first way corresponds to stream ciphers and the second to block ciphers [1].

IV. CHAOS BASED IMAGE CRYPTOSYSTEM: ARCHITECTURE

The architecture of chaos based image cryptosystem mainly consists of two stages: the confusion stage and the diffusion stage. The typical block diagram of the architecture is as depicted in the figure 1.

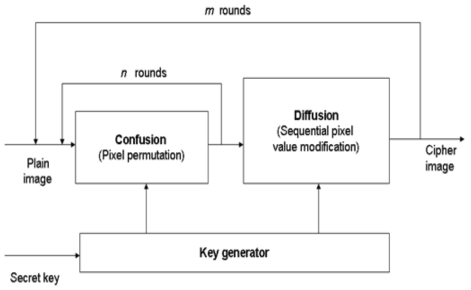

Figure 1. Architecture of a chaos - based image cryptosystem.

The confusion stage is the pixel permutation where the positions of the pixels are scrambled over the entire image without disturbing the values of the pixels. With this the image becomes unrecognizable. Hence these initial conditions and control parameters serve as the secret key. It is not very secure to have only the permutation stage since it may be broken by any attack. To enhance the security, the second stage of the encryption process aims at changing the value of each pixel in the entire image. The process of diffusion is carried out through a chaotic map which is mainly dependent on the initial conditions and control parameters. In the diffusion stage, the pixel values are modified sequentially by the sequence generated from the chaotic systems. The whole confusion-diffusion round repeats for number of times to achieve security of satisfactory level. The randomness property which is inherent in chaotic maps makes it more suitable for image encryption [7].

V. INSIGHT INTO DIFFERENT ENCRYPTION TECHNIQUES

In the scheme proposed by K. Sakthidasan Sankaran and B.V. Santhosh Krishna, the cryptosystem consists of two stages: Confusion stage and Diffusion stage. Different chaotic systems are employed in both the confusion and diffusion stages. Here complex chaotic maps are chosen rather than the simple ones to further increase the complexity of the algorithm, thereby improving the security. The input to the cryptosystem is a plain image that is to be encrypted. Encryption process comprises of confusion and diffusion stages. In confusion stage, pixel position permutation is done using one of the 3D chaotic systems. This is followed by the diffusion stage wherein the pixel value diffusion is carried out again with any one of the chaotic system. The initial conditions and the control parameters used for generating the chaotic sequence in both the stages serve as the secret key in the 2 stages. Separate keys are used for permutation and diffusion stage of the encryption process for enhancing the security of the algorithm. The resulting image is called the cipher image. The decryption process also comprises of 2 stages i.e. Diffusion followed by confusion stage. In the diffused image decryption stage, the original pixel values are retrieved by using any one of the chaotic system (Lorenz, chen, Lu). The diffusion key used in the 2^{nd} stage of encryption is used here also. In the final decryption process, to get back the original position of the image same confusion key as used in the first stage of encryption is used. The output of the decryption stage is nothing but the original image [7].

In this scheme the authors A. Anto Steffi and Dipesh Sharma proposed modified algorithm for encryption and decryption of images using chaotic maps. The 2 chaotic systems are used Lorenz and Baker maps. As mentioned in [7], the authors perform encryption process comprising of confusion and diffusion stage. In the confusion and diffusion stage, the pixel positions and values are changed (based on one of the 2 chaotic systems i.e. Lorenz or Baker) thereby shuffling the image. In both the stages separate keys are used for generating the chaotic sequence. In decryption stage, reverse operation is performed and the original image is obtained [8].

In this paper by Somaya, Al-Maadeed, Afnan Al-Ali, and Turki Abdalla, new image encryption scheme consists of pixel shuffler unit and a stream cipher unit. Pixel scrambling has 2 important issues which are useful for image encryption. Along with rearranging of pixel location (diffusion), it also changes the values of each pixel value (confusion). Confusion is performed by stream cipher through non-linear function operation. The pixel shuffler unit consists of a permutation map which can be applied in two directions: vertical and horizontal to decrease the adjacent pixels correlation. A 2D Henon map is employed as a pseudorandom number generator to build a permutation matrix. Now After pixel permutation, W7 algorithm is applied. The W7 algorithm generates a pseudorandom cipher bit stream called the key stream whose length is equal to shuffled image binary sequence. The cipher image is obtained by XORing the shuffled image binary sequence with the key stream. For decryption, the received cipher image is XORed with key stream and reverse shuffling operation is done via the inverse permutation [6].

In the paper by Hazem Mohammad Al-Najjar and Asem Mohammad AL-Najjar, an image encryption based on logistic map chaotic function is discussed. The encryption system can be divided into 2 approaches as pixel replacement approach and pixel scrambling approach. In pixel replacement approach, the pixel values are changed where as in pixel scrambling the pixel positions are changed. This algorithm consists of 2 replacement approaches to change the value of the pixel without shuffling the image itself. To achieve this, two pixel mapping tables that are created by using the logistic map are used. The pixel mapping table (PMT) contains the pixel values from 0 to 255 in the shuffled order with the size 256x1. The algorithm uses only replacement approaches to encrypt the image. The 2 different replacement approaches are: in the first approach, the pixels are shifted by suing a random value and mapping it by using PMT. In the second approach, replacement is done by using the XORing operation with specific random vector generated by using the logistic map. The process of decryption is done in the reverse order [9].

This proposed scheme uses the composite of the chaotic coupled map lattices to achieve the goal of image encryption. A gray scale image of size mxn (I_{mxn}) is considered for the purpose. The image is transformed into a matrix of $I_{mxn\ x\ 1.}$ Using the chaotic logistic map the strength of the coupling is generated which in turn is used for finding the chaotic trigonometric maps. The 2D dynamical coupled resulting sequences from this operation are again bitwise XORed to get the final cipher image. The decryption process is same as the encryption but with reverse steps [10].

In this paper presented by kamlesh Gupta and Sanjay Silakari, the main image of size MxN is divided into 3 separate images as Red, Green and Blue images. While the red and green images are transformed into vertical and horizontal planes respectively, the blue image is retained as it is. From the Transformed/rotated image, one row is read from each of planes to create a plane of these 3 image planes. First level of confusion is done by the 2D cat map. The final confusion stage is performed by a cascade of 2 maps i.e. first by cat map and then by standard map. The confusion stage is followed by the diffusion stage and cipher image is obtained by XORing each pixels of confused image with the diffused image. Decryption process is the reverse operation of the encryption procedure [11].

In their paper, Chong Fu et.al. proposed a novel bidirectional diffusion strategy which can significantly accelerate the spreading process to promote the efficiency of chaos –based image encryption. Also to enhance the security of the system, a plain-text related chaotic orbit turbulence mechanism is introduced in the diffusion stage by disturbing control parameters of the employed chaotic system according to the cipher pixel. The image shuffling is done by Chirikov map. The shuffled image histogram is same as that of the plain image since the permutation operation shuffles only the pixel positions without changing its value. As a result of this, the shuffled image is weak against statistical attack and known plain text attack. To overcome this, a diffusion procedure based on chebyshev map is employed. In the diffusion stage, to confuse the relationship between cipher and plain image, the pixel values are modified sequentially. The chaotic chebyshev map is used to generate the key stream for the diffusion. In general diffusion process is a time consuming procedure. For conventional chaos cipher images, overall 3-4 rounds are needed usually to achieve a satisfactory diffusion performance. This kind of computational complexity greatly downgrades its efficiency. Hence to improve the efficiency of the chaos based image encryption, a bidirectional diffusion scheme which accelerates the spreading process is used. The proposed diffusion module consists of 2 independent diffusion stages with different spreading direction where as the permutation module is kept unchanged. In the first stage, the difference is spread out to all pixels by modifying the pixel values sequentially left to right, top to bottom. In the second stage, right to left, a bottom to top sequential modification is carried out rather than starting the next round of permutation-diffusion as in the conventional diffusion schemes. As a result of this, the diffused pixels are spread out to the cipher image instead of wider range of the cipher image. Hence the overall encryption round are reduced without downgrading the security level [12].

In this algorithm, the image is represented in the matrix form wherein the gray levels are in the range 0 to 1. This pixel matrix is converted into an array. The pixel values are converted to unsigned integer in the range of 0 to 255 using mod operation. Generation of chaotic sequence in the range 0 to 1 using circle map with initial condition and control parameters is done. By XORing the pixel array and the chaotic sequence an intermediate cipher is generated. This intermediate cipher image is shuffled to get the final cipher array. The resultant cipher array is transformed to get the final cipher image. The initial conditions and map parameters are secret keys. The decryption process is reverse operation of encryption [13].

In this paper, Shima Ramesh Maniyath1 and Supriya M, propose a secure and computationally feasible image and video encryption/decryption algorithm based on DNA sequences. The main aim was to reduce the big image encryption time. A plain image ‘Á’ of size MxN is considered for encryption process. A new image A1 is obtained by confusing the input plain image with a scrambling sequence generated by the DNA sequence. The scrambling of image is done with the help of Arnold cat map. Next another image A2 is obtained by XORing the image A1 with DNA template B1 which is generated by the second DNA sequence. This process is repeated for 2 rounds and at the end of 2 rounds, a cipher image is obtained. In this paper for generating the DNA template/sequence DNA digital coding technology is used. For any pixel, the range of its gray value is 0 – 255. Instead of using gray value, four bases i.e. 00, 01, 10 and 11 are replaced by A, T, C and G [14].

VI. SECURITY ANALYSIS OF THE ENCRYPTION SCHEMES

Security analysis can be referred as the art of finding the weakness of a cryptosystem and retrieval of either the whole or a part of a ciphered image or finding the secret key without knowing the decryption key of the algorithm. There are many techniques available for applying analysis, depending on what access the analyst has to the plaintext, cipher text, or other aspects of the cryptosystem. Some of the most common types of attacks to encrypted images are discussed as below [1], [13]:

A. Key Space Analysis

The number of try's to find the decryption key by checking all possible keys refers to key space of the cryptosystem that grows exponentially with increasing key size. That is doubling the key size for an algorithm does not simply double the required number of operations, but rather squares them. For example an algorithm with a 128 bit in key size defines a key space of 2128, which takes about 1021 years to check all the possible keys, with nowadays high performance computers. Hence a cryptosystem with large key size looks computationally robust against a brute force attack.

B. Key Sensitivity Analysis

Another requirement for a good image encryption scheme is sensitiveness to the secret key used. The change in a single bit of the secret key should produce a completely different encrypted or the decrypted image.

C. Statistical Analysis

Statistical analysis of image demonstrates the relationship between the original and ciphered image. Therefore, ciphered image must be completely different from the original. For an image there are many ways to determine whether the ciphered image leaks any information about the original image. The histograms and the correlations of two adjacent pixels in the plain image as well as in the cipher image are used for statistical analysis of the encryption scheme discussed. An image-histogram describes the image-pixels distribution by plotting the number of pixels at each intensity level. The histograms give the statistical characteristics of an image. If the histograms of the encrypted image are same as the random image, the encryption algorithm has good performance. Histograms for each of the encryption scheme discussed reveal the fact that the random numbers generated from the chaotic map are uniformly distributed like white-noise. The Histograms of the discussed schemes consists of spikes that are almost uniformly distributed and significantly different from those of the original images and therefore bear no statistical resemblance to the plain-image. Hence they do not provide any clue to employ any statistical attack on the image encryption technique discussed.

D. Correlation co-efficient analysis

In addition to the histogram analysis, study of the correlation between two horizontal, vertical and diagonal diagonally adjacent pixels of the plain image and the encrypted image is used. In case of plain image each pixel is usually highly correlated with its adjacent pixels either in horizontal, vertical or diagonal directions where as for encrypted image these correlation will be very small. A high correlation value implies the best match between the plain and cipher images. This means that if the correlation coefficient of the plain image and the deciphered image is large, then there is maximum similarity between the two images. The correlation coefficients of the adjacent pixels of the ciphered image obviate that the discussed algorithm has a good ability of diffusion and confusion and hence are highly resistive against the statistical attack

E. Information entropy analysis

For testing the robustness of the encryption algorithm, the concept of entropy is also used. Theoretically, a true random system should generate 2^8 symbols with equal probability, i.e., $m = \{m_1, m_2, m_3, \ldots, m_2{}^8\}$ for 8 bit depth. The entropy of the plain images and the ciphered images are compared. From this analysis it is clear that the entropy of the ciphered image is approximately equal to 8, which proves the ability of the encryption technique against the entropy attack.

F. Differential Analysis

The aim of this analysis is to determine the sensitivity of the encryption algorithm to slightest changes. If an opponent can create a small change (e.g. one pixel) in the plain image to observe the results, this manipulation should cause a significant change in the encrypted image. Then the opponent is not able to find a meaningful relationship between the original and encrypted image with respect to diffusion and confusion. Hence the differential attack loses its efficiency and become useless. Two criteria NPCR and UACI are used to test the sensitiveness of a single bit change the plain-image. Number of pixels change rate (NPCR) is defined as the percentage of different pixel numbers between two encrypted images, whose plain images have only one pixel difference. Unified average changing intensity (UACI) is defined as the average intensity of differences between 2 cipher images, corresponding to plain images that have only one pixel difference. The high values of these two parameters Indicate that small change in plain image creates significant changes in the ciphered images. Hence the discussed algorithms are highly resistive against differential attack.

VII. COMPAIRSON OF CHAOTIC MAPS

All the encryption algorithms discussed here employed different security analysis as mentioned in the previous, to validate the good performance and evaluate the robustness of a cryptosystem. All the security analysis details are concluded in the form of table as shown in Table II. From the table an analysis can be made of each method used for image encryption using chaos theory.

TABLE II. COMPAIRSON OF VARIOUS CHAOS BASED CRYPTOGRAPHY TECHNIQUES

<table>
<tr><th>Reference</th><th>Chaotic map used</th><th>Features</th></tr>
<tr><td>[7]</td><td>Lorenz
Chen
Lu</td><td>Key space - Large
Key Sensitivity - Medium
Correlation coefficient
<table>
<tr><th>Coefficient</th><th>Plain image</th><th>Cipher image</th></tr>
<tr><td>Horizontal</td><td>0.9791</td><td>0.0052</td></tr>
<tr><td>Vertical</td><td>0.9357</td><td>0.0539</td></tr>
<tr><td>Diagonal</td><td>0.9183</td><td>0.1141</td></tr>
</table></td></tr>
<tr><td>[8]</td><td>Lorenz,
Baker</td><td>Key space – 2^{128}
Key Sensitivity – High
Correlation coefficient
<table>
<tr><td>Horizontal</td><td>0.9598</td><td>-0.003</td></tr>
<tr><td>Vertical</td><td>0.9763</td><td>-0.0013</td></tr>
</table>
Average Entropy – 7.9973</td></tr>
<tr><td>[6]</td><td>Henon map</td><td>Key space – 2^{128}
Key Sensitivity – High
Correlation coefficient
<table>
<tr><th>Coefficient</th><th>Plain image</th><th>Cipher image</th></tr>
<tr><td>Horizontal</td><td>0.9976</td><td>0.0096</td></tr>
<tr><td>Vertical</td><td>0.9924</td><td>0.0038</td></tr>
</table>
Average Entropy – 7.9904
NPCR – 0.0015% & UACI – 0.0005%</td></tr>
<tr><td>[9]</td><td>Logistic map</td><td>Key space – 10^{45}
Key Sensitivity – High
Correlation coefficient
<table>
<tr><th>Coefficient</th><th>Plain image</th><th>Cipher image</th></tr>
<tr><td>Horizontal</td><td>0.9278</td><td>0.0965</td></tr>
<tr><td>Vertical</td><td>0.9609</td><td>0.1086</td></tr>
<tr><td>Diagonal</td><td>0.9060</td><td>0.0161</td></tr>
</table>
Average Entropy – 7.9996
NPCR – 99.6231& UACI – 33.4070</td></tr>
<tr><td>[10]</td><td>Chaotic coupled map lattices, Chaotic trigonometric map</td><td>Key space - 2^{302}
Correlation coefficient
<table>
<tr><th>Coefficient</th><th>Plain image</th><th>Cipher image</th></tr>
<tr><td>Horizontal</td><td>0.9341</td><td>0.0014</td></tr>
<tr><td>Vertical</td><td>0.9634</td><td>0.0036</td></tr>
<tr><td>Diagonal</td><td>0.9402</td><td>0.0027</td></tr>
</table>
NPCR – 0.25% & UACI – 0.19%</td></tr>
<tr><td>[11]</td><td>Arnold Cat map</td><td>Key space – 2^{148}
Key Sensitivity – High
Correlation coefficient
<table>
<tr><th>Coefficient</th><th>Plain image</th><th>Cipher image</th></tr>
<tr><td>Horizontal</td><td>0.9156</td><td>0.001</td></tr>
<tr><td>Vertical</td><td>0.8808</td><td>0.006</td></tr>
<tr><td>Diagonal</td><td>0.8603</td><td>0.091</td></tr>
</table>
Average Entropy – 7.9981
NPCR – 99.62 & UACI – 33.19</td></tr>
<tr><td>[12]</td><td>Chirikov map ,
Chebyshev map</td><td>Key space - 2^{167}
Key sensitivity – High
Correlation Coefficient
<table>
<tr><th>Coefficient</th><th>Plain image</th><th>Cipher image</th></tr>
<tr><td>Horizontal</td><td>0.9404</td><td>0.0088</td></tr>
<tr><td>Vertical</td><td>0.9299</td><td>-0.0087</td></tr>
<tr><td>Diagonal</td><td>0.9257</td><td>-0.0060</td></tr>
</table>
Average Entropy – 7.9902
NPCR – 99.609 & UACI – 33.464</td></tr>
<tr><td>[13]</td><td>Circle map</td><td>Key space – 2^{256}
Key sensitivity – High
Correlation Coefficient
<table>
<tr><th>Coefficient</th><th>Plain image</th><th>Cipher image</th></tr>
<tr><td>Horizontal</td><td>0.9712</td><td>0.0012</td></tr>
<tr><td>Vertical</td><td>0.9698</td><td>0.0032</td></tr>
<tr><td>Diagonal</td><td>0.9861</td><td>0.0058</td></tr>
</table>
Average Entropy – 7.9902
NPCR – 99.63 & UACI – 33</td></tr>
<tr><td>[14]</td><td>Arnold map</td><td>Correlation Coefficient
<table>
<tr><th>Coefficient</th><th>Plain image</th><th>Cipher image</th></tr>
<tr><td>Horizontal</td><td>0.9489</td><td>-0.0041</td></tr>
<tr><td>Vertical</td><td>0.9473</td><td>-0.0089</td></tr>
</table>
NPCR – 0.0015%
UACI – 0.004%</td></tr>
</table>

VIII. CONCLUSION

The security of digital images has become highly important for communication over open networks and the internet. In this survey paper, the existing chaos based image encryption schemes have been discussed and analyzed to validate their performance against different types of attacks. To conclude, all the encryption schemes are useful for real time image encryption and each scheme is unique in its own way which is appropriate for different applications. Security can be enhanced by having multiple chaotic maps for image encryption. Also there are many more chaotic maps that need to be explored. To name few we have Duffling map, Horseshoe map, Ikeda map, Gauss map etc. Hence encryption that can be referred as a scientific art which is ever changing and fast growing should always exhibit high rate of security.

REFERENCES

[1] Ali Soleymani, Zulkarnain Md Ali, and Md Jan Nordin," A Survey on Principal Aspects of Secure Image Transmission", World Academy of Science, Engineering and Technology 66 2012, pp 247 – 254.

[2] Monisha Sharma, Manoj Kumar Kowar" Image Encryption Techniques using Chaotic Schemes: A Review", International Journal of Engineering Science and Technology Vol. 2(6), 2010, pp 2359-2363.

[3] Abhinav Srivastava," A survey report on Different Techniques of Image Encryption", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 6, June 2012.

[4] Pooja Mishra, Biju Thankachan," A Survey on Various Encryption and Key Selection Techniques", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 7, January 2013, ISSN: 2277-3754.

[5] Alireza Jolfaei, Abdolrasoul Mirghadri," An Image Encryption Approach using Chaos and Stream Cipher", Journal of Theoretical and Applied Information Technology, pp 117 – 123

[6] Somaya Al-Maadeed, Afnan Al-Ali, and Turki Abdalla, A New Chaos-Based Image-Encryption and Compression Algorithm", Hindawi Publishing Corporation, Journal of Electrical and Computer Engineering, Volume 2012, Article ID 179693.

[7] K.Sakthidasan Sankaran and B.V.Santhosh Krishna," A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of information and Education Technology, Vol. 1, No. 2, June 2011.

[8] A. Anto Steffi, Dipesh Sharma," Modified Algorithm of Encryption and Decryption of Images using Chaotic Mapping", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 2, February 2013.

[9] Hazem Mohammad Al-Najjar, Asem Mohammad AL-Najjar," Image Encryption Algorithm Based on Logistic Map and Pixel Mapping Table".

[10] Sodeif Ahadpour, Yaser Sadra," A Chaos-based Image Encryption Scheme using Chaotic Coupled Map Lattices.

[11] Kamlesh Gupta1, Sanjay Silakari," New Approach for Fast Color Image Encryption Using Chaotic Map", Journal of Information Security, 2011, 2, 139-150

[12] Chong Fu, Jun-jie Chen, Hao Zou, Wei-hong Meng, Yong-feng Zhan, and Ya-wen," A chaos-based digital image encryption scheme with an improved diffusion strategy", Optical Society of America, 30 January 2012 / Vol. 20, No. 3 /pp 2363 – 2378.

[13] D. Chattopadhyay1, M. K. Mandal1 and D. Nandi," Symmetric key chaotic image encryption using circle map", Indian Journal of Science and Technology, Vol. 4 No. 5 (May 2011) ISSN: 0974-6846, pp 593 – 599.

[14] Shima Ramesh Maniyath1 and Supriya M," An Uncompressed Image Encryption Algorithm Based on DNA Sequences, Computer Science & Information Technology (CS & IT), CCSEA 2011, CS & IT 02, pp. 258–270