# A Review on Multiple Chaotic Maps for Image Encryption with Cryptographic Technique

Govind Chandra
U.T.U. Deharadun
B.T.K.I.T
Dwarahat

Naveen Chandra
U.T.U. Deharadun
B.T.K.I.T
Dwarahat

Swati Verma
U.T.U. Deharadun
B.T.K.I.T
Dwarahat

## ABSTRACT
In the present time**,** Due to the rapid growth of digital communication and multimedia application, security becomes an important issue of communication, storage and transmission of digital data such as image, audio and video. Chaotic map based encryption is one of the ways to ensure high security of the image data. Encryption technique are used in many fields such as medical science, military, geographic satellite images. Thus due to this protecting the image data confidentiality, integrity, security, privacy as well as the authenticity has become an important issue for communication and storage of images via insecure channel like internet. Modern cryptography technique provides essential techniques for securing information and protecting multimedia data. In recent years, many encryption technology have been proposed. In this paper, first a general introduction given for cryptography and images encryption and followed by discussion of different type of chaotic based image encryption techniques and reviewed the related works for each technique. , At last, The main purpose of this paper is to help in design of new chaotic based image encryption techniques in future by studying the behavior of several existing chaotic based image encryption algorithms.

## Keywords
Cryptography, Decryption, Encryption, Image Encryption.

## 1. INTRODUCTION
In the past few days highly growth of digital and multimedia technology, image protection has become an important issue for communication of digital images through the networks and encryption is the one of ways to provide the security of digital images. Image encryption techniques try to convert original image to another image that is hard to understand, to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. Image encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. Furthermore, special and reliable security in Storage and transmission of digital images is needed in many applications, such as cable-TV, online personal photograph album, medical imaging systems, military image communications and confidential video conferences, etc. Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions making such algorithms hard to break in practice by any adversary. Therefore to prevent multimedia information from non-authorized users, cryptography gives an important role for digital content's security. There are many researchers, which noticed that there is a tight relationship between cryptography and chaos and several characteristics of chaotic systems have their corresponding similarity in traditional cryptosystems The advantages of chaotic based image encryption scheme are easy to implement, faster encryption speed and strong against attacks. Many image encryption schemes based on chaotic have been proposed. The sensitivity to initial value of chaotic system is widely applied to information encryption, the relevant chaos encryption and chaos password research project which put forward by experts and scholars is also more and more.

### 1.1 What is Image Encryption?
Image encryption is an intelligent hiding of information. An original important and confidential plaintext is converted into cipher text that is apparently random nonsense. This cipher text can be saved or transmitted over the network. At the receiver, the cipher text can be transformed back into the original plaintext by using a decryption algorithm The main idea in the image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. The image data have special properties such as bulk capacity, high redundancy and high correlation among the pixels that imposes special requirements on any encryption technique. The most common technique of secure the digital images is to scramble the digital data such that original message of the documents should not be known. There are several approaches to achieve this for example steganography, compression, digital watermarking and cryptography. In this paper we focus on the encryption techniques of digital image based on the chaos mapping. Basically image encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key and the transforming information using "encryption algorithm" into a form that cannot be deciphered without a decryption key. On the other hand, decryption OF image retrieves the true information from the encrypted form image. There are several digital image encryption systems to encrypt and decrypt the image data, and there is not available the single encryption algorithm that satisfies the different image types. The encryption techniques based on the chaos mapping provides the encrypted digital images to hold the multilevel encryption method and also decreases the computational complexity of the encryption process. Most of the algorithms specifically designed to encrypt digital images are proposed in the mid-1990s. There are two major groups of image encryption algorithms: (a) non-chaos selective methods

and (b) Chaos-based selective or non-selective methods. Most of these algorithms are designed for a specific image format compressed or uncompressed, and some of them are even format compliant. There are methods that offer light encryption (degradation), while others offer strong form of encryption. Some of the algorithms are scalable and have different modes ranging from degradation to strong encryption. The encryption techniques based on the chaos have different types of applications in various areas for examples the internet communication, military, health care, mapping and positioning, picture messaging applications on cell-phones, multimedia systems, medical imaging, Tele-medicine, privacy and government documents etc. The evolution of image encryption process is moving towards a future of endless possibilities. Everyday new methods of encryption techniques are discovered.

## 1.2 What is Cryptography?

Cryptographic techniques help secure transmission and storage of data. Cryptography involves the encoding of image at senders side which converts the image so that the contents are not understandable called Encryption and Decryption at receivers side to obtain the original image. Even if the eavesdropper gets access to the image one will not understand the contents. In applications like aeronautic, military, medical secure communication is the most important concern. Nowadays due to high digitalization more information is shared in form of images. Thus efficient image encryption technique is the need of present time. The encryption of images is much difficult than encryption of text or binary data because images have higher correlation and redundancy among pixels. Thus different encryption algorithms like AES, DES etc. are inefficient for image encryption. Chaotic functions are being used for image encryption rather than the traditional algorithms.

## 1.3 What is Chaotic Systems?

The term chaotic comes from chaos. Chaos does not have a defined meaning; it may refer to a state that does not have deterministic behavior. Chaotic systems depend completely on initial condition. These systems are dynamic therefore with a chaotic system the results vary largely with a little change in initial condition. Chaotic theory is a field of mathematics and has various applications in meteorology, economics, philosophy etc. Various image encryption techniques have been proposed during the last years based on multiple one-dimensional, two-dimensional or higher-dimensional chaotic systems, coupled chaotic maps etc. The chaotic cryptography is gaining more attention than others because of its lower mathematical complexity & better security. Chaotic theory concerns deterministic systems whose behavior can be predicted. These systems can be predicted for a while and then they become random. Chaotic theory was summarized by Edward Lorenz as follows "When the present determines the future, but the approximate present does not approximately determine the future." Chaos-Based techniques have been extensively studied in the recent years, because their properties lead to the potential cryptography.

# 2. LITERATURE REVIEW

2.1 One of the works by Asia Mahdi Naser Alzubaidi, showed an image encryption scheme based on 3D logistic transform, it divided the image in different color channels of YCBCR and applied different techniques of selective encryption and chaotic encryption. On Y component a selective encryption algorithm is performed to protect the sensitive data. Further the confusion process is adopted by using 2D Arnold cat transformation to make more distortion of the relationship among adjacent pixels of Y image and to hide the statistical structure of pixels. Scrambling process depend on row-column method applied independently on Cb and Cr components .Then to diffuse the correlation between crypto-image and plain-image 2D Baker on scrambling CbCr channels and Henon Chaotic map on encrypted Y channel are used [1].

2.2 Secured medical image transmission using chaotic map by Bremnavas, B.Poorna and I.Raja Mohamed [2], used only Henon chaotic map for medical image encryption thus making it an easy task for attackers to decrypt and limited their work to medical images only. First step in this work is to generate the noisy signal using the Chaotic Henon map. The user sets the cover region dynamically by setting value for control parameters. The input patient medical image data has been taken. Here the Henon equations are generated with the signal in both 'x' and 'y' axes. This gives the advantage of sending two patients medical images at a single transmission. For example, the first patient medical is added in 'x' axis and then another one is added in 'y' axis.

2.3 Research by ChinchuThampi and Dona Jose [3], utilized 3D chaotic map. It included a key stream generation process, diffusion-substitution and masking process. For diffusion first 3D chebyshev map is iterated 80 times and its output as input to 3D logistic map, then for substitution S-boxes were used and the last step of masking was shuffling parts of image. A set of three hexadecimal values & floating point values are used for generation of initial conditions of chaotic maps. The first stage consists of key stream generation using three dimensional chebyshev map and a three dimensional logistic map. First a set of random keys are generated using 3D chebyshev maps given as 'Fn(x) = cosnθ where x=cosθ' and that keys in turn are used as initial conditions for three dimensional logistic maps. Then these random values generated using these maps are used for forward encryption. Then an inverse encryption is performed. Additionally to improve security and to have proper substitution S-box of AES is used [3].

2.4 Lalita Gupta, Rahul Gupta and Manoj Sharma [4], proposed an encryption scheme which focused on disturbing the correlation among image pixels. They used pixel shuffler horizontally as well as vertically, 2D bakers map described with the following formulas $B(x, y) = (2x, y/2)$ When $1/2 < x < 1$, $B(x, y) = (2x -1, y/2 + 1/2)$ When $0 < x < 1/2$ and created confusion in the image with bit XOR with noise image nonlinear (liapunav exponential) function operation to satisfied condition of chaos. The diffusion template is created by randm number generator based on Gaussian distribution and is capable of providing the key length of 64 bits although its length can be extended further.

2.5 Rajinder Kaur et al [5], International Journal of Computer Science and Mobile Computing, has introduced a region based selective image encryption, it has followed selective compression where parts of the image that contain vital information are compressed in a lossless way whereas regions containing unimportant information are compressed in a lossy manner. Henon map is used for key generation. The image is divided into blocks and then these blocks are shuffled. The transformed image is fed to blow-fish algorithm. This algorithm is generally used for textually data encryption.

Using blow-fish algorithm is one drawback of this scheme as it would make the process slow and it is not as much reliable.

2.6 Ansari et al [6], "An Image Encryption Approach Using Chaotic Map in Frequency Domain",The DCT [] of the image is calculated and also the image is shuffled using 2D bakers map. Two bakers map are used one with initial set keys and other is used with Gaussian image generated with mean variance. The results of both DCT and bakers maps are XORed iteratively. Also the diffusion template is created by random number generator based on Gaussian distribution. The technique uses Bakers map and capable of providing the key length of 128 bits although it's length can be extended further. The technique is simulated using Matlab.

2.7 Pawan N. Khade and Prof. Manish Narnaware [7], "3D Chaotic Functions for Image Encryption". This paper proposes the chaotic encryption algorithm based on 3D logistic map, 3D Chebyshev map, and 3D, 2D Arnolds cat map for color image encryption. Here the 2D Arnolds cat map is used for image pixel scrambling and 3D Arnold's cat map is used for R, G, and B component substitution. 3D Chebyshev map is used for key generation and 3D logistic map is used for image scrambling. The Chebyshev map is used for public key encryption and distribution of generated private keys. Arnold cat map perform the dual encryption, firstly it performs the shuffling and secondly it performs the substitution. Using ACM the correlation among the adjacent pixels can be disturbed completely. On the other hand, the 3D cat map can substitute grey/ colour values. We implemented 3D ACM on both colour and grayscale image and following are the results.

2.8 Ramesh Kumar yadava et al [8], "A New Approach of Colour Image Encryption Based on Henon like Chaotic Map". The Henon like chaotic system is converted in to one-dimensional chaotic map which is mathematically defined as: $Xn+2 = 1 - a_{X2n+1 + bsin (wxn)}$. The colour image is transformed in to its (RGB) 3 pieces of component matrix. One dimensional Henon chaotic map obtained takes R component of color image to generate the random bit stream. The bit values obtained is bit XOR with the original pixel values of R component of original transform matrix. The vector result of G and B component of transform color image with the matrix after bit XOR obtained from the previous stage produce the cipher image.

2.9 Priyanka Gupta et al [9], "Image Encryption Based on Arnold Cat Map and S-Box". This scheme is good and efficient technique using Arnold map of shuffling pixels and the shuffled image is encrypted by nonlinear byte-substitution using S-box. These two steps are performed for k iterations. Although AES and DES are useless in image encryption, the concept of S-box of AES can be used in substitution phase of image encryption. During image encryption, Arnold cat map is also introduced to shuffle the pixel positions of the image in to order to disturb the high correlation among the pixels. As a result, the algorithm is secure against statistical attack.

2.10 In the confusion stage, in [10] by Kwok-Wo Wong et al, both the permutation on pixel position and the change of pixel value are carried out at the same time while the diffusion process remains unchanged. As a result, the pixel value mixing effect of the whole cryptosystem is contributed by two levels of diffusing operations: the modified confusion process and the original diffusion function. As the diffusion effect is not solely contributed by the diffusion function, the same level of security is achieved in fewer cipher rounds. The encryption speed is thus accelerated. Before performing the pixel relocation, diffusion effect is injected by adding the current pixel value of the plain image to the previous permuted pixel and then performs a cyclic shift. Other simple logical operations such as XOR can be used instead of the addition operation. The shift operation can also be performed before addition.

2.11 Wadia Faid Hassan Al-Shameri in [11], investigate the dynamical properties of the Hénon map which exhibit transitions to chaos through period doubling route and focus on the mathematics behind the map. It includes analysis of the fixed points of the Hénon map and algorithm to obtain Hénon attractor. Implementation of that dynamical system can be done using MATLAB programs and are used to plot the Hénon attractor and bifurcation diagram in the phase space. A strange attractor is a concept in chaos theory that is used to describe the behaviour of chaotic systems. The Hénon map has yielded a great deal of interesting characteristics as it was studied. At their core, the Hénon map is basically a family of function denoted by: $x_{n+1} = 1\text{-}ax_n^2 + y_n$ & $y_{n+1} = bx_n$

2.12 In [12] Nilesh Y. Choudhary encrypts a gray image using 2D Arnold map. The image is divided into blocks, size from 4*4 to N/2 * N/2. Each block is one by one feed to arnold map and finally an encrypted image is obtained. This scheme is an easy one using only one map but arnold map have a feature of giving back the same image after some number of iterations so there is a chance of reaching back to the original image.

2.13 In [13] Mayak Mishra et al. use an external key of 80 bits which is divided into blocks of 8 bit each. First logistic map is used Xn+1 = 3.9999Xn (1-Xn), Yn+1 = 3.9999Yn (1-Yn). Next step is to read three consecutive bytes, these three bytes represent the values of red, green and blue (RGB) color respectively. To make the cipher more robust against any attack, the secret key is modified after encrypting a block of sixteen pixels of the image. Then encryption is performed on first 16 bits of the image using the following formula: ((R)10 + (K4)10 + (K5)10) mod 256, ((G)10 + (K5)10 + (K6)10) mod 256, ((B)10 + (K6)10 + (K4)10) mod 256. After encryption of the 16 bit block, the session key is modified using the formula: (Ki)10 = ((Ki)10 + (K10)10) mod 256, ($1 \leq i \leq 9$). For security analysis key space analysis was done time analysis etc.

2.14 Reema Rhine and Nikhila T Bhuvan in [14], proposed a survey of image hiding. Using Rubik's cubic data hiding as Rubik's Cubic can scramble the sequence of an original sequence, it can be applied for information encryption or information hiding. In the processing, one can easily find out that the cubic located in the corner, center and sides are transformed only to corner, center and side locations respectively. In the beginning, the hidden data (treated similar as an image) is partitioned into different unit block size such as pixel based, 3*3 pixels based, or other n*n pixels based. Then, 54 units will be selected sequentially and transformed into 6 faces according to the six faces of a Rubik's cubic by designated an index number. The data hiding process is performed from left to right and then top to bottom in the cover image, i.e. horizontally, with the covert information.

2.15 In [15], the relationship between the parameters of Henon map is studied, and the chaos of Henon map is also discussed based on different coupled networks. From the

simulate results, we found with the increasing of parameter *a* the chaos of Henon map will be emerged. At the same time, the transition from non-chaotic to chaotic in coupled networks is exhibited. The Lyapunov exponent and henon map and the relationship between the parameter a and Henon map. For $y_n+1=b*x_n$, we can simple get picture y is similar with picture x, the difference is only a coefficient. So we can get the relationship between the parameter a and Henon map only by studying the relationship between the parameter a and the parameter x. Lyapunov exponent is a kind of factor which can describe the way to get the chaotic state in the iterative process. We can definite as following when symbol λ stands for it: This work was supported by National Science Foundation of China (Grant Nos. 61153001 and 10971245)and the Independent Research Foundation of the Central Universities (Grants Nos. DC110103 and DC110311).

## 3. CONCLUSION

In this paper, many of the important encryption techniques have been discuss and analyzed in order to make familiar with the various encryption algorithms used in for image encryption which has been transferred over network. The results of the simulation show that every algorithm has advantages and disadvantages based on their techniques which are applied on images. On the basis of study of all the above mentioned research papers thoroughly, the following suggestions can be drawn: To protect multimedia contents, Chaos based algorithm should be implemented. More complex & compressed algorithm should be used to provide high speed and security to the System. Modified version of various algorithms are used to increase the security level and to achieve the substantial security, we can use existing image encryption techniques but only few existing image encryption techniques fulfill this requirement. The security analysis parameter shown that the existing image encryption techniques are resistive against the different attacks like statistical attacks, key sensitivity analysis attack etc.

## 4. REFERENCES

[1] Asia Mahdi, Naser Alzubaidi, "Selective Image Encryption with Diffusion and Confusion Mechanism", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) - Volume 4, Issue 7, July 2014

[2] Bremnavas1, B.Poorna2 and I.Raja Mohamed, "Secured medical image transmission using chaotic map", Computer Science and Engineering Elixir Comp. Sci. Engg. 54 (2013) 12598-12602

[3] Chinchu Thampi1, Dona Jose," More Secure Color Image Encryption Scheme Based on 3D Chaotic Maps", International Journal For Advance Research In Engineering And Technology-Vol. 1, Issue IX, Oct.2013

[4] Lalita Gupta1, Rahul Gupta and Manoj Sharma, "Low Complexity Efficient Image Encryption Technique Based on Chaotic Map", International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 11 (2014), pp. 1029-1034

[5] Rajinder Kaur1, Er. Kanwalpreet Singh, "Comparative Analysis and Implementation of Image Encryption Algorithms", International Journal of Computer Science and Mobile Computing (IJCSMC) - Vol. 2, Issue. 4, April 2013, pg.170 – 176

[6] Shoaib Ansari1, Neelesh Gupta2, Sudhir Agrawal, "An Image Encryption Approach Using Chaotic Map in Frequency Domain", International Journal of Emerging Technology and Advanced Engineering-Volume 2, Issue 8, August 2012

[7] Pawan N. Khade and Prof. Manish Narnaware, "3D Chaotic Functions for Image Encryption", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012

[8] Ramesh Kumar yadava, Dr. B. K.singh*, S.K.sinha*, K. K.pandey, "A New Approach of Colour Image Encryption Based on Henon like Chaotic Map", Journal of Information Engineering and Applications ISSN 2224-5782 (print) ISSN 2225-0506 (online)-Vol.3, No.6, 2013

[9] Priyanka Gupta, Sonia Singh and Isha Mangal, "Image Encryption Based On Arnold Cat Map and S-Box", International Journal of Advanced Research in Computer Science and Software Engineering-Volume 4, Issue 8, August 2014

[10] Kwok-Wo Wong, Bernie Sin-Hung Kwok, "An Efficient Diffusion Approach for Chaos-based Image Encryption", Journal of Information Engineering and Applications ISSN 2224-5782 (print) ISSN 2235-0516 (online)-Vol.3, No.7, 2014

[11] Wadia Faid Hassan Al-Shameri, "Dynamical Properties of the Hénon Mapping", Int. Journal of Math. Analysis, Vol. 6, 2012, no. 49, 2419 - 2430

[12] Nilesh Y. Choudhary, Ravindra K. Gupta, "Partial Image Encryption based on Block wise Shuffling using Arnold Map", International Journal of Computer Applications (0975 – 8887) Volume 97– No.10, July 2014

[13] Mayank Mishra, Prashant Singh, Chinmay Garg, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 7 (2014), pp. 741-746

[14] Xuelian Sun, Kuifeng Zheng1, Lidong Wang1, Wei Zhao1, Xuefeng Sun2, "Chaos Of Henon Map Based On The Coupled Networks", Journal Of Theoretical And Applied Information Technology 10th January 201 3. Vol. 47 No.1

[15] Reema Rhine, Nikhila T Bhuvan, "Image Scrambling Methods for Image Hiding: A Survey", IJCSNS International Journal of Computer Science and Network Security, VOL.1 5 No.2, February 2015.

[16]