A proficient Image Encryption using Chaotic Map Approach

Deepshikha Rathore
Department of Information and Technology
SATI , VIDISHA INDIASATI, VIDISHA INDIA

Anil Suryavanshi
Department of Information and Technology
SATI , VIDISHA INDIASATI, VIDISHA INDIA

ABSTRACT
Important information for general users, advanced data and multimedia, arts, entertainment, advertising, education, training and business sectors have, the faster and more digital and multimedia applications development are transmitted through the network that can be accessed by should not be. Therefore confidentiality, integrity, security, confidentiality, authenticity of the images as well as the issue of communication and storage of images has become an important issue for the defense. In recent years, the technology to protect confidential images are applied have developed various encryption and unauthorized users. Letter aspects and chaotic map based on a review of existing different image encryption technology. This paper introduces a general discussion of a technology for the first time to review and image encryption chaotic system and various chaotic image encryption technology based and related tasks. Finally, the main objective of this paper is designed to help new chaotic image encryption technology based on the future behavior of the current chaos-based image encryption algorithms studied.

Keywords
Image encryption, chaotic map, Logistic map, Arnold cat map, Baker map.

1. INTRODUCTION
A large number of digital images for processing computer networks and digital multimedia development, rapid growth can only be transmitted in an open system. Unauthorized use of images in both research and application protection has become a common concern. Such a large data capacity and conventional data encryption techniques as intrinsic properties of high correlation between pixels in a digital image might not be appropriate for images. Many researchers, such aperiodicity, ergodicity primary rules and parameters and properties as high sensitivity Motivated by chaotic pseudo-randomness, chaos-based image encryption schemes investigated and analyzed different.

Chaotic maps are used for image encryption which involves features like non-deterministic, random, periodicity etc. In

Chaotic map, logistic map is the common one. It was discovered by R. M. May in 1976 [3].

$$X_{i+1} = rx_n (1-x_n) \quad (1)$$

It exhibits chaotic properties which is derived from non-dynamical discrete systems and generates a random sequence, defined as: X_0 is the initial value for the sequence; r is a parameter which is user defined and lies between 3 and 4 to generate a chaotic sequence; and n is the number of iterations. Xn lies between 0 and 1. The random sequence generated from (1) exhibits chaotic properties and used for encrypting the image. Researchers have obtained following conclusion on the basis of value of r [3]:

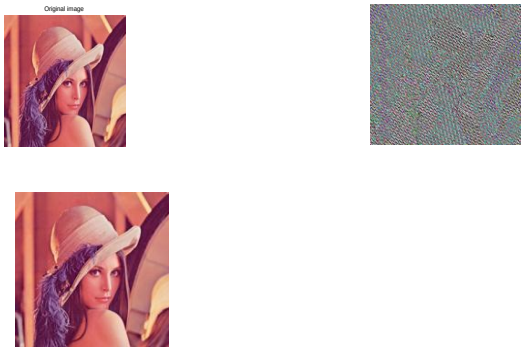
Table 1 Values Of R

Value of r	Xn characteristics
r<1	Xn approaches 0 and steady state
1<r<3	Xn grows as g increases
3<r<3.44	Xn oscillates after some iteration among two values
3.44<r<3.56	Xn oscillates after some iteration among four values
3.56<r<3.82	Xn exhibits chaotic behavior and oscillates for certain values of g near 3.82
3.82<r<4	Xn oscillates among 6,12 and so on values and exhibits chaotic properties

Let's take a M x M image and generate the sequence up to M x M iterations using (1). The random sequence generated from (1) is quantized to binary format with the following equation [4]:

$$H(x) = \begin{cases} 0, & 0 < m(i,j) \le 0.5 \\ 1,, & 0.5 < m(i,j) \le 1 \end{cases} \quad (2)$$

Where, m (i, j) is a random number in the sequence. The quantized sequence H(x) is XORed with each bit of M x M image and produces the encrypted image. For the experimental results, 'lena.jpg' image has been taken. The original, encrypted and decrypted images are shown in Fig. 1. Here, the parameters values we have taken are r=3.93 and X0 = 0.732



(a) Original image (b) Encrypted image
(b) Decrypted image

Fig.1. Logistic Map

The major demerit of logistic mapping is the key sensitivity; which depends on a single system parameter r and an initial condition X0. With increase in control parameters, the statistical complexity decreases. Another disadvantage is occurrence of periodic sequences in chaotic region which is more prone to differential attacks such as chosen plaintext attack. A large amount of secret can be revealed under same conditions.
Due to the disadvantages of logistic map, different versions of chaotic maps have been developed. Here, we have analyzed the common chaotic maps.

B. Baker map
The Baker map is a chaotic map from unit square M x M into itself. The Baker Map is an extension of 1D Tent map. A great amount of diffusion is modeled by couples of Baker map and also exhibits deterministic chaos features. It
forms parameters as encryption key for the encryption of chaotic function. The Baker map after described by Fridrich is denoted by (4).

$$B(a) = \begin{cases} \left(2a, \frac{b}{2}\right), for\ 0 \le a < 0.5 \\ \left(2 - 2a, 1 - \frac{b}{2}\right), for\ 0.5 \le a < 1 \end{cases} \quad (4)$$

Equation (4) shows that if the value of 'a' is expanded by twice horizontally, the value of 'b' contracts by half vertically. Here, the M x M number of sequence generated from Baker map is used to create 1 x M and M x 1 vector respectively. The vectors are then multiplied with each other to form M x M matrix with dynamic values. These values are quantized and XORed bitwise with the M x M original image to form an encrypted image. At the receiver end, the sequence from Baker map is again generated with same initial conditions to gain the original image. By taking a=0.321 and b=0.823, the Baker map encryption to the 'lena.jpg' is shown in Fig.

(a) Original image (b) Encrypted image
(c) Decrypted Image

Fig.2. Baker Map

2. RELATED WORK

Chaotic image encryption has been researched since the last decade. In this regard, some of them have been published; many research papers are discussed below-

Mazleena Salleh, Subariah Ibrahim Ismail Isnin [1] a torus or a work inspired by J. Fridrich which adopts a square, two-dimensional chaotic map below for the purpose of encryption. A chaotic image encryption system is based on a concept developed and was tested on multiple images of different sizes. I had some important values that have occurred in the weak encryption. The algorithm attempts to start some action to increase the encryption strength, so as to enhance research work to eliminate all possible weak keys so. These functions, image transfer and management of the pixel gray scale value to change password pixels are transposing. The original pixel value replacement scattering permutation algorithm encryption status and value to randomize and combines both to hide.

Md. Billal Hussein, Md. Toufikur Rahman, ABM Saadmaan Rahman, Syed Islam to secure and enhance the multimedia communication pixel using 3D rotation and XOR-based encryption techniques chaos by using [2] proposed hybrid encryption technology. Simulation results demonstrate our method against various types of attack presents. Overall there are five steps to complete the encryption process. They are: a) generation of 3D anarchy. B) Histogram generation chaos c) line rotation. D) Column rotation. E) XOR operation.

A Kanso, M Ghebleh [3] the color (or gray scale), namely, Arnold cat map images to a new encryption algorithm is based on a 3D map chaotic. Suggested algorithm an input image of any size, accounts for the third dimension takes RGB values, and the encryption / decryption process is m × 3 × N, where N and M, uses. MR algorithm under study due to a combination of erratic rule, two search terms, chaotic decimates the 3D map of CR and DR, due to the

lack of security of encryption chaotic map based on the direct use of the three sections of the image output the3D and images completely unrecognizable to their outputs uses.

The proposed algorithm is composed of three phases that a secure image encryption algorithm satisfies all requirements. In step 1, the input color image output via RGB color components Cr 3D map of chaotic block according to the rules for image pixels (typical size) permuting are shuffled. In Phase II and III and Dr. mixture is conducted through the use of masking rules pixels revised terms MR and 3D map chaotic mix of both masking.

Young Zhou, Long Bao, CL Philip Chen [4], with a simple structure of the security weakness cryptanalysis problem, the introduction of a new chaotic system to overcome. New chaotic map that integrates two existing 1D chaotic maps to generate a number. To demonstrate the application, he then separate attacks, plain-text attacks, in particular the introduction of a novel image encryption algorithm chosen to tolerate a great confusion and diffusion properties. Set of keys with a single algorithm, which generates a new encrypted image, is completely different from any previous one, each time the application is for an original image. The algorithm is able to ensure the chosen plain-text attack.

Round 4 encryption algorithm structure is proposed. Random Pixel entry, line separation, 1D replacement, line combinations and image rotation: five steps in each round of encryption. The algorithm first, a random pixel in the original image at the beginning of each line, 1-D data matrix according to the 1D, 1D matrix, each row of data values change each procedure inserts a replacement applies different which, 2D Data Matrix combines matrices back row and its position in the original image, and 2D matrix rotates counterclockwise 90 degrees.

The process four times, the final encrypted image receives. We can change the original images as proposed algorithm

randomly different voices with great confusion and diffusion properties encrypted images.

Ch.K. Volos, IM Kyprianidis, I.N. Stouboulos [5], a new approach for the efficient and practical image encryption scheme suggested. The basic idea of this method is a chaotic true random bits generator (TRGB), which has two mutually, coupled identical chaotic circuit, is based on the interaction between, through a gray scale is to encrypt. Two different synchronization event, renowned complete chaotic synchronization and synchronization coupled system recently proposed a new phenomenon, Π- synchronization interval show coexistence proposed inversion phenomenon. According to a chaotic binary sequence generator, the preset keys help XOR- generates gray-scale image pixels.

Sukalyan Mon, Sen. [6], is based on gray-scale images of chaos, a non-adaptive motion a partial encryption algorithm is proposed, which is the main factor, mature. Original gray scale image, the couple's tent encrypted using maps based on the binary code number generator (PRBNG) is decomposed into eight-bit binary plane then. Significant four bit planes, the 5% level of significance in determining the contribution of a small plane on a pixel value is encrypted using keys, which are applied, as determined by the repetition of the tent map based PRBNG relationship goes. A little bit encrypted key with four planes planes are combined to create the final image chipper.

Jing-Yuan Wang, Na Wei, Dou-Dou Zhang [7], the better the image encryption based on the gravity model and chaotic system is presented. The original image generated by the first two chaotic scenes logistics map is tailor. Then modified gravity models using improved the image is diffused. Plain image by changing a pixel to improve the effects of the encrypted image, logistics chaotic system once again is used to spread further. The novel algorithm can resist common attacks that have good effect.

Yicong Zhou, Weijia Cao, C.L. Philip, Chen [8], the proposed bit plane decomposition based image encryption methods to increase security. The algorithm selects a source image a bit plane. This bit of the original image planes using XOR function. The proposed algorithm for the bit-level scrambling permutation algorithm is applied to obtain the encrypted image and combines the processed bit planes. The source image, security key bit plane to generate any bit plane decomposition method, and any permutation bit-level scrambling algorithm can use any image. Simulation results are provided and security analysis.

3. PROPOSED WORK AND SECURITY ANALYSIS OF ENCRYPTION SCHEME

Image encryption and decryption using chaotic map are written in MATLAB. In the encryption process, first the image is read from the file. Then keys are generated using the one dimensional chaotic logistic map. Thus the image is encrypted. The obtained encrypted image is again encrypted through baker map. Thus a completely encrypted output for the image is obtained. Image decryption is performed in the reverse order of encryption. Thus the original image is obtained.

Algorithm of proposed methodology:

In this section we will describe the method that how the proposed algorithm is implemented. We have implemented a chaotic crypto system for image encryption which is based on multiple chaotic maps. In section 4.3.1 we have describe maps which are used for encryption and decryption of the image. Following Steps are followed for encryption process.

Step 1: Read an image of size (M*N).

Step 2: Call Logistic map, for encrypting the image by logistic map.

Step 3: Generate pseudo-random sequence by using logistic map.

Step 4: Apply encryption algorithm between input image and pseudo-random sequence.

Step 5: After performing encryption process we will get a get shuffled image, save that image into a variable and pass it into Baker map for further encryption process.

Step 6: Then, call the Baker function for one more time encrypting the image.

Step 7: Generate pseudo-random sequence by using baker map.

Step 8: Apply encryption algorithm between input image and pseudo-random sequence.

Step 9: After applying encryption algorithm between shuffle image and pseudo-random sequence, and then will get the final encrypted image.

3.1. Image Encryption and Decryption

The output for the proposed method is shown below. First figure shows the plain image that we read. The second figure shows the output of encrypted image. The third decrypted image is shown in the third figure. The figure 3.1 shows the plain image. The figure 3.2 shows the image after encryption process. The figure 3.3 shows the decrypted image.

Fig 3.1 plain image

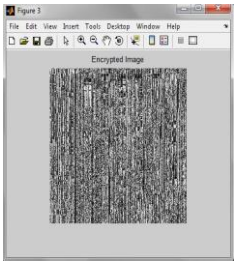


Fig 3.2 Encrypted image

Fig 3.3 Decrypted image

Encryption time of Images

It is the length of time required to encrypt the image. This time required should be low so as to process the image faster. Greater encryption time would consume a lot more time to encrypt the image. So the performance is measured on the basis of time.

Table 2 Encryption Time of different images.

S.No.	Images	Logistic Map	Baker Map
1	Lena	0.169790	0.032689
2	Penguin	0.018848	0.032797
3	Fruit	0.019122	0.032823
4	Cameraman	0.019215	0.034160

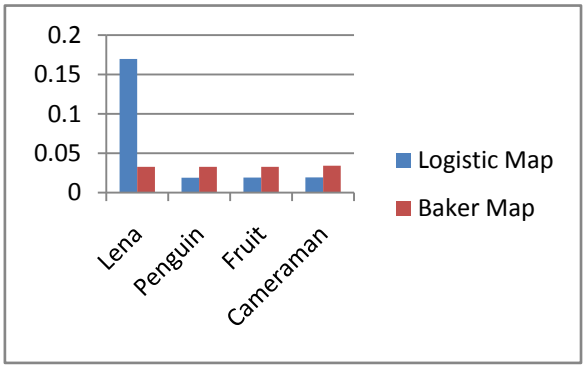


Fig 4 Comparison of Encryption Time of different image

3.2. Histogram Analysis

Defined as how much time per a pixel value histogram of the pixel value is calculated. Cipher plain image to image it is beneficial to prevent leakage of information to a competitor bears no statistical similarity. Figure 5.4 shows a histogram of the image and the field the encrypted image. A plain image histogram contains large spikes. Cipher or a similar histogram of the image is encrypted. It is unlike from the original image and the original or plain image is a statistical similarity. Consequently the suggested image encryption process does not provide a statistical attack.

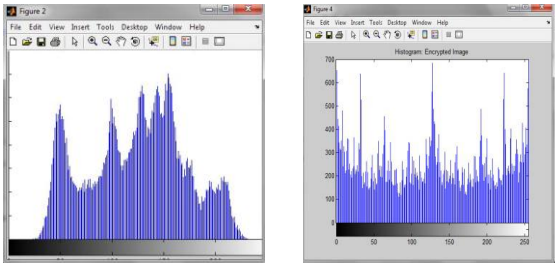


Fig 4.4 Histogram of plain and encrypted image

3.3. Correlation co-efficient analysis

Histogram analysis, plain image, horizontal, vertical and diagonal diagonally adjacent pixels and also in giving the study of the relationship between the encrypted image. Horizontal, vertical or diagonal direction or adjacent pixels with each pixel in the image are added, while the normally high plain, the image correlation is encrypted, will be very small. A high correlation value is plain and cipher out the best match between the images. Plain image and enlarge the image to read the correlation coefficient, the maximum similarity between two images means. Ciphered adjacent pixels of the image of the correlation coefficient. The encryption and decryption algorithm is the ability to have a good discussion and therefore highly resistant against attacks that would not statistical.

Table. 3 Correlation of different images.

S.No.	Images	Logistic Map	Baker Map
1	Lena	1	1
2	Penguin	1	1
3	Fruit	1	1
4	Cameraman	1	1

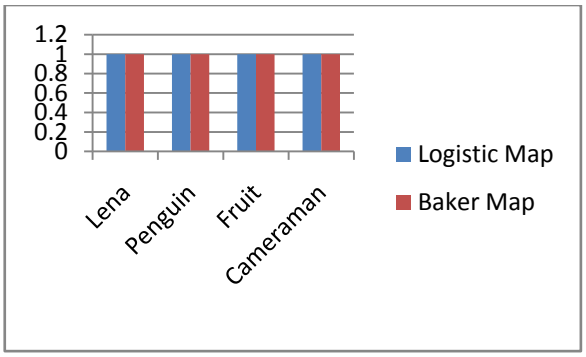


Fig. 5 Comparison of correlation coefficient.

3.4. PSNR (Peak Signal to Noise Ratio)

Peak signal-to-noise ratio, often abbreviated PSNR, the maximum possible power of a signal and noise that affects the fidelity of its representation of an engineering term for the ratio between the powers. PSNR is usually expressed as a logarithmic decibel scale. In this case the original image signal and the noise introduced by encryption error. A high PSNR encrypted image that indicates high quality. PSNR most easily mean squared error (MSE) is defined by.

The PSNR is defined as

$$\text{PSNR}=10\log_{10}\left(\frac{S^2}{\text{MSE}}\right)$$

This equation, M and N are the width and height of the original image. I (i, j) and k (i, j) respectively pixel values of the original image and the encrypted image.

Table 4 PSNR values

S.No.	Images	Logistic Map	Baker Map
1	Lena	40.0361	40.0271

2	Penguin	40.0288	40.0364
3	Fruit	40.0376	40.0368
4	Cameraman	40.0251	40.0265

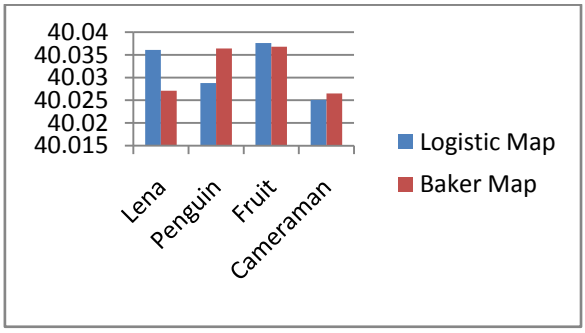


Fig. 6 Comparison of PSNR

4. CONCLUSION

Digital images for communication on security of open networks and the internet have become extremely important. In this paper, the current chaos-based image encryption schemes discussed and against different types of attacks have been analyzed to validate their performance. To conclude, all the encryption schemes are useful for real-time image encryption and are suitable for various applications of each scheme, which is unique in its own way. Image encryption for security can be enhanced by having several chaotic maps. Also needs to be explored that many more chaotic maps. To name a few, we Duffling map, horseshoe map, Ikeda map, the Gauss always must demonstrate a high level of security is an ever-changing, and fast growing as a scientific art that can be sent etc. Therefore encryption maps can be extended to audio and video encryption techniques in future.

5. REFERENCES

[1] Mazleena Salleh, Subariah Ibrahim, Ismail Isnin,"Enhanced Chaotic Image Encryption Algorithm Based on Baker's Map" IEEE 2003.

[2] Md. Billal Hossain, Md. Toufikur Rahman, A B M Saadmaan Rahman, Sayeed Islam, "A new Approach of Image Encryption Using 3D Chaotic Map to Enhance Security Of Multimedia Component" IEEE 2014.

[3] A. Kanso, M. Ghebleh, "A Novel Image Encryption Algorithm based on 3D Chaotic map" Commun Nonlinear SciNumerSimulat Elsevier 2011.

[4] Yicong Zhou, Long Bao, C.L. Phillip Chen, "A New 1D Chaotic System for Image Encryption" Signal Processing 2014.

[5] Ch.K. Volos, I.M. Kyprianidis, I.N. Stouboulos, "Image Encryption Process Based On chaotic Synchronixation Phenomena" 2013.

[6] SukalyanSom, SayaniSen, "A Non-adaptive Partial Encryption of grayscale Images based on Chaos" First International Conference on Computational Intelligence: modeling, techniques and Applications (CIMTA-2013).

[7] Xing-yuan Wang, Na Wei, Dou-dou Zhang, "A Novel Image Encryption Algorithm Based on Chaotic System and Improved Gravity model" 2014.

[8] Yicong Zhou, Weijia Cao, C.L. Philip, Chen, "Image Encryption Using Binary BitPlane" 2014.

[9] Motingsu, Wenying Wen, "An Analysis of Chaos based Security Solution for Fingerprint Data" 2014 Elsevier GmbH.

[10] Mrinal Kanti Mandal, Gourab Dutta Banik, Debassish Chattopadhyay and Debashis Nandi, "An Image Encryption Process Based on Chaotic Logistic Map" IETE Journal 2012.

[11] Jui Cheng and Jiun-In Guo, "A new chaotic key-based design for image encryption and decryption", International Symposium on Circuits and Systems, IEEE, 2000, vol.4.

[12] Gabriel Peterson, "Arnold's Cat Map", Math 45 – Linear Algebra,Fall 1997.

[13] Robert M. May, "Simple mathematical models with very complicated dynamics", Nature 261(5560), 1976.

[14] Jiri Fridrich," Symmetric Ciphers based on Two-Dimensional Chaotic Maps", International Journal of Bifurication and Chaos, vol. 8, no. 6, 1998.

[15] Ibrahim S. I. Abuhaiba1, Hanan M.Abuthraya, Huda B. Hubboub and Ruba A. Salamah, "Image Encryption Using Chaotic Map and Block Chaining", I.J Computer Network and Information Security, vol.7, July 2012.

[16] David Arroyo, Chengqing Li,Shujun Li, Gonzalo Alvarez and Wolfgang A. Halang, "Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm", Chaos, Solitons& Fractals, Elsevier, vol. 41, no. 5, 2008.

[17] Musheer Ahmad and M. ShamsherAlam, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal on Computer Science and Engineering, vol. 2(1), 2009.

[18] Ramesh Kumar Yadava, Dr. B. K.Singh, S. K. Sinha and K. K. Pandey, "A New Approach of Colour Image Encryption Based on Henon like Chaotic Map", Journal of Information Engineering and Applications, vol. 3, no. 6, 2013.

[19] Alireza Jolfaei and Abdolrasoul Mirghadri, "An Image Encryption Approach using Chaos and Stream Cipher", Journal of Theoretical and Applied Information Technology", 2010.

[20] Chittaranjan Pradhan, Shibani Rath and Ajay Kumar Bisoi, "Non Blind Digital Watermarking Technique Using DWT and Cross Chaos", 2nd International Conference on Communication, Computing & Security, Elsevier, 2012.

[21] Uanrong Chen, Yaobin Mao and Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons and Fractals, Elseiver (21), 2004.

[22] Mei Jiansheng, Li Sukang and Tan Xiaomei, "A Digital Watermarking Algorithm Based On DCT and DWT", International Symposium on Web Information Systems and Applications, May 2009.