International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Review of Image Encryption Using Chaos based Techniques

Shourya Chand[1], Ritik Aggarwal[2], Ekansh Dubey[3]

[1]BTECH Computer Science, Bharati Vidyapeeth's College of Engineering New Delhi, A 4, Rohtak Road, Paschim Vihar, Delhi, 110063

[2]BTECH Computer Science, Bharati Vidyapeeth's College of Engineering New Delhi, A 4, Rohtak Road, Paschim Vihar, Delhi, 110063

[3]BTECH Computer Science, Bharati Vidyapeeth's College of Engineering New Delhi, A 4, Rohtak Road, Paschim Vihar, Delhi, 110063

Abstract: ***In open communication network, it is utmost crucial to keep sensitive information protected from becoming vulnerable to unauthorized access. Encryption process provides high security to the digital data content. Chaos theory has been broadly serviceable for encrypting image due to its multiple features. The discrete chaotic cryptographic system approaches are established on block and stream encryption schemes. If these two are combined the security level is significantly advanced. Chaos is used for expanding confusion and diffusion in images. Chaotic map gives benefits of large key space and high level security. In this paper, the survey of various chaos-based image encrypting techniques is done based on existing works. The paper also lays emphasis on the methodology of different techniques in detail.***

Keywords: chaos theory, image encryption, decryption, cipher, cryptography

1. Introduction

In the recent years with a rapid growth in computer network which allows large files to be transmitted easily over the internet, the image safety has become a necessary concern for communication of digital images. Encryption is a prime way to ensure the ward of digital images. Image encryption [1] [3] [9] plays a conspicuous and crucial role in information hiding. Image encryption works by trying to transform plain image to a different image that is tough to understand, to keep the image confidential among users and it is essential that nobody could get to know the matter without a key assigned for decryption. Image encryption method prepares information to be unreadable. Modern cryptography [4] lays major emphasis on the mathematics and computer science, the cryptographic schemes are centered around computational hardness and hard to break. Therefore, to prevent private information from non-authorized users, cryptography plays an essential role as it digitally secures the content. Major features include quicker encryption or ciphering speed and mobility against most attacks. Many image encrypting schemes established on chaos theory have been designed. Each and every point in the chaotic system is nearly approximated by other points with different trajectories. Thus, a minute change in the trajectories may lead to different behavior in the future. Hence the sensitivity to primary or initial conditions is very important factor in chaos based systems.

At sender's side, the image is encrypted so that its contents are not understandable and at receiver's side, the image is decrypted using a key so as to obtain the authentic image. Even if someone views the encrypted image or an eavesdropper gets access to the image, they won't be able to understand the content. Applications in real-world systems include in military, medical and aeronautics. The image encryption requires high correlation and high redundancy among block pixels and thus the process is more tedious than text encryption which is done through AES, DES, Blowfish algorithms, etc. Chaotic functions are used in encrypting images. These systems have high sensitivity to initial conditions. The chaos cryptosystems provide better security and have low mathematical complexity. These crypto systems are deterministic in nature and their behavior in the future depends solely on the initial condition.

(a)

(b)

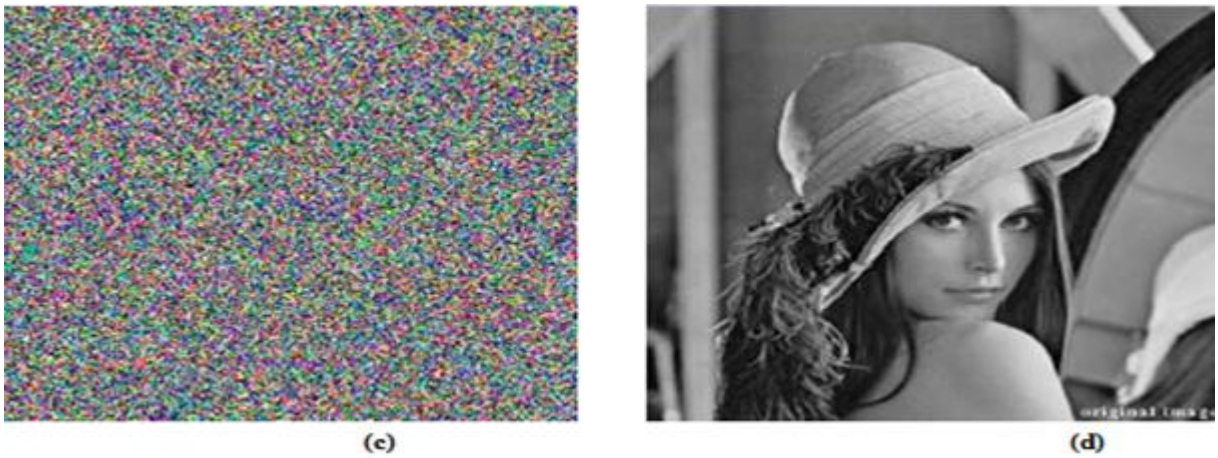

Illustration of image encryption using Lena image, Figure (1.a) Plain image, (1.b) Key image, (1.c) Encrypted image, (1.d) Decrypt image

2. Background

Image encryption is an astute way to hide information. A private and plaintext is transformed into cipher text that appears random rubbish when read. The encrypted text is used in transmission and communication process over the network. At the receiving end, the cipher text can be deciphered into the original text through a decryption algorithm. The primary purpose is to safely transfer the image to the receiver while ensuring that no unapproved or unauthorized user gets access to it. The image content has vital properties like high redundancy, capacity, space, correlativity among the bit pixels that require demands on an encryption technique. The one which is most often used to provide security to the digital images is by scrambling of bit pixels' data. Cryptography, digital marketing and compression are some of the techniques that have been suggested. In this paper, the focus is on encrypting the digital image with basis on chaos theory. Encrypting image is the task of converting or transforming the information using a technique to make it not accessible to anyone other than those possessing special knowledge referred to as "key" and converting that information using "encryption algorithm" into a form that cannot be decrypted without a key for decryption. Decryption of image through the key retrieves the original information from the encrypted image. There are many digital image encryption techniques to cipher and decipher the image. No one algorithm for image encryption satisfies all the 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. Different techniques designed to cipher digital image were formulated around in the mid-1990s. The chaos-based encryption techniques have different types of applications in many fields for example in the internet communication, military, health care, marine research, etc. The image encryption process has tremendous future possibilities. New image encryption methods are being discovered every day and image security is rapidly becoming a serious issue.

The organization of the paper is as follows. Following the introduction, the literature survey of various image encryption algorithms are discussed in Section 2. Section 3 discusses the methodology of encryption techniques. Section 4 discusses the comparison analysis between different image encryption chaos-based techniques. Section 5 describes the concluding remarks.

3. Survey

3.1 Non-linear chaotic algorithm

Haojiang Gao et.al [1] discussed some algorithms for the encryption of image established on chaotic structure, but the inhibitions of weak security due to small-scale key space in chaotic one-dimensional cryptosystems are prevalent. This research propones a distinct nonlinear chaotic technique where a tangent function and power function is used despite of linear function. Its structure variables are retrieved by analyzing experimentally. And then in a password system a technique for encrypting a image is designed. The experimentally obtained results exhibit that the method for encrypting a image established on NCA gives benefits of desirable high-level security caused due to huge key space, which maintains the required efficiency. On comparison to the other security algorithms in this field like DES, AES, the suggested technique for encrypting an image is more secure.

3.2 Magic Cube Transformation

Zhi-liang ZHU, Hua CHAI, Chong WANG, Hai YU [2] propose a unique method established on chaos technique. This method uses the principle of puzzle cube for shuffling all pixel values in a 3-dimension plane, and modify them using the pseudo-random pattern obtained by compound chaotic map i.e., a combo of sine map, chaotic map and cosine map. The method generally achieves the goal of high speed and various experimental analysis prove that it achieves a very high security level.

3.3 An image Encryption Approach Using Chaotic Map in Frequency Domain

Ansari et.al [3] proposed a distinct approach for Encrypting an image which uses chaotic maps in the Frequency Domain. The Discrete Cosine Transform (DCT) of image is evaluated and shuffling of image is performed by 2D baker's map. Two bakers map are used where first uses the primary set

keys and the other is used with Gaussian image generated with mean variance. The gain of both baker's maps and DCT are XORed repetitively. The scattering pattern is formed by a number generator which engender a random pattern based on Gaussian distribution. The suggested encryption method uses two Bakers map thus capable of accommodate the key space up to 128 bits. The technique is derived on MATLAB.

3.4 Multiple- Image encryption with chaotic maos and bit-plane decomposition

Zhenjun Tang et.al [4] proposed an encryption method for numerous colored greyscale images for creating a more secured image transmission. The infant input grayscale image is prorated into bit-planes and swapping of bit-blocks among various bit-planes takes place randomly. XOR logical operation is enforced between these scrambled data and a matrix controlled using a chaotic map which operates as a secret key. The component of grayscale image i.e. green, red, alpha and blue are viewed to generate an encrypted image.

3.5 Breaking an Image Encryption lgorithm based on the New substitution stage with chaotic functions

Mirzakuchaki et.al [5] introduced an encrypting technique established on the novel substitution stage using chaotic functions. This algorithm chiefly comprises of two main phases' confusion and diffusion. Permutation of pixels of images is done by some chaotic maps and treated as confusion process while in diffusion process, the conversion of pixels in a unique way such that even a small variance in a pixel of the authentic input image stimulate the corresponding encrypted image to be assessed differently.

3.6 Circular Inter-intra bit-level permutation and chaos-based image encryption

Adrian-Viorel Dianconu [6] suggested an efficient permutation at circular intra-inter bit-level based confusion strategy. The cryptosystem's design uses a promiscuous random number generating strategy in the starting stages of the encryption manner for reckoning of the matrices (cipher). Using the random patterns of real numbers produced in association with multilevel discretization method, di-bit pairs are generated which are directly proportional to image dimensions. This chaos system reduces the iterations of Fridrich's structure encryption scheme.

3.7 Pseudo-random masks and pixel mapping

ChengqingLi et.al [7] suggest an encryption manner established on hybrid (CA) cellular automata and depth conversion integral imaging. In a standard RGB representation of image, the R, B and G channels are analogous to each other so the same encryption process is practiced on each channel in alongside. The authentic input colored image is combo of three channel and CGII is for recording them as EIA. The recorded EIA is converted into depth-converted EIA using mapping algorithm. Each of these converted channel is hidden by a pseudo-random progression. The concealed depth-converted EIA is shuffled by a sequence, introduced by chaotic logistic map. Finally, all these three channels are merged to form an encrypted image.

3.8 A fast image encryption algorithm based on chaotic map

Wenhao Liu et.al [8] suggested a novel two-dimensional SIMM hyper chaotic map based on close-loop intonation coupling model. A junction-decomposition mechanism is given for encrypting the color image. Chaotic shift transform is combined to obtain good scrambling effect. On combination of CST with 2D-SIMM map, a fast encryption scheme is formed that is highly secure, has low time ramification and can resist common attacks.

3.9 Substitution permutation network and chaos

Belazi et.al [9] suggested a scheme establish on chaos and permutation-substitution network to encrypt image. It is combo of 4 phases of cryptography and uses two chaotic systems to control the architecture of encryption process for a desirable lofty encryption performance. A dispersion phase works on bitwise XOR logical operation and a different chaotic map is designed. An exchange phase with basis on S-boxes and by a permutation function we accomplish block alteration phase, MAP function, to bolster the analytical efficiency of the encryption scheme.

3.10 A secure image encryption method based on dynamic harmony search (DHS) combined with chaotic map

Khadijeh Mirzaei et.al [10] advanced a grayscale image encrypting manner using Dynamic Harmony Search (DHS) for achieving maximum or peak entropy and minimum correlation. In this method, a cipher image is created practicing chaotic map then the maximum or peak entropy and minimum correlation coefficient is achieved employing harmony search algorithm. The plane image is diffused to maximize the entropy and minimize the correlation coefficient using DHS algorithm, in the proximate step we use a fitness function. Permutations are applied horizontally and vertically on the best image (cipher) obtained from previous step to achieve more image security.

4. Methodology

4.1 Pseudo- random masks and pixel mapping

A hybrid (CA) Cellular Automata [7] can generate a 2-D pseudo-random mask which is highly secured. The stored information in the cell is dispersed to the unified neighboring cells. The mask is obtained by CA rule 150 and rule 90 when used simultaneously, which are expressed by:

$\alpha_i^{t+1} = \alpha_{i-1}^t \oplus \alpha_{i+1}^t$,

$\alpha_i^{t+1} = \alpha_{i-1}^t \oplus \alpha_i^t \oplus \alpha_{i+1}^t$,

Where α_i^t represents state of node i at time t.

4.2 Multiple-image encryption with chaotic maps and bit=plane decomposition

Bit-plane decomposition [4] , pixels of image in decimals ranging from 0 to 255 is represented in binary sequence of 8-bits therefore the grayscale image can decompose into 8-bit plane where i^{th} bit plane consist of i^{th} bit of all pixels (i=1 to 8). A positive or zero decimal number *d* can be conveyed in binary representation with n-bit as:

$$d = \sum_{i=1}^{n} b_i 2^{i-1} = b_1 2^0 + b_2 2^1 + \ldots + b_i 2^{i-1} + \ldots + b_n 2^{n-1}$$

Chaotic maps are more efficient for the security purpose due to their random behavior. In the suggested method, two chaotic maps are there i.e., Henon map which is 2-D discrete chaotic map that can be defined as:

$$\begin{cases} x(k+1) = 1 - ax^2(k) + y(k) \\ y(k+1) = bx(k) \end{cases}$$

Where a and b are the control parameters and Logistic map which can be symbolize as:

$$x_{i+1} = \mu x_i (1 - x_i)$$

Where μ is the controlling parameter. To control random-bit block pattern and to conduct X-OR operation respectively.

4.3 Dynamic harmony Search (DHS) combined with chaotic map

A random-like behavior of chaotic map [10] is best suitable for security purpose, the chaotic map that is employed in this proposed method is asymmetric tent map and is symbolized as:

$$X_{n+1} = \begin{cases} X_n/\alpha \ \ for\, X_n \epsilon [0, \alpha] \\ (1 - X_n)/(1 - \alpha) \ \ for\, X_n \epsilon [\alpha, 1] \end{cases}$$

Where α is parameter, X_n is the current state value and X_{n+1} is the succeeding state values of the function.

4.4 New substitution phase based on chaotic function

The cryptographic system is established on the combination of dual one-dimensional chaotic functions [5]. The equations of chaotic functions are symbolized as:

$$f_1(x_i) = x_{i+1} = 8x_i^4 - 8x_i^2 + 1 \ ; i = 1,2,\ldots,M$$

The generated outcomes are mapped to the interval of range [0,255] and are used as matrix K1 of size M×1 (where M serves as the number of rows in plain-image).

$$f_2(x_i) = x_{i+1} = 4x_i^3 - 3x_i \ \ ; \ \ i = 1,2,\ldots,N$$

The size of this matrix is 1×N (where N serves as the number of total rows in plain image). The above two functions are combined to use.

$$a = \frac{x_1 + x_2}{2}$$

$$\begin{cases} if \ \ a < 0, & f_1 = 8x_1^4 - 8x_1^2 + 1 \\ & f_1 = x_1 \\ if \ \ a > 0, & f_2 = 4x_2^3 - 3x_2 \\ & f_2 = x_2 \end{cases}$$

A shifting operation of corresponding number in matrix K1 is performed on the rows of original image in such manner that the plain-image's first row is circularly shifted by the very first number of matrix K1 and the same operation is enforced on each row as on first row. Once this horizontal rotation is implemented to all the rows of plain-image, the outcome is then circularly shifted in the vertical direction in accordance to matrix K2. The resulted outcome of last stage is expressed as one-dimensional 8-bit integer vector P = {p1, p2…, pM×N}. The trade operation is as follows:

$$c_1 = bitxor\left(p_1, bitxor\left(\mathrm{mod}\left(\sum_{i=2}^{\ldots} p_i, 256\right), k_1\right)\right)$$

$$c_i = bitxor\left(p_i, bitxor\left(\mathrm{mod}\left(c_{i-1} + k_i, 256\right), k_i\right)\right) \ \ ; i = 1,2,\ldots,M \times N$$

4.5 Magic Cube Transformation

Pseudo-random pattern is introduced by practicing compound chaotic map [2] as follows:

$$X_{n+1} = \begin{cases} f_0(X_n) = \mu X_n (1 - X_n) \\ f_1(X_n) = \lambda \sin(\pi X_n) \\ f_2(X_n) = \delta \cos(\pi \mid X_n - 0.5 \mid) \end{cases}$$

which includes sine map, chaotic map and cosine map.

Encryption Process: The Input the initial sequence of the magic cube. For every pixel D_i, the previous pixel D_{i-1} is set for determining the function employed to iterate. Iterate the chaotic mapping function to get a pseudo-random number K_i. Using K_i the pixel values get shuffled as follows:

$$C_i = D_i \oplus K_i \oplus D_{i-1}$$

Iterate steps 2 and 3 to process all the pixels.

4.6 Substitution-permutation network and chaos

The MAP function [9] is avail to achieve a chaotic manner ranging from $\{0, 1, \ldots., n^2\}$, represented by MAP (*n*,*p*) where *p* is prime number and *n* represents an integer.

The PRIMES function [9] is avail to return a row vector which contains all the prime numbers that are $\geq g$, and is represented as: *p*=PRIMES (*g*), where *p* and *g* both are of selfsame data type.

Encryption process:

- A random pattern I_0 is generated using a novel chaotic map for an input 8-bit grayscale image formulated as:

$$x_{n+1} = \mu(x_n^4 - x_n^2) + 1$$

Here $x_0 \in [0,1]$ is the primary value and $\mu \in [3,8]$ is a controlling parameter.

- Obtained sequence is mapped in integer sequence $J_0 \in [0,255]$ as:

$$J_0 = u\mathrm{int}8\left(\mathrm{mod}\left(I_0 10^{17}, 256\right)\right)$$

then, mask J_0 applied on input image, represented as P (M, M) as per the equation follows:

$$P_{sc} = bitxor(P, J_0)$$

- Generate 8 S-boxes of dimension (8 × 8) using chaotic linear functional transformation (LFT) S-boxes i.e.,

$$f : PGL(2, GF(2^8)) \times GF(2^8) \rightarrow GF(2^8),$$

$$f(x) = \frac{ax + b}{cx + d}$$

then decompose the diffused images P_{sc} into 8 blocks $\{B_i, i = 1\ to\ 8\}$. Now simulate each pixel p_j of each block B_i using the equation:

$$s_j = SB_i(p_j), i = 1, \dots, 8\ and\ j = 1, \dots, n$$

- Iterate the logistic map function to obtain the scrambled pattern F with primary parameter y_0 and α_0 as control parameter. Then convert the accomplished sequence to integer sequence $G \in [0,255]$ as:

$$G = \mathbf{mod}\left(F \times 10^{14}, 256\right)$$

Now, apply mask G on the P_s in accordance to the equation below:

$$P_c = bitxor(P_s, G)$$

- Disintegrate matrix P_c to size (m,m) then form a matrix P_d of size $\left(\frac{M}{m}, \frac{M}{m}\right)$ using these blocks. Then shuffle P_d by the sequence S to generate matrix P_p, permuted matrix. And $S$is MAP$\left(\frac{M}{m}, p\right)$ where p represents the prime number obtained as: $p = Q(\lfloor L/2 \rfloor)$ where L denoted the length of sequence Q produced by iterating the PRIMES function g as:

$$g = \left\lceil \frac{\sum_{i=1}^{M}\sum_{j=1}^{M}\left|P_s(i,j) - P_{sc}(i,j)\right|^2}{\max\left(P_s\right)} \right\rceil$$

- If cmpt ≤ 8, update y_o, α_o, x_o, and μ_o. Then repeat above steps to until cmpt=8 to get encrypted image.

5. Comparison Analysis

The comparison analysis of all the above methodologies is done on the basis of key space, key sensitivity, speed of encryption and decryption and the security of the cipher image to various attacks.

Techniques	*Encryption Speed*	*Decryption Speed*	*Key Space*	*Security*	*Sensitivity*
New substitution phase based on chaotic functions	Moderate	Slow	2^{268}	High	High
Substitution-permutation network and chaos	Moderate	Moderate	2^{624}	Very High	Very High
Dynamic harmonic search combined with chaotic map	High	High	2^{416}	Very High	Less
Image Encryption using Bit-plane Decomposition	Less	Less	2^{382}	High	High
Pseudo-random masks and pixel mapping	Moderate	Moderate	2^{256}	High	Very High
Magic cube transformation	High	Moderate	2^{168}	High	Very High

6. Conclusion

As the use of transmitting and storing images using digital techniques are increasing, it becomes a crucial concern that how to conserve the confidentiality, authenticity and integrity of images. Secure and economic data transmission is the need of the hour. Security of the digital images became an important issue since the communications of digital products over open network started occurring frequently. This paper reviews the existing works on various chaos based encrypting techniques for image. We conclude that the techniques are useful for real-time systems and suitable for applications. An array of simulation tests done are compared with many important work in image encryption field to prove the performance and security of the algorithms including differential, statistical quality, speed and contrast analysis prove that these bonanzas have superior performance than those in literature.

References

[1] Haojiang Gao, Yisheng Zhang, Shuyun Liang, Dequn Li, "A new chaotic algorithm for image encryption", Audio, Language and Image Processing, 2008. ICALIP 2008. International Conference, 2005
[2] Zhi-liang ZHU, Chong WANG, Hua CHAI, Hai YU, "A Chaotic Image Encryption Scheme Based on Magic Cube Transformation", IEEE Conference Publications, 2011
[3] Shoaib Ansari, Neelesh Gupta, 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
[4] Zhenjun Tang, JuanSong, Xianquan Zhang, Ronghai Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps", Optics and Lasers in Engineering, Volume 80, May 2016
[5] Benyamin Norouzi, Sattar Mirzakuchaki, "Breaking an Image Encryption Algorithm based on the New Substitution Stage with Chaotic Functions", Optik - International Journal for Light and Electron Optics 127(14), Volume 127, Issue 14, July 2016
[6] Adrian-Viorel Dianconu, "Circular inter-intra bit-level permutation and chaos-based image encryption", Information Sciences, Volumes 355–356, Elsevier, August 2016
[7] XiaoweiLi, ChengqingLi, In-KwonLee, "Chaotic image encryption using pseudo-random masks and pixel mapping", European Association for Signal Processing, Volume 125, Elsevier, August 2016
[8] Wenhao Liu, Kehui Sun, Congxu Zhu, "A fast image encryption algorithm based on chaotic map", Elsevier, 2016
[9] AkramBelazi, Ahmed A. Abd El-Latif, SafyaBelghith, "A novel image encryption scheme based on substitution-permutation network and chaos", European Association for Signal Processing, Elsevier, 2016
[10] Khadijeh Mirzaei Talarposhti, Mehrzad Khaki Jamei, "A secure image encryption method based on dynamic harmony search (DHS) combined with chaotic map", Optics and Lasers in Engineering, Volume 81, Elsevier, 2016