Survey of Chaos based Image Encryption and Decryption Techniques

Ephin M
Assistant Professor SG/IT
Karunya University
Coimbatore, India

Judy Ann Joy
PG Scholar, MMT
Karunya University
Coimbatore, India

N. A. Vasanthi
Dean/CSE
Nehru Institute of Engg.&Tech.
Coimbatore, India

ABSTRACT

Nowadays security becomes an important issue of communication and storage of images. One of the method used to ensure the high security of images is encryption. Images are used in many fields such as biometric authentication, medical science, military; they are stored or transferred through the network and the security of such image data is important. Due to some intrinsic features of the images, such as bulk data capacity and high correlation among pixels the earlier encryption techniques such as AES, DES, RSA, etc are not suitable for practical applications. The latest trend in encryption is chaos based. It has many unique characteristics such as the sensitive dependence on initial conditions, nonperiodicity, nonconvergence, and control parameters. In this paper survey of different chaos-based image encryption techniques has been discussed.

Keywords

Chaos, Image Encryption, Image Decryption.

1. INTRODUCTION

Information exchanges across the internet and the storage of data on open networks have created an environment in which it is very easy to disclose important information to illegal users. For this reason, encryption techniques were used. Encryption techniques protect the data from illegal tampering and use. Encryption of data has become an important way to protect data resources especially on the Internet, intranets and extranets. Encryption is the process of applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. The main goal of security management is to provide authentication of users, integrity, accuracy and safety of data resources.

Today the web is going towards multimedia data [12]. The high percentage of multimedia data is images. Images are used in many fields such as biometric authentication, medical science, military, online personal photograph album, etc. Therefore it's very important to protect the image from unauthorized access. That is, it is necessary to assure confidentiality, integrity and authenticity of the digital images transmitted. Image encryption techniques try to convert original image to another image that is hard to understand and to keeps the image confidential between users. And without the decryption key no one can access the original images. Image encryption has applications in many fields such as military communication, internet communications, multimedia systems, medical imaging, telemedicine, etc [15]. Image encryption is different from text encryption [22]. Due to some intrinsic features of the images, such as bulk data capacity and high correlation among pixels the earlier encryption techniques such as AES, DES, RSA, etc are not suitable for practical applications [13-21]. In this case chaos based encryption techniques are considered good for practical use.

Chaos theory was discovered by Edward N Lorenz in 1963 [26, 35]. Chaos theory has been established since 1970s by many different research areas, such as mathematics, physics, engineering, biology, economics, and philosophy, etc [25]. In common usage, chaos means a state of disorder. Since there is no universally accepted mathematical definition of chaos, a commonly used definition is that, for a dynamical system to be said as chaotic, it must have the following properties: 1) It must be sensitive to initial conditions, 2) Its periodic orbit must be dense, and 3) It must be topologically mixing. Sensitive to initial conditions means that a small difference in the initial conditions will produce widely diverging outcomes for chaotic systems, so that long-term prediction is impossible. The topological mixing (or topological transitivity) property ensures the ergodicity of a chaotic map, which means that if we partition the state space into a finite number of regions, no matter how many, any orbit of the map will pass through all these regions [35].

Since 1990s, many researchers have noticed that there exist the close relationship between chaos and cryptography [27-32]. The main difference between chaos theory and cryptography is that cryptosystems work on a finite field, while chaos is meaningful only on a continuum. Nevertheless, these two scientific notions are very closely related. Many fundamental concepts in chaos theory, such as mixing and sensitivity to initial conditions and parameters, actually coincide with those in cryptography. The mixing property is closely linked to the diffusion feature of cryptosystems [33]. The similarities and differences between the two subjects can be listed [30], as shown in Table 1. Chaotic maps and cryptographic algorithms have some similar properties: both are sensitive to tiny changes in initial conditions and parameters; both have random like behaviors; and cryptographic algorithms shuffle and diffuse data by rounds of encryption, while chaotic maps spread a small region of data over the entire phase space via iterations. The only difference in this regard is that encryption operations are defined on finite sets of integers while chaos is defined on real numbers.

Due to the exceptional properties of mixing and sensitivity to the initial conditions and parameters of chaotic maps [23], chaos-based encryption is a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. Chaos based algorithms provide a good combination of speed, complexity, high security, reasonable computational overheads and computational power.

Table 1. Similarities and differences between chaos and cryptography

Chaotic Systems	**Cryptographic algorithms**
Phase space: set of real numbers	Phase space: finite set of integers
Iterations	Rounds
Parameters	Key
Sensitive to initial conditions and parameters	Diffusion

2. EVALUATION OF DIFFERENT IMAGE ENCRYPTION TECHNIQUES

A new method based on Fractional Wavelet Packet Transform (FWPT) is introduced by L. Chen and D. Zhao to encrypt images, in which fractional order of fractional wavelet packet transform is used as the key. FWPT [24] is a Wavelet Packet Transform (WPT) realized in a Fractional Fourier domain. In this method first the image is decomposed into various subbands. Then some of the subbands are randomly selected and encrypted using fractional wavelet packet transform. The selected encryption with FWPT is more effective than that with WPT, because it is realized in the fractional Fourier domain and the information is more randomly distributed at fractional Fourier plane than at Fourier plane. This paper has an advantage to achieve data confidentiality. And it has a drawback of limited key space and limited perceptual quality [13]. Key space size is the total number of different keys that can be used for the encryption. A good encryption scheme should have the key space that should be large enough to make brute-force attacks infeasible. Limited perceptual quality means after encryption we will get the glimpse of the original image. [1]

Due to the drawback of weak security in one-dimensional chaotic cryptosystems Haojiang Gao, Yisheng Zhang, Shuyun Liang and Dequn Li presents a new Nonlinear Chaotic Algorithm (NCA). The one-dimensional chaotic map, for example logistic map have linear function. But the Nonlinear Chaotic Algorithm (NCA) uses power function and tangent function instead of linear function. In the encryption process, at first the encryption key is set. Then the NCA is iterated 100 times to obtain the encrypted image. After the encryption the encrypted image is send through the public communication channel and the encryption key is send through the secure communication channel. And at the receiver side the decryption is similar to encryption algorithm. This paper has the advantages of high level security and sensitive to key. [2]

F. Sun, S. Liu, Z. Li, and Z. Lu presents a novel image encryption scheme based on spatial chaos map The basic idea is to encrypt the image in space with spatial chaos map pixel by pixel, and then the pixels are confused in multiple directions of space. In the encryption process initially the original image is transformed into a matrix and then this matrix is encrypted using results of iteration of spatial chaos map. Using the initial conditions and control parameters of chaotic map, the spatial chaos map is iterated once and a new matrix is generated. Then in the next step the spatial chaos map parameters are modified. This process will be repeated for some time and finally we will get the ciphered image. The decryption procedure is similar to that of encryption with reverse of ciphered image as input instead of original image in the encryption procedure. Since both decryption and encryption procedures have similar structure, they have essentially the same algorithmic complexity and time consumption. It is highly secure. Its key space is incomparably large to resist the attacks. [3]

In the image encryption scheme presented by N. K. Pareek, V. Patidar, and K. K. Sud, an external secret key of 80-bit and two chaotic logistic maps are employed. By providing different weightage to all its bits, the initial conditions for both the logistic maps are derived using the external secret key. In the algorithm, the first logistic map is used to generate numbers ranging from 1 to 24 (numbers may be repeated). Using the numbers generated from the first logistic map the initial condition of the second logistic map is modified. By modifying the initial condition of the second logistic map in this way, its dynamics gets further randomized. Further, in the proposed encryption process, to encrypt the pixels of an image, eight different types of operations are used and which one of them will be used for a particular pixel is decided by the outcome of the logistic map. After encrypting each block of sixteen pixels of the image, the secret key is modified, to make the cipher more robust against any attack. Key sensitivity is high in this method. Even though it can resist brute force attack, it has a small key space. It has a key space of 2^{80} $(\approx 1.20893 \times 10^{24})$. [4]

In the paper introduced by Guanrong Chen, Yaobin Mao, Charles K. Chui, the two-dimensional chaotic cat map is generalized to 3D for designing a real-time secure symmetric encryption scheme. At first select a sequence of 128 bits as the key, and then split them into eight groups, which are further mapped onto several parameters of the 3D cat map and the logistic map. Then the two- dimensional image is changed to three dimensional image. Then using three-dimensional cat map we will generate shuffled images. Then using logistic map we will perform XOR plus mod operation on the shuffled image. And transform the three-dimensional cubes back to a two-dimensional image. Thus the encrypted image is obtained. The decryption process is similar to that of encryption process. It has fast encryption speed. Compared with other encryption techniques it has small key space. Its key space is $2^{128} \approx 3.4028 \times 10^{38}$. But it will resist brute force attack. [5]

In the paper presented by Yaobin Mao, Guanrong Chen, Shiguo Lian, the two-dimensional chaotic baker map is generalized to 3D for designing a real-time secure symmetric encryption scheme. At first select a sequence of 128 bits as the key, and split them into six groups, which are further mapped onto several parameters. Then the two- dimensional image is changed to three dimensional image. Then using three-dimensional baker map we will generate shuffled images. Then using logistic map we will perform XOR plus mod operation on the shuffled image. And transform the three-dimensional cubes back to a two-dimensional image. Thus the encrypted image is obtained. The decryption process is similar to the encryption process. It has fast encryption speed [16]. It will resist brute force attack. But compared with other encryption techniques it has small key space. Its key space is $2^{128} \approx 3.4028 \times 10^{38}$. [6]

Jinhui Lai, Song Liang, Delong Cui introduced a novel image encryption algorithm based on Fractional Fourier transform and chaotic system. In that the encryption process includes two steps. At first the image is encrypted double random phase using Fractional Fourier domain. Then that image is again encrypted using a matrix generated by chaotic system and thus the encrypted fingerprint image is obtained. The decryption process is similar to encryption process. It is the inverse of encryption process. It will resist brute force attack. But it has small key space. Its key space is 10^{60}. [7]

Song Zhao, Hengjian Li and Xu Yan have introduced a secure and efficient fingerprint images encryption scheme. In this paper a novel chaotic fingerprint images encryption scheme is proposed combining with shuttle operation and nonlinear dynamic chaos system. At first, a new image total shuffling operation is employed to shuffle the positions of image pixels in the spatial-domain. Then the pixels of shuttled image are arranged by the order from left to right and then top to bottom. And then it is converted to binary representation. Then the Nonlinear Digital Filter (NDF) chaotic is iterated. To obtain the encrypted image the keystreams generated by NDF are XOR-ed with the binary representation of the image. The decryption algorithm is similar to the encryption algorithm. That is decrypting the image using NDF with the same parameters and initial values as that used in the encryption system. And then anti-shuttle the resulting image. Then, we will obtain the original image. This encryption process will resist brute force attack and the encryption algorithm is sensitive to the key. The encryption process is not time efficient. [8]

Daesung Moon, Y. Chung, Sung Bum Pan, K. Moon and Kyo ll Chung proposed an efficient selective encryption of fingerprint images for embedded processors. They developed an image-based selective bitplane encryption algorithm. The selective bitplane encryption algorithm consisting of two steps: image distortion and LSB encryption. In image distortion, we distort the full fingerprint image by using very simple operations. For each pixel, we select its LSB as a random noise and generate the LSB bitplane. Then, we take a simple exclusive-OR of the LSB bitplane and all the pixels of the fingerprint image. Without knowledge of the LSB bitplane, an opponent cannot recover the ridge structure of the fingerprint image from the result of image distortion. Therefore, in the LSB encryption, we only need to encrypt further the LSB bitplane by using a shared session Key. As the client and sensor share the same key, the client can recover the original fingerprint image by decrypting the encrypted LSB bitplane and then applying the same exclusive-OR operation. It will guarantee confidentiality of the fingerprint image between a sensor and a client in real-time. It has a disadvantage of limited perceptual quality. [9]

Tiegang Gao and Zengqiang Chen proposed an image encryption based on a new total shuffling algorithm. They introduced a new image total shuffling matrix to shuffle the positions of image pixels and then uses the states combination of two chaotic systems to confuse the relationship between the plain-image and the cipher-image. The image total shuffling matrix is generated by doing some iterations of logistic map and then changing the positions of row and columns of the matrix. And finally the cipher image is obtained using Lorenz chaotic system and Chen's chaotic system. This encryption algorithm has large key space and is sensitive to the key. It will resist all kinds of brute force attack. But the encryption algorithm is not time efficient since the row and column transformation require much time. [10]

Delong Cui introduced a novel image encryption algorithm based on Fractional Fourier transform and chaotic system. In that the encryption process includes two steps. At first the image is encrypted double random phase using fractional fourier domain. Then that image is again encrypted using a matrix generated by chaotic logistic map and thus the encrypted fingerprint image is obtained. The decryption process is similar to encryption process. It is the inverse of encryption process It will resist brute force attack. But it has small key space. Its key space is 10^{60}. [11]

Gaurav Bhatnagar and Q. M. Jonathan Wu has proposed a chaos based security solution for fingerprint data during communication and transmission. The core idea is to transform the original fingerprint image first using the proposed Reversible hidden transform (RHT). RHT is a simple integer transform that transforms an integer pair to another integer pair at a considerably lower mathematical complexity based on some secret parameters. Then, the transformed fingerprint image is decomposed into various subbands using fractional wavelet packet transform (FrWPT) [24] and piece-wise linear chaotic map (PWLCM). Now, each subband is deformed by singular value decomposition (SVD) and chaotic map followed by inverse FrWPT to get the encrypted fingerprint image. This deformation is chosen in such a way that the reverse deformation exists and can be used at the receiver end to decrypt the image. At the decryption/receiver end, the reverse process is done to decrypt the image. The major advantages of this paper includes: i) Large key space. ii) Highly sensitive to the keys. iii) Perceptually efficient, iv) Time efficient. v) High security. [13]

3. RESULT ANALYSIS

There are many chaos based image encryption techniques available today. Each techniques described in the above papers are studied well. By comparing the above papers we can conclude it in the form of a table. And it is shown in Table 2. We have found out the advantages and disadvantages of each paper. By analyzing the table we can easily understand the methods, advantages and disadvantages of each paper.

4. CONCLUSION

In this internet world, the security for the digital images has become highly important since the communication by transmitting of digital products over the open network occur very frequently [34]. In this paper, the existing chaos based image encryption techniques have been surveyed. Those encryption techniques are studied and analyzed well, to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for real-time image encryption. Each technique is unique in its own way, which is suitable for different applications. Everyday new encryption techniques are evolving hence fast and secure conventional encryption techniques will always work out with high rate of security.

Table 2: Comparison of different chaos based image encryption techniques

Reference:	Method	Advantage	Disadvantage
[1]	• Fractional wavelet packet transform	• Achieve data confidentiality	• Limited key space • Limited perceptual quality.
[2]	• Nonlinear chaotic algorithm	• High level security	• Small key space.
[3]	• Spatial chaotic map	• Highly secure	• Small key space.
[4]	• Two chaotic logistic map	• Key sensitivity is high**.**	• Small key space.
[5]	• 3D chaotic cat map • Logistic map	• Fast encryption speed	• Small key space • Plain-image must be square size
[6]	• 3D chaotic baker map • Logistic map	• Fast encryption speed	• Small key space • Plain-image must be square size
[7]	• Fractional fourier transform. • Logistic map	• Resist brute force cracking	• Small key space
[8]	• Logistic map • Nonlinear digital filter chaotic map	• Resist brute force attack • Encryption algorithm is sensitive to the key	• Not time efficient
[9]	• Selective bitplane encryption	• Guarantee confidentiality	• Limited perceptual quality
[10]	• Logistic map • Lorenz chaotic system and Chen's chaotic system	• Large key space • Sensitive to the key • Resist brute force attack	• Not time efficient
Reference:	**Method**	**Advantage**	**Disadvantage**
[11]	• Fractional Fourier Transform. • Logistic map	• Resist brute force cracking	• Small key space

5. REFERENCES

[1] Chen, L., & Zhao, D. 2008. Image encryption with fractional wavelet packet method. Optik-International Journal for Light and Electron Optics, 119(6), 286-291.

[2] Gao, H., Zhang, Y., Liang, S., & Li, D. 2006. A new chaotic algorithm for image encryption. Chaos, Solitons & Fractals, 29(2), 393-399

[3] Sun, F., Liu, S., Li, Z., & Lü, Z. 2008. A novel image encryption scheme based on spatial chaos map. Chaos, Solitons & Fractals, 38(3), 631-640.

[4] Pareek, N. K., Patidar, V., & Sud, K. K. 2006. Image encryption using chaotic logistic map. Image and Vision Computing, 24(9), 926-934.

[5] Chen, G., Mao, Y., & Chui, C. K. 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 21(3), 749-761

[6] Mao, Y., Chen, G., & Lian, S. 2004. A novel fast image encryption scheme based on 3D chaotic Baker maps. International Journal of Bifurcation and Chaos, 14(10), 3613-3624.

[7] Lai, J., Liang, S., Cui, D. 2010. A Novel Image Encryption Algorithm Based on Fractional Fourier Transform and Chaotic System. In Multimedia Communications (Mediacom), 2010 International Conference on (pp. 24-27). IEEE.

[8] Song, Z., Hengjian, L., & Xu, Y. 2008. A secure and efficient fingerprint images encryption scheme. In Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for (pp. 2803-2808). IEEE.

[9] Moon, D., Chung, Y., Pan, S. B., Moon, K., & Chung, K. I. 2006. An efficient selective encryption of fingerprint images for embedded processors. ETRI journal, 28(4), 444-452.

[10] Gao, T., & Chen, Z. 2008. Image encryption based on a new total shuffling algorithm. Chaos, solitons & fractals, 38(1), 213-220

[11] Cui, D. 2010. A novel fingerprint encryption algorithm based on chaotic system and fractional Fourier transform. In Machine Vision and Human-Machine Interface (MVHI), 2010 International Conference on (pp. 168-171). IEEE.

[12] Sharma, M., & Kowar, M. K. 2010. Image encryption techniques using chaotic schemes: A review.

[13] Bhatnagar, G., & Wu, Q. 2012. Chaos-Based Security Solution for Fingerprint Data During Communication and Transmission. Instrumentation and Measurement, IEEE Transactions on, 61(4), 876-887.

[14] Nemade, V. S., & Wagh, R. B. 2012. Review of different image encryption techniques. World Journal of Science and Technology, 2(3).

[15] Srivastava, A. 2012. A survey report on Different Techniques of Image Encryption. International Journal of Emerging Technology and Advanced engineering. Vol. 2, pp. 163-167.

[16] Han, F., Hu, J., Yu, X., & Wang, Y. 2007. Fingerprint images encryption via multi-scroll chaotic attractors. Applied mathematics and computation, 185(2), 931-939.

[30] Kocarev, L. 2001. Chaos-based cryptography: a brief overview. Circuits and Systems Magazine, IEEE, 1(3), 6-21.

[31] Jakimoski, G., & Kocarev, L. 2001. Chaos and cryptography: Block encryption ciphers based on chaotic maps. Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, 48(2), 163-169

[32] Schmitz, R. 2001. Use of chaotic dynamical systems in cryptography. Journal of the Franklin Institute, 338(4), 429-441.

[17] Behnia, S., Akhshani, A., Mahmodi, H., Akhavan, A. 2008. A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons & Fractals, 35(2), 408-419.

[18] Chang, C. C., Hwang, M. S., Chen, T. S. 2001. A new encryption algorithm for image cryptosystems. Journal of Systems and Software, 58(2), 83-91.

[19] Bandyopadhyay, T., Bandyopadhyay, B., Chatterji, B. N. 2012. Secure Image encryption through key hashing and wavelet transform techniques. International Journal of Emerging Technology and Advanced Engineering. Vol. 2, pp. 26-31

[20] Acharya, B., Panigrahy, S. K., Patra, S. K., Panda, G. 2009. Image encryption using advanced hill cipher algorithm. International Journal of Recent Trends in Engineering, 1(1), 663-667.

[21] Kwok, H. S., & Tang, W. K. 2007. A fast image encryption system based on chaotic maps with finite precision representation. Chaos, Solitons & Fractals,32(4), 1518-1529.

[22] Sharma, P., Godara, M., Singh, R. 2012. Digital Image encryption techniques: A Review. International Journal of Computing & Business Research. ISSN: 2229-6166.

[23] Zhang, L., Liao, X., & Wang, X. 2005. An image encryption approach based on chaotic maps. Chaos, Solitons & Fractals, 24(3), 759-765.

[24] Huang, Y., Suter, B. 1998. The fractional wave packet transform. Multidimensional Systems and Signal Processing, 9(4), 399-402.

[25] Hao B. 1993. Starting with parabolas: an introduction to chaotic dynamics. Shanghai China: Shanghai Scientific and Technological Education Publishing House.

[26] Lorenz EN. 1993. The Essence of Chaos. University of Washington Press, Seattle, WA.

[27] Brown, R., Leon, O. 1996. Clarifying chaos: Examples and counterexamples. International Journal of Bifurcation and Chaos, 6(02), 219-249.

[28] Fridrich, J. 1998. Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos, 8(06), 1259-1284.

[29] Dachselt, F., Schwarz, W. 2001. Chaos and cryptography. Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on,48(12), 1498-1509.

[33] Kocarev, L., Jakimoski, G., Stojanovski, T., & Parlitz, U. 1998. From chaotic maps to encryption schemes. In Circuits and Systems, ISCAS'98. Proceedings of the 1998 IEEE International Symposium on (Vol. 4, pp. 514-517). IEEE.

[34] John Justin, M., Manimurugan, S. 2012. A Survey on Various Encryption Techniques. International Journal of Soft Computing. Volume-2. Issue-1, pp. 429-432

Mao, Y., & Chen, G. 2005. Chaos-based image encryption. Handbook of Geometric Computing, 231-265.