International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 2 (2014), pp. 197-206

http://www. irphouse.com /ijict.htm

Review on Different Chaotic Based Image Encryption Techniques

Nitin Kumar[1], Deepika[2], Divya Wadhwa[3], Deepak Tomer[4] and S. Vijayalakshmi[5]

[14]M.TECH.(CSE-Final Year),Computer Science and Engineering Department, Galgotias University, Plot No.2, Sector-17A,Yamuna Expressway, Greater Noida,G.B. Nagar-203201(U.P.), India.
[23]M.TECH.(I.T.-Final Year), Banasthali University, Rajasthan, India.
[5]CSE Dept. Galgotias University, Greater Noida.

Abstract

In present times, Due to the rapidly growth of digital and multimedia applications, more multimedia data are developed and transmitted through the networks in ,art, entertainment, advertising, education, training and commercial areas, which may have important information that should not be accessed by the general users. Therefore issue of protecting the confidentiality, integrity, security, privacy as well as the authenticity of images has become an important issue for communication and storage of images. In recent years, various encryption techniques are developed and applied to protect the confidential images from unauthorized users. This paper has a review on the aspects and existing different image encryption techniques based on chaos to design an image cryptosystem. In this paper, first a general introduction given for cryptography and images encryption and followed by discussion of different chaotic based image encryption techniques and related works for each technique reviewed. Finally, 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: Image, Image Encryption, Chaotic, Cryptography.

1. Introduction

With the 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 [1]. 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 [2]. 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 [3]. 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 [4]. Many image encryption schemes based on chaotic have been proposed [4]. 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 [5].

2. Image Encryption

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 [5]. 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 ttransforming 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 [8]. 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[9].

3. Literature Review

In this section, presenting the research work of some prominent authors in the same field and explaining a short description of various chaos based techniques used for image Encryption

3.1.The Chaotic Feature of Trigonometric Function and Its Use for Image Encryption, 2011

Chenghang Yu, Baojun Zhang and Xiang Ruan analyzed the chaotic features of trigonometric function and proposed a new algorithm based on the trigonometric function for fast and secure image encryption. Large quantity of experiment data and performance analysis prove that the trigonometric function is of excellent chaotic features and is very suitable for image encryption. Trigonometric function is one of the most basic and important function in nature. It is of many interesting features in encryption field. In fact, not all of the trigonometric functions can be used for encryption. The encryption feature of a trigonometric function is determined by the parameters such as the frequency and the phase. In future, we'll analyze the features of trigonometric function further and hope to propose more useful applications in the field of cryptography Trigonometric function is the most basic and important function in nature. Any functions can be disassembled into the sum of multi-trigonometric functions. By research, we find that the trigonometric function is of great chaos features a chaotic neural network with self-feedback of trigonometric function is presented by introducing non-linear trigonometric function as self-feedback of chaotic neural network. In this technique image encryption a complicated chaotic system using the boundary property of trigonometric function is used for image encryption[1].

3.2. Multi chaotic systems based pixel shuffle for image encryption,2009
C.K. Huang and H.H. Nien introduces a new pixel shuffle technique with multi chaotic systems for the image encryption. Since the chaotic system is highly sensitive to initial values and system parameters, meanwhile, has an enormous key space, the proposed method combined with four chaotic systems and pixel shuffle can fully banish the outlines of the original image, disorders the distributive characteristics of RGB levels, and dramatically decreases the probability of exhaustive attacks. We conduct FIPS PUB 140-1, correlation coefficient, NPCR, and UACI to test on the security analysis and the distribution of distinguished elements of variables for the encrypted image. The adopted examples show the highly confidential encrypted images and demonstrate a good potential in the application of the digital-color image encryption[2].

3.3 Cryptanalysis of a multi-chaotic systems based image cryptosystem, 2010
Ercan Solak, Rhouma Rhouma and Safya Belghith proposed the method of image encryption by cryptanalysis a recently proposed image cryptosystem by two different attacks. The weakness of this cryptosystem arise from the use of the same shuffling process for every plain image. And that is a consequence of using the same sequences generated by the four chaotic systems. The cryptosystem proposed in shuffles plaintext image bits using chaotic systems. The shuffling parameters are generated by the iterations of four 3D chaotic systems. The key of the cryptosystem is the set of 12 initial conditions for the chaotic maps. The parameters of the chaotic systems are fixed and public. The shuffling is performed in two stages. In the first stage, designated bits of all the pixels are shuffled. In the second stage, the bits of each pixel are shuffled among themselves. In this technique, the original plaintext is an m * n RGB image with each pixel color represented as a byte. For the purpose of encryption, the plaintext is first vector zed using the usual row scan. The resulting vector is a N * 1 vector of bytes, where N = mn. In order to manipulate the bits of pixels, the vector is further split into its bits, resulting in a N * 8 plaintext matrix, where each entry takes values 0 or 1[3].

3.4 Image Encryption Based on Diffusion and Multiple Chaotic Maps,2011
G.A. Sathishkumar, Dr. K. Bhoopathy bagan and Dr.N.Sriraam proposed encryption algorithm belongs to the category of the combination of value transformation and position permutation In this , two different types of scanning methods are used and their performances are analyzed. In the typical schematic of the proposed method first, a pair of sub keys is given by using chaotic logistic maps. Second, the image is encrypted using logistic map sub key and in its transformation leads to diffusion process. Third, sub keys are generated by four different chaotic maps and images are treated as a 1D array by performing Raster scanning and Zigzag scanning. The scanned arrays are divided into various sub blocks. Then for each sub block, position permu action and value transformation are performed to produce the encrypted image. The sub keys are generated by applying the suitable chaotic map banks. Based on the initial conditions, the generated chaotic map banks are allowed to hop through various orbits

of chaotic maps. The hopping pattern is determined from the output of the previousmap.Hence for each sub block various chaotic mapping patterns are applied which further increases the efficiency of the key to be determined by the brute force attack. In each orbit, a sample point is taken and used as key for a specific block and a condition to choose the particular orbit in a particular map is adopted. Then, based on the chaoticsystem, binary sequence is generated to control the bit-circulation functions for performing the successive data transformation on the input data. In addition to chaotic features of mixing, unpredictable, and extreme sensitive to initial seeds, through multiple chaotic maps and orbits hopping mechanism spread out the pseudo random number base to a wide flat spread spectrum in terms of time and space. [4].

3.5 Image Encryption Based on the General Approach for Multiple Chaotic Systems, 2011

Komal D Patel, Sonal Belani(2011) proposed new image encryption technique based on new chaotic system by adding two chaotic systems: the Lorenz chaotic system and the Rössler chaotic system. From Experimental analysis they demonstrate that the image encryption algorithm has the advantages of large key space and high-level security, high obscure level and high speed [6].

3.6. New Image Encryption Algorithm Based on Logistic Map and Hyper-chaos, 2013

LEI Li-hong ,BAI Feng-ming,HAN Xue-hui proposed a new image encryption algorithm based on logistic map and hyperchaotic systems, two kinds of keys were produced by using logistic chaotic iteration and hyper chaotic systems. The two kinds of keys are alternately used in the image encryption process, so the the encryption keys have a better random distribution. The encryption algorithm introduced Ciphertext cross-diffusion to increase the ciphertext sensitivity .The simulation results of the experiment showed the evenly distributed ciphertext pixels, the large key space, the small correlation of neighbor ciphertext pixels, highly sensitive keys and so on. Therefore, the algorithm has some potentiality in the field of image secure storage and image secure communication[7].

3.7 Digital Image Encryption Algorithm Based on Chaos and Improved DES, 2013

Rajinder Kaur, Er.Kanwalprit Singh worked based on the chaotic encryption and Improved DES encryption and a combination of image encryption algorithm is used to find the gaps. In this paper new encryption logistic Map produced pseudo random sequence on RGB image and make double times encryption with improved DES. Combination of Chaos And improved DES makes the final algorithm more secure, faster and more suitable for digital image encryption[10].

3.8 A modified image encryption scheme based on 2D chaotic map, 2010
Rashidah Kadir, Rosdiana Shahril, Mohd Aizaini Maarof proposed image encryption scheme an external secret key (as used by Chen et al. For image encryption and by Pareek et for text ciphers) of 80-bit and two chaotic logistic maps are employed. The initial conditions for the both logistic maps are derived using the external secret key by providing different weight age to its bits. In the algorithm, the first logistic map is used to generate numbers ranging from 1 to 24 (numbers may be repeated). The initial condition of the second logistic map is modified from the numbers, generated by the first logistic map. By modifying the initial condition of the second logistic map in this way, its dynamics gets further randomized[11].

3.9. An Improved Image Encryption Algorithm based on Chaotic System, 2009
Shoo Liu, Jing Sun, Zhengquan Xu proposed a new encryption algorithm by analyzing the principle of the chaos encryption algorithm based on logistic map. Moreover, the security and performance of the proposed algorithm is also estimated. The experimental results based on coupled chaotic maps approve the effectiveness of the proposed method, and the coupled chaotic maps shows advantages of large key space and high-level security. The system is in a stream-cipher architecture, where the PRKG is formed by two chaotic maps, serving the purpose of stream generation and random mixing, respectively. It is found that such a design can enhance the randomness, even under finite precision implementation. A detailed statistical analysis on the proposed encryption scheme is given. From the experimental results, it is concluded that it outperforms existing schemes, both in terms of speed and security. Having a high throughput, the proposed system is ready to be applied in fast real time encryption applications. The ciphertext generated by this method is the same size as the plaintext and is suitable for practical use in the secure transmission of confidential information over the Internet[12].

3.10 Benchmarking AES and Chaos Based Logistic Map for Image Encryption,2013
S.HRAOUI, F.GMIRA, A.O.JARAR, K.SATORI ,LIIAN , A.SAAIDI and LIMAO made a comparative study between a classical crypto-system based on AES and another one based on the chaotic attractor known by the name the logistic map .The aim of this work is to analyze the security performance of these two cryptosystems and assess both of their algorithms running speed. In this paper, we compared the efficiency of two image encryption techniques, one with the AES algorithm and the other with the chaotic attractor. The experimental results shows that the AES algorithm presents better security performance but slightly slower in terms of the encryption running speed, this allows us to recommend it for selective image encryption, unfortunately, it is noted that the logistic map shows some periodic windows that make it vulnerable. However, due to the computational cost, and the simplicity of implementation this map is a good alternative for image encryption in real time communication[13].

3.11 A Novel Image Encryption Scheme Based on Dynamical Multiple Chaos and Baker Map,2012

XiaoJun Tong , Yang Liu, Miao Zhang and Zhu Wang proposed encryption algorithm includes two parts:firstly, the positions of the original image pixels are permuted by Baker map; secondly, the values of the permuted pixels are encrypted by multiple-chaotic map The security analysis of the proposed image encryption is discussed here, such as sensitivity analysis, statistical analysis, sp800-22 testing, and entropy testing and so on to prove that the proposed encryption scheme is secure against the most common attacks. A fast image encryption scheme is proposed which utilizes dynamical multiple-chaotic map confuse the relationship between the cipher image and the plain image. Baker map is used to permute the positions of image pixels in the spatial-domain and the mixing of confusion and diffusion can produces more randomness. The experimental results demonstrate that image encryption technique has advantages of high-level security, such as high robust against statistic attacks and the precision of cipher be sensitive to the secret key approach to 10-14. At the same time, the probability of precision degradation is lower than simple-chaotic map encryption scheme and has high encryption than other famous encryption methods[14].

3.12 New Image Encryption Algorithm Based on Arnold and Coupled Chaos Maps,2010

Yunpeng Zhang, Peng Sun, Jing Xie, Lifu Huang proposed a new algorithm based on multi-digital image chaotic encryption systems. The practice shows that the algorithm can quickly encrypt and decrypt a digital image, and achieve a better result. The analysis of the algorithm's security proves that the algorithm has a good sensitivity of the key, a large enough key space and the encrypted pixel value is uniform distributed, and so on. ill a word it has an excellent safety and reliability[15].

4. Performance Parameters

According to Suhaila O. Sharif et al proposal, eight classifiers were used to identify the cipher text they are Support Vector Machine, Naïve Bayesian,neural network,Bagging ,Instance based learning ,Decision Tree, AdaBoostM1, Rotaion Forest and its accuracy were calculated. There was the aim to find the best classification algorithm based on high accuracy for four different block ciphers called DES, IDEA, AES, and RC2. Resulted in, the Rotation Forest classifier has the highest classification accuracy of (53.33 %) meaning that 128 out of 240 input data were correctly classified. According to Dr. Vikas Saxena and Jolly Shah in a survey manuscript on video encryption defined a set of different parameters based on which the performance can be evaluated and compared with the existing video encryption algorithms such parameters are visual degradation , encryption ratio, speed, compression friendliness, format compliance and Cryptographic security .

5. Conclusion

With the fast development of computer technology and widely application of internet, the security for the digital images has become highly important since the communication by transmitting of digital applications over the open network occur very frequently. In this paper, it has been reviewed that the existing works on the chaos based image encryption techniques. These encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security of digital images on transmitting through the networks. To sum up, all the techniques are useful for real-time digital image encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always workout with high rate of security.

References

[1] Chenghang Yu, Baojun Zhang and Xiang Ruan(2011),The Chaotic Feature of Trigonometric Function and Its Use for Image Encryption, Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD).

[2] C.K. Huang and H.H. Nien(2009), Multi chaotic systems based pixel shuffle for image encryption, Optics Communications 282 (2009) 2123–2127.

[3] Ercan Solak, Rhouma Rhouma and Safya Belghith(2010),Cryptanalysis of a multi-chaotic systems based image cryptosystem, Optics Communications 283 (2010) 232–236.

[4] G.A.Sathishkumar ,Dr.K.Bhoopathy bagan and Dr.N.Sriraam(2011), Image Encryption Based on Diffusion and Multiple Chaotic Maps, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.

[5] John Justin M, Manimurugan S (2012), A Survey on Various Encryption Techniques, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[6] Komal D Patel, Sonal Belani(2011),Image Encryption Using Different Techniques:A Review, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 1, Issue 1, November 2011).

[7] LEI Li-hong ,BAI Feng-ming,HAN Xue-hui(2013), New Image Encryption Algorithm Based on Logistic Map and Hyper-chaos, International Conference on Computational and Information Sciences.

[8] Mohammad Ali Bani Younes and Aman Jantan(2008), Image Encryption Using Block-Based Transformation Algorithm, IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03.

[9] Parameshachari B D, K M Sunjiv Soyjaudah, Chaitanyakumar M V)(2013), A Study on Different Techniques for Security of an Image, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-6, January 2013.

[10] Rajinder Kaur, Er.Kanwalprit Singh(2013).Image Encryption Techniques:A Selected Review, *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 6 (Mar. - Apr. 2013), PP 80-83*.

[11] Rashidah Kadir, Rosdiana Shahril, Mohd Aizaini Maarof(2010), a modified image encryption scheme based on 2D Chaotic map, International Conference on Computer and Communication Engineering (ICCCE 2010), 11-13 May 2010, Kuala Lumpur, Malaysia.

[12] Shubo Liu, Jing Sun1, Zhengquan Xu(2009), An Improved Image Encryption Algorithm based on Chaotic System, Journal of Computers, Vol. 4, No. 11.

[13] S.HRAOUI, F.GMIRA, A.O.JARAR ,K.SATORI and A.SAAIDI(2013),Benchmarking AES and Chaos BasedLogistic Map for Image Encryption, 978-1-4799-0792-2/13/$31.00 ©2013 IEEE.

[14] XiaoJun Tong , Yang Liu, Miao Zhang and Zhu Wang(2012), A Novel Image Encryption Scheme Based on Dynamical Multiple Chaos and Baker Map, 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science.

[15] Yunpeng Zhang, Peng Sun, Jing Xie and LifuHuang(2010), A New Image Encryption Algorithm Based on Arnold and Coupled Chaos Maps, International Conference on Computer and Communication Technologies in Agriculture Engineering.