INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

REVIEW ON DIFFERENT CHAOTIC BASED DIGITAL IMAGE ENCRYPTION TECHNIQUES

MISS. GAURI ULHE[1], PROF. KOMAL BIJWE[2]

Computer Science and Engineering, Prof. Ram Meghe Institute of Technology and Research, Badnera.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Due to rapid growth of communication facilities and decreasing cost of computer hardware has bought tremendous expansion for commercial academic. So due to that 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. Giving protection to digital images during transmission becomes more serious concern when they are confidential war plans, secret weapon photographs, military data and architectural design of building etc. There are many mechanisms like cryptography, steganography, hash functions, digital signatures have been designed to provide the ultimate safety for secret data. Therefore issue of protecting the confidentiality, integrity, security, privacy as well as the authenticity of images become an important issue for communication and storage of images. Various encryption techniques are developed to protect the confidential images from unauthorized users. This paper has a review on the different image encryption techniques based on chaos. Finally, The 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

Corresponding Author: MISS. GAURI ULHE

Access Online On:

www.ijpret.com

How to Cite This Article:

Gauri Ulhe, IJPRET, 2015; Volume 3 (9): 1310-1315

PAPER-QR CODE

INTRODUCTION

The rapid growth of computer and network technology, sending data in form of text, videos, images, sounds and have become an important security issue. Now more data in image format needs to be transferred over the network, as images are more descriptive in nature. If the digital images contain covert data like medical images X-rays military maps, etc., then they need a solid mechanism for transmission of images. The special attributes of digital images like bulk data capacity, high redundancy and high correlation between neighboring pixels must be considered carefully while choosing them as media for electronic data transfer. Hence an inevitable and best solution to send images can be cryptography. Cryptography can be defined as the art of creating an unintelligible intelligent information. Encryption of textual data is mostly relevant to one-dimensional data, that' why these techniques are incompetent for two-dimensional digital images. Now-a-days, research on image transfer has reached a high standard and lots of encryption mechanisms have been devised. These techniques can be broadly classified into cryptography, steganography and digital watermarking. Steganography is the art of hiding a secret message within a larger one. However, cryptography still stands out as the preferred way of image transfer. Encryption in digital images mostly works at pixel level, which is the lowest level of information in the image. The advantages of chaotic based image encryption scheme are easy to implement, faster encryption speed and strong against attacks [3]. Many image encryption schemes based on chaotic have been proposed [3].

RELATED WORK

In this section, describing the research work of some prominent authors in the same field and present description of various chaos based techniques used for image Encryption. There are number of technique based on chaos based encryption.

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 function in nature. There are many interesting features in encryption field. 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. Trigonometric function is the most basic and important function in nature. Any functions can be disassembled into the sum of multi-trigonometric functions. In

this technique image encryption a complicated chaotic system using the boundary property of trigonometric function is used for image encryption [1].

2. Cryptanalysis of a multi-chaotic systems based image cryptosystem, in the year 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 is arise from the use of the same shuffling process for every plain image. 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 [2].

3. 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 technique, 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 previous map. 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 chaotic system, binary sequence is generated [3].

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

LEI Li-hong, BAI Feng-ming 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 an image secure communication [4].

5. 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[5].

6. 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 [6].

7. 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. 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 [8].

- **8. Chaotic Image Encryption Based on Running-Key Related to Plaintext 2014**

Cao Guanghui, Hu Kai, Zhang Yizhi, Zhou Jun, and Zhang Xing proposed a new algorithm based on chaotic encryption on running key related to plaintext. According to the type of key related to plaintext, the existing image encryption algorithms can be divided into two categories. One is initial-key related to plaintext. The other is running-key related to plaintext.. This algorithm uses plaintext to disturb the current chaotic number and then takes the disturbed chaotic number as the next input of chaotic iteration. Repeat this process and use the last value as the initial key. By doing so, the correlation initial-key and plaintext is created. The other encryption does not use the whole chaotic numbers, but only utilizes partial elements as running key. Due to cipher-text closely related to plaintext, running-key is indirectly related with plaintext[9].

CONCLUSION

Due to increasing development of computer technology and wide application of internet, the security for the digital images 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 different 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. Each technique is unique depending upon their feature.

REFRENCES

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 (FSKD).

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

3. G. A. Sathishkumar ,Dr.K.Bhoopathy bagan and Dr.N.Sriraam(2011), Image Encryption Based on Diffusion and Multiple Chaotic Maps, (IJNSA), Vol.3, March 2011.

4. 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

5. Rajinder Kaur, Er.Kanwalprit Singh(2013).ImageEncryptionTechniques:A Selected Review, *IOSR Journal of Computer Engineering (IOSR-JCE) e- ISSN: 2278-0661, (Mar. - Apr. 2013), PP 80-83*.

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

7. 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.

8. Cao Guanghui, Hu Kai, Zhang Yizhi, Zhou Jun, and Zhang Xing, Chaotic Image Encryption Based on Running-Key Related to Plaintext**,** The Scientific World Journal Volume 2014.