Image Cryptography: A Survey towards its Growth

Pradeep Kumar
Manipal University Jaipur
2 PUBLICATIONS **1** CITATION
SEE PROFILE

Advance in Electronic and Electric Engineering.
ISSN 2231-1297, Volume 4, Number 2 (2014), pp. 179-184
© Research India Publications
http://www.ripublication.com/aeee.htm

Image Cryptography: A Survey towards its Growth

Prasenjit Kumar Das[1], Mr. Pradeep Kumar[2] and Manubolu Sreenivasulu[3]

[1]Dept. of CSE, MUJ, Manipal University Jaipur, Jaipur.
[2,3]Dept. of CSE, MUJ, Manipal University Jaipur, Jaipur.
E-mail: [1]prasenjitkumardas@muj.manipal.edu, [2]pradeepkumar@jaipur.manipal.edu,
[3]sreenevasulumanubolu@muj.manipal.edu

Abstract

This paper mainly focus on the different cryptographic algorithms used for the image encryption and decryption in the field of image security. Security has gained a lot of importance as information technology is widely used.Since, digital image has become an important medium of communication, researcher's have come up with different techniques from time to time to ensure security of the images. Cryptography refers to the study of mathematical techniques and related aspects of Information Security like data confidentiality, data Integrity, and of data authentication. This paper presents a survey of different image cryptographic algorithms proposed in the last decades with some advance methods. Moreover it provides the various aspects used for the image security.

Keywords: Cryptography; Image encryption; Image decryption.

1. Introduction

As digital image play an important role in multimedia technology, it becomes more important for the user's to maintain privacy. And to provide such security and privacy to the user, image encryption is very important to protect from any unauthorised user access. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication. Colour images are being transmitted and stored in large amount over the Internet and wireless networks, which take advantage of rapid development in multimedia and network technologies. For long time cryptography plays an important role in the field of security and it is battleground for the mathematicians and scientists, starting from Shanon’s that dates back to 1949[1].Several cryptographic algorithms have been proposed upto now like AES, DES,RSA, IDEA etc.

The image encryption techniques are different from the data encryption techniques. And there several security problems associated with digital image processing and transmissions, so it is necessary to maintain the integrity and theconfidentiality of the image. Moreover digital images are comparatively less sensitive than data because any single change in the pixels of the does not change the entire image. In other words a small modification of digital image is acceptable compared to data but it is more prone to attackers. Fig 1 shows a general image encryption process using any image encryption algorithm and resultant encrypted image.

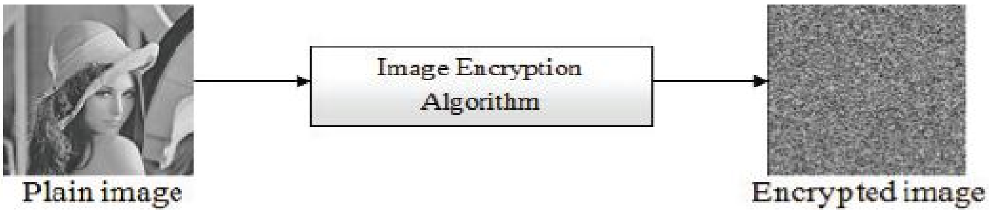

Fig. 1: Image Encryption.

2. Literature Review

2.1 New Mirror-Like Image Encryption Algorithm and Its VLSI Architecture.

Jiun-In Guo and Jui-Cheng Yen [2] have presented an algorithm which was mirror like. In this algorithm there were 7 steps. In the first, 1-D chaotic system is determined and its initial point x (0) and sets k = 0. Then, the chaoticSequence is generated from the chaotic system. After that binary sequence is generated from chaotic system. And in last 4 stages image pixels are rearranged using swap function according to the binary sequence.

2.2 A new image encryption algorithm based on hyper chaos, 2008

The method proposed by Tiegang Gao and Zengqiang Chen [3],uses hyper chaos to encrypt the image. The method is divided into two parts. In the first part, total shuffling of the image pixels take place.in second part, the shuffling image is encrypted using the hyper chaos. The hyper chaos is used to change the gray values of the image pixels. First part contains then row transformation based on the logistic map, using which, the rows of the plain image are shuffled. Then column transformation takes place which is also dependent on the logistic map. The columns of row-transformed image are then further shuffled. After the shuffling place, the image pixels are dispersed randomly and hence the image becomes encrypted but the histogram of the shuffled image remains same as that of the histogram of the plain image. hence, further encryption of the shuffled image takes place based on the hyper-chaotic system..

2.3 A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system, 2011

Presented by Xiaopeng Wei, Ling Guo, QiangZhanga,Jianxin Zhang and ShiguoLian[4]. In this paper, a novel color image encryption algorithm based on DNA sequence operation and hyper- chaotic system is proposed. In the proposed scheme, Chen's hyper-chaotic system is used to scramble the position of the pixels. The color image is converted into three matrices for R, G and B which are further transformed into binary matrices. Then these matrices are encoded according to DNA encoding rule. The chen's hyper-chaotic sequence is used to scramble the R ,G and B. the scrambled R,G and B are converted into blocks and then DNA addition operation is performed on the blocks. Now, the blocks are recombined and DNA decoding operation is performed to get the binary matrices. These binary matrices are further combined to get the encrypted image. The method improves the ability to resist differential attack by using hamming distance to generate the secrete keys. Furthermore, experimental results and security analysis shows that the algorithm has good encryption effect. Larger secret key space and high sensitive to the secrete key.

2.4 An Image Encryption and Authentication scheme, 2011

The scheme was proposed by Jing Qiuand ping Wang [5].The method presents a fast image encryption and authentication scheme. In the scheme, a 512 bit message authentication code (MAC) of the plain image is converted into 64 bytes and these 64 bytes are replaced with the image pixels in some way. Replaced pixels are then embedded into the image by reversible data embedding technique. Then the embedded image is masked by using the pseudo random sequence in feedback mode. The MAC provides authentication and also provides some encryption to the image. The scheme provides encryption as well as authentication to the image the embedded MAC plays important role in determining the integrity of the image.

2.5 Image cryptography: The Genetic Algorithm Approach, 2011

The genetic algorithm approach was proposed by SandeepBhowmik and SriyankerAcharya[6]. In this approach, the Genetic algorithm an important method of artificial intelligence has been applied to generate 'key' for the encryption algorithm .In this work a hybridized technique called BlowGA is used which is a combination of Blowfish and GA. This new approach has outperforms the result both Blowfish and GA separately.

2.6 Image Encryption Using Differential Evolution Approach in Frequency Domain

Ibrahim S I Abuhaiba and Maaly A S Hassan [7] present a new effective method for image encryption which employs magnitude and phase manipulation using Differential Evolution (DE) approach. In order to demonstrate the security of the new image encryption algorithm, key space analysis, statistical analysis, and key sensitivity analysis was carried out by them.

2.7 An Image Encryption based on elementary cellular automata, 2012

A novel symmetric image encryption scheme based on elementary cellular automata (ECA) is proposed by Jun JIN [8].The main concept of the scheme is derived from the analytical study of the state transition behaviour of length 8 ECA with periodic boundary conditions. A Cellular automata (CA) is a mathematical model of a system, having discrete inputs and outputs. It represents the sequential of a number of interconnected cells, arranged in a regular manner. Each cell has a finite set of possible values. A CA executes in discrete time steps and the value of a particular cell(local state) is affected by the cell values in its nearest neighbourhood on the previous step. The values of a cell also depend on a function known as the CA rule. Elementary CA is the simplest case, which is a linear array of cells, with three neighbourhood dependencies, and state of each cell is either 0 or 1.when dealing with finite CA periodic boundary(for cyclic boundary) conditions are usually applied.

2.8 An authenticated image encryption scheme based on chaotic maps and memory cellular automata, 2013

The method proposed by AtiehBakhshandeh and ZibaEslami [9], provides authentication and encryption to the image based on chaotic maps and linear memory cellular automata (LMCA). The cellular automata are discrete dynamical systems composed of an array of N identical objects called cells. Each cell can hold a state {0,1}.Each cell is updated synchronously according to a local transition function in discrete time steps. The updated state of each cell depends on the input of the function. The input is the previous state of a set of cells, including the cells that are called the neighbourhood.

2.9 An Encryption and Decryption Algorithm for Image Based on DNA

In 2013, a novel colour image encryptionalgorithm based on DNA sequence operation and hyper chaotic system was proposed[10] . In this paper chen’s hyper-chaotic system is used to scramble the position of the pixels then the colour image is converted into three matrices for R, G and B which are transformed into binary matrices and DNA addition operation is performed .The experimental results and the security analysis will shows that algorithm has good encryption effect, larger secret key space and high sensitivity to the secret key.

2.10 Image Encryption Based on Bit-plane Decompositionand Random Scrambling

Qiudong Sun, Wenying Yan, Jiangwei Huang, WenxinMa[11] general random scrambling method was designedwhich has more stable scrambling degree than the classicalmethod Arnold transform. At first, they decomposed a grayimage into several bit-plane images. Then we shuffled them by a random scrambling algorithm separately. Lastly, we merged the scrambled bit-plane images according to their original levels on bit-planes and gained an encrypted image. Due to each bit-plane image is scrambled by usingdifferent scrambling random sequences, the bits located at the same coordinates in different bit-planes are almost not stay on the original positions when each bit-plane being scrambled separately. For each pixel, its all bits of gray level, therefore, may be come from those pixels located different positions. Consequently, the reconstructed graylevels of image are changed ineluctable. It is obvious that our method can do both positions exchange scrambling and gray level change scrambling at the same time.

3. Conclusion

Image plays an important role in lives and they are used in many applications in our day to day lives. Therefore it is necessary to affirm the integrity and confidentiality of the digital image that being transmitted.

Some of the image encryption techniques are discussed that plays an important role in image transmission. In this paper a survey of some important image cryptography is provided in last decades.

This encryption methods are studied and analysed well to promote the performance of encryption methods. Each technique is unique in its own way and this make it suitable for its many application. Everyday new techniques are evolving hence fast and secure conventional encryption techniques work with high security rate. This survey provide a way to realize the different aspects that are used from chaotic to Genetic algorithms approach and DNA sequence for image encryption.

References

[1] Shannon CE [1949] "Communication theory of secrecy system,"Bell System Technical Journal, Volume 28, pp. 656 – 715.

[2] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryptionalgorithm and its VLSI architecture", Pattern Recognition and Image Analysis, vol.IO, no.2, pp.236-247, 2000.

[3] TiegangGao, Zengqiang Chen, "A new image encryption algorithmbased on hyper-chaos", Physics Letters A 372 (2008) 394–400.

[4] Xiaopeng Wei, Ling Guo, QiangZhanga, Jianxin Zhang and ShiguoLian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system", The Journal of Systems and Software 85 (2011) 290– 299.

[5] Jing Qiu and Ping Wang, " Image encryption and authentication scheme", IEEE, Computational Intelligence and Security (CIS), 2011 Seventh International Conference, 3-4 Dec. 2011, 784 – 787.

[6] SandeepBhowmik and SriyankarAcharya, "Image Cryptography: The Genetic Algorithm Approach", IEEE, 2011,978-1-4244-8728-8.

[7] Ibrahim S I Abuhaiba , Maaly A S Hassan, "Image Encryption Using Differential Evolution Approach In Frequency Domain" , Signal & Image Processing An *International Journal (SIPIJ) Vol.2, No.1,March 2011.*

[8] Jun Jin, “An image encryption based on elementary cellular automata”,Optics and Lasers in Engineering 50 (2012) 1836–1843

[9] AtiehBakhshandeh and ZibaEslami , “An authenticated image encryption scheme based on chaotic maps and memory cellular automata”, Optics and Lasers in Engineering, Volume 51, Issue 6, June 2013, Pages 665-673.

[10] RanuSoni, Arunjohar and vishakhasoni, “An Encryption and Decryption Algorithm for Image Based on DNA”, IEEE, 2013,978-0-7695-4958-3/13

[11] Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma, “ImageEncryption Based on Bit-plane Decomposition and RandomScrambling”, *Journal of Shanghai Second Polytechnic University ,vol. 09 IEEE, 2012.*