Different Algorithms used in Image Encryption: A review

Bharti Ahuja
Department of Computer Science & Engineering
Sagar Institute of Research & Technology
Bhopal, M.P., India
bharti.ahuja.salunke@gmail.com

Rashmi Lodhi
Department of Computer Science & Engineering
Sagar Institute of Research & Technology
Bhopal, M.P., India
rrashi_jbp@yahoo.co.in

Abstract—As a result of the development of computer network technology, communication of information through personal computer is becoming more convenient. Meanwhile, it also gives hackers opportunities to attack the network. Therefore the communication security is now an important issue for multimedia communications. In recent years, many image cryptosystems are proposed. As encryption process is applied to the whole image, it is difficult to improve the efficiency. Encryption of digital image processing becomes more and more important for Internet data transportation and many methods can be applied for the processing.

In this paper, we survey on existing work which is used different techniques for image encryption and we also give general introduction about cryptography.

Keywords— Cryptography, Encryption, Decryption

I. INTRODUCTION

In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via e-mails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the 'security threat'. It poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring.

Data security basically means protection of data from unauthorized users or hacker, providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. In order to improve the security features in data transfers over the internet and for information hiding into digital media, many techniques have been developed like: Cryptography, Steganography and Digital watermarking.

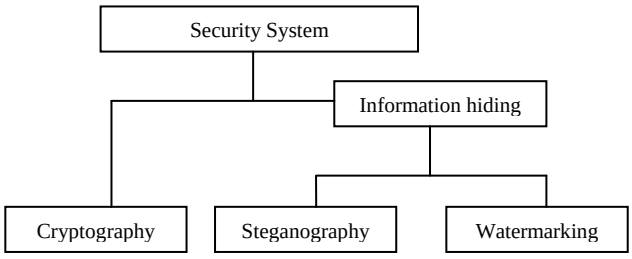

Fig. 1 : Techniques for Information Security.

Cryptography is the art and science of securing messages. It is the practice and study of hiding information. It attempts to make sure that the message is comprehensible only to the 'legal' recipient of the message - the person for whom it is intended. The aim here is that even if an unintended person gets hold of the message, he will not be able to make sense of it without the key much as with a good lock. Anyone can find their way to your home, but cannot get in without the key. In cryptography the key is some information that the sending and receiving parties agree upon. If the agreed upon information is a secret message, we are in the domain of symmetric-key cryptography. Its counter part is asymmetric-key cryptography.

Cryptography is realized through encryption and decryption procedures. Encryption is a modification of the message in such a way that its content can be reconstructed only by a legal recipient, while decryption is the reconstruction of the original message from the encrypted message (also called cipher-text). A cryptosystem implements the encryption and decryption mechanisms. Mathematically, a discrete valued cryptosystem is defined by a set of possible:

• Plaintexts P

• Cipher texts C

• Cipher keys K

• Encryption and decryption transforms E and D.

Cryptography technique is used when secret message are transferred from one party to another over a communication line. There are two main types of cryptography:

• Secret key cryptography

• Public key cryptography

Secret key cryptography is also known as *symmetric key* cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

Public key cryptography, also called *asymmetric key cryptography*, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys. Cryptography technique needs some algorithm for encryption of data.

Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, we need to ensure information security and safety. Image is also an important part of our information .Therefore it's very important to protect our image from unauthorized access. There are so many algorithms available to protect image from unauthorized access which is described in next section.

The second section of the paper is subdivided into thirteen parts, where different techniques have used for image encryption. In Section III, a conclusion will be reached.

II. LITERATURE SURVEY

With the rapid development of Internet and the wide application of multimedia technology, people can communicate the digital multimedia information with others conveniently in the internet. In many cases, we hope our image data which are transmitted on the network do not be browsed or processed by illegal receivers. Therefore, the security of digital images attracts much attention recently and many different methods for image encryption have been proposed.

A. Image encryption using chaotic logistic map,2006

N.K. Pareek, Vinod Patidar introduce a image encryption method using chaotic logistic map [1]. In this paper image encryption scheme, an external secret key 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 weightage to all its bits. Further, in the encryption process, eight different types of operations are used to encrypt the pixels of an image and which one of them will be used for a particular pixel is decided by the outcome of the logistic map. To make the cipher more robust against any attack, the secret key is modified after encrypting each block of sixteen pixels of the image. The results of several experimental, statistical analysis and key sensitivity tests show that the image encryption scheme provides an efficient and secure way for real-time image encryption and transmission.

B. Image encryption with compound chaotic sequence cipher shifting dynamically,2007

Xiaojun Tong, Minggen Cui design a new two-dimensional chaotic function using two one-dimensional chaotic functions, and then prove the chaotic properties to a new function by choosing one of the two one-dimensional chaotic functions randomly [2].

C. Cryptanalysis of an image encryption scheme based on a compound chaotic sequence,2008

Chengqing Li, Shujun Li, Guanrong Chen, Wolfgang A. Halang design an image encryption scheme based on a compound chaotic sequence. In this paper, the security of the scheme is studied and the following problems are found: (a) a differential chosen-plaintext attack can break the scheme with only three chosen plain-images; (b) there is a number of weak keys and some equivalent keys for encryption; (c) the scheme is not sensitive to the changes of plain-images; and (d) the compound chaotic sequence does not work as a good random number source[3].

D.The algorithm of Fractional Fourier Transform and application in digital image encryption,2009

Yuhong Zhang, Fenxia Zhao introduce a image Encryption algorithm using fourier transform. In this paper the matrix algorithm of discrete fractional Fourier transform is an approximate method to calculate the FrFT [4]. But the Limitation is that, the encrypted digital Image can be decrypted by someone who attempts parameter; he may get the correct decryption digital image. In other word, this encryption can improve with more complex method as encrypt two or more digital image as one [4].

E. Image Encryption with Discrete Fractional Cosine Transform and Chaos,2009

Lin Zhang, Jianhua Wu and Nanrun Zhou proposed a method for image encryption with discrete fractional cosine transform and chaos .Chaos function has extreme sensitivity to the initial conditions, the effect of image encryption with DFrCT and chaos is better than in the case of DFrCT. Due to the reality of DFrCT and the confusion properties, the proposed cryptosystem is extremely secure and the transmission of the encrypted images is fast [5].

F. Hybrid Image Encryption Using Multi-Chaos-System,2009

H. H. Nien, W. T. Huang, C. M. Hung, S. C. Chen, S. Y. Wu proposed A Hybrid Image Encryption using Multi-Chaos-System, this method uses hybrid encryption technique for the color image based on the multichaotic-system which combines Pixel-Chaotic-Shuffle (PCS) and Bit-Chaotic-Rearrangement (BCR) and increases the key space of images [6].

G.Image Encryption With Multiorders of Fractional Fourier Transforms,2010

Ran Tao, Xiang-Yi Meng, Yue Wang proposed the another technique for image encryption using multi order fractional Fourier transform. In this paper, the encrypted image is obtained by the summation of different orders of IDFRFT of the interpolated sub images. The whole transform orders of the utilized FRFT are used as the secret keys for the decryption of each sub image. Compared with the traditional image encryption methods based on the FRFT, the method is with a larger key space and the amount of keys can be set as large as two times the amount of the pixels in the original image. In future work, one can also combine the proposed method with other image encryption methods to enhance the security of the system [7].

H.Image Encryption using Discrete Fractional Transforms,2010

Neeru Jindala, Kulbir Singh proposed a method for image encryption using Fractional Fourier Transforms and compares the DFrFT and DFrCT and the performance of two recently proposed image encryption algorithms involving the use of discrete fractional transform. Simulation results under conditions of ideal encryption, decryption with correct and incorrect keys verify the performance of these techniques, that DFrCT is better for the encryption. Robustness of keys for decryption has also measured [8].

I. A Chaos-Based Image Encryption Algorithm Using Wavelet Transform,2010

Zhu Yu, Zhou Zhe, Yang Haibing, Pan Wenjie, Zhang Yunpeng proposed a method Chaos-Based Image Encryption Algorithm using Wavelet Transform, in this paper the algorithm uses the wavelet decomposition concentrating image information in the high-frequency sub-band image, and then encryption is applied for the sub-band image. After a wavelet reconstruction is introduced in order to spread the encrypted part throughout the whole image. A second encryption process is used to complete the encryption process. Theoretical analysis and experimental results show that the algorithm has an obvious increase in efficiency, as well as satisfied security [9].

J. Double-image encryption based on discrete fractional random transform and chaotic maps,2011

Huijuan Li, Yurong Wang design a novel double-image encryption algorithm based on discrete fractional random transform and chaotic maps. The random matrices used in the discrete fractional random transform are generated by using a chaotic map. One of the two original images is scrambled by using another chaotic map, and then encoded into the phase of a complex matrix with the other original image as its amplitude. Then this complex matrix is encrypted by the discrete fractional random transform. By applying the correct keys which consist of initial values, control parameters, and truncated positions of the chaotic maps, and fractional orders, the two original images can be recovered without cross-talk[10].

K.Image encryption by using local random phase encoding in fractional Fourier transform domains,2011

Zhengjun Liu, Lie Xu, Jingmin Dai, Shutian Liu proposed an image encryption algorithm based on fractional Fourier transform. A local random phase encoding is introduced into this algorithm. The data at the local area of complex function is converted by fractional Fourier transform[11].

L. SD-AEI: An Advanced Encryption Technique for Images,2012

Somdip Dey proposed a method, SD-AEI, for image encryption, which is an upgraded module for SD-EI combined image encryption technique and basically has three stages: 1) In first stage, each pixel of image is converted to its equivalent eight bit binary number and in that eight bit number, the number of bits, which are equal to the length of password are rotated and then reversed; 2) In second stage, extended hill cipher technique is

applied by using involutory matrix, which is generated by same password used in second stage of encryption to make it more secure; 3) In third stage, the whole image file is randomized multiple number of times using Modified MSA Randomization encryption technique and the randomization is dependent on an unique number, which is generated from the password provided for encryption[12].

M. A New Hybrid-Domain Image Encryption based on Chaos with Discrete Cosine Transform,2012

R. Krishnamoorthi, P.Murali proposed a new hybrid-domain image encryption technique that uses the frequency-domain encryption with Discrete Cosine Transform (DCT) incorporating multi resolution approach and spatial domain for pixel shuffling. First, original image divided into significant and insignificant blocks using prewitt's edge detector operator and significant blocks are encrypted using Arnold cat map and Logistic map. Next, insignificant blocks are shuffled in the DCT domain using Arnold cat map then inverse DCT applied and pixels in the blocks are XORed with discretised output of logistic map. Finally, diffusion process is applied to get final encrypted image and the numerical simulations have demonstrated the security and robustness of the proposed encryption scheme[13].

III. CONCLUSION

In the digital world nowadays, the security of digital images become more and more important since the communications of digital products over open network occur more and more frequently. In this paper, we have surveyed existing work on image encryption. We also give general guide line about cryptography. We conclude that all techniques are useful for real-time image encryption.

REFERENCES

[1] N.K. Pareek, Vinod Patidar, "Image encryption using chaotic logistic map", Elsevier, Image and Vision Computing 24 (2006) 926–934.
[2] Xiaojun Tong, Minggen Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically", Elsevier, Image and Vision Computing 26 (2008) 843–850.
[3] Chengqing Li, Shujun Li, Guanrong Chen, Wolfgang A. Halang,"Cryptanalysis of an image encryption scheme based on a compound chaotic sequence", Elsevier, Image and Vision Computing 27 (2009) 1035–1039.
[4] Yuhong Zhang, Fenxia Zhao, "The algorithm of Fractional Fourier Transform and application in digital image encryption", IEEE 2009.
[5] Lin Zhang, Jianhua Wu and Nanrun Zhou, "Image Encryption with Discrete Fractional Cosine Transform and Chaos", Fifth International Conference on Information Assurance and Security, IEEE 2009.
[6] H. H. Nien, W. T. Huang, C. M. Hung, S. C. Chen, S. Y. Wu," Hybrid Image Encryption Using Multi-Chaos-System", IEEE 2009.
[7] Ran Tao, Xiang-Yi Meng, Yue Wang, "Image Encryption With Multiorders of Fractional Fourier Transforms", IEEE transactions on information forensics and security, 2010.
[8] Neeru Jindala, Kulbir Singh,"Image Encryption using Discrete Fractional Transforms", International Conference on Advances in Recent Technologies in Communication and Computing, IEEE 2010.
[9] Zhu Yu, Zhou Zhe, Yang Haibing, Pan Wenjie, Zhang Yunpeng,"A Chaos-Based Image Encryption Algorithm Using Wavelet Transform", IEEE 2010.
[10] Huijuan Li, Yurong Wang," Double-image encryption based on discrete fractional random transform and chaotic maps", Elsevier, Optics and Lasers in Engineering 49 (2011) 753–757.
[11] Zhengjun Liu, Lie Xu, Jingmin Dai, Shutian Liu,"Image encryption by using local random phase encoding in fractional Fourier transform domains" Elsevier, Optik 123 (2012) 428– 432.
[12] Somdip Dey, "SD-AEI: An Advanced Encryption Technique For Images", IEEE 2012.
[13] R. Krishnamoorthi, P.Murali," A New Hybrid-Domain Image Encryption based on Chaos with Discrete Cosine Transform", 4th International Conference on Electronics Computer Technology, IEEE 2012.