A Survey on Techniques for Image Encryption

Dhara K Soni[1]
[1]Department of Computer Engineering
[1]Silver Oak College of Engineering and Technology

Abstract- *As the exchange of data over the open networks as Internet is rapidly growing, security of the data becomes a major issue. One possible solution to this problem is to encrypt the data. The data can be text, image, audio, video etc. In today's world most of the multimedia applications involve images. Image encryption provides guarantee to classified transmission and capacity of image over web. In this survey paper an attempt has been made to review the aspects and approaches of the design used for image encryption.*

Keywords- Asymmetric key cryptography, Decryption, Encryption, Image encryption, Symmetric key cryptography.

I. INTRODUCTION

With the ever-increasing growth of multimedia applications, security is an important issue in communication and encryption is one the ways to ensure security. 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, so that nobody could get to know the content without a key for decryption.

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor [1]. There are basically two type of Encryption and Decryption in cryptography.

1) Asymmetric key cryptography

2) Symmetric key cryptography

In symmetric-key schemes, both the keys are the same. Communicating parties must have the same key before they can achieve secure communication. In asymmetric-key encryption schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key that enables messages to be read. Cryptography technique is used when secret message are transferred from one party to another over a communication line. 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. The algorithms which are available to protect images are described below.

II. PRELIMINARIES

2.1 Plain Text

The original message that the person wishes to communicate with the other is defined as plain text. In cryptography the actual message that has to be send to the other end is given a special name as plain text.

2.2 Cipher Text

The message that cannot be understood by anyone or eaningless message is what we call as cipher text. In cryptography the original message is transformed into non-readable message before the transmission of actual message.

2.3 Ciphers

A cipher encrypts a single letter or group of letter as a unit, regardless of meaning.

2.4 Codes

A code encodes a word or phrase usually at a time in a fixed way without using key.

2.4 Encryption

An encryption is a process of converting plaintext into cipher text. An encryption is used to provide confidentiality to the data. Encryption process requires an encryption algorithm and key. Encryption is done by sender.

2.5 Decryption

Decryption is a reverse process of an encryption. Decryption is used to convert cipher text in plain text. It happens at receiver side. Key which is used at sender side will also be available to the receiver side to decrypt the data.

2.6 Key

Key performs a very important role in cryptography. Selection of key is very important because all the security is

depend onthe key selection. A key can be a text or any special symbol.

III. LITERATURE SURVEY

[1] Image Encryption Using Advanced Hill Cipher Algorithm, 2009

Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda [1] have proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption. They have taken different images and encrypted them using original Hill cipher algorithm and their proposed AdvHill cipher algorithm. And it is clearly noticeable that original Hill Cipher can't encrypt the images properly if the image consists of large area covered with same colour or gray level. But their proposed algorithm works for any images with different gray scale as well as colour images.

[2] A Novel Image Encryption Algorithm Based on Hash Function, 2010

Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki [2] proposed a novel algorithm for image encryption based on SHA-512 hash function. The algorithm consists of two main sections: The first does pre-processing operation to shuffle one half of image. The second uses hash function to generate a random number mask. The mask is then XORed with the other part of the image which is going to be encrypted. This algorithm can be applied on both the color images and gray scale images.

[3] A Digital Image Encryption Algorithm Based Composition of Two Chaotic Logistic Maps, 2010

Ismail Amr Ismail, Mohammed Amin, and Hossam Diab[3] introduces an efficient chaos-based stream cipher, composing two chaotic logistic maps and a large enough external secret key for image encryption. In the proposed image encryption scheme, an efficient chaos-based stream cipher, composing two chaotic logistic maps and a large enough external secret key for image encryption. The external secret key is used to derive the initial conditions for the chaotic maps, and is employed with the two chaotic maps to confuse the relationship between the cipher image and the plain image. In the encryption phase, the pixels are encrypted using an iterative cipher module based feedback and data-dependent inputs mechanism for mixing the current encryption parameters with previously encrypted information. To make the cipher more robust against any attack, the secret key is
modified after encryption of each pixel of the plain image.

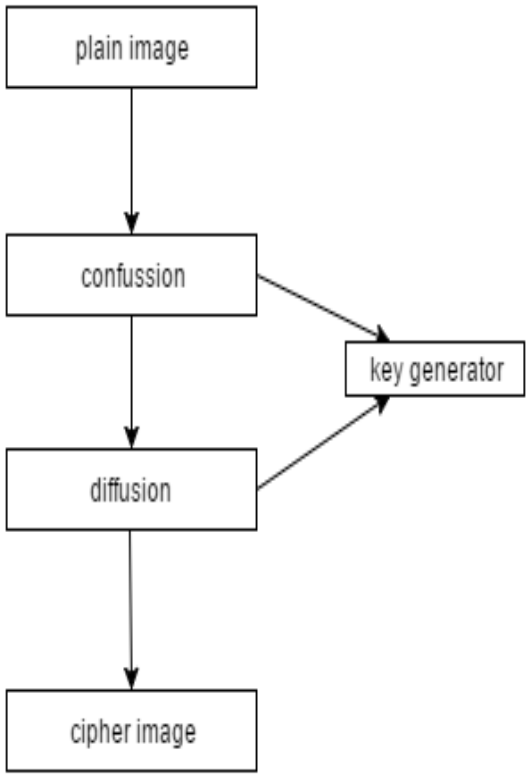
[4] A New Chaotic System for Image Encryption, 2012

Long Baoa, Yicong Zhoub [4] proposed a new system for image encryption. This paper introduces a new chaotic system which is composed of three different one-dimensional chaotic maps. The proposed system uses the Logistic map as a controller to choose the Tent map or Sine map to generate random sequences. The new system shows more complicated chaotic behaviours. The proposed encryption system uses the substitution-permutation network (SPN) structure. To enhance the security level, the encryption and decryption keys with the size of 240 bits are known to be long enough to withstand the brute-force attacks.

[5] A novel image encryption based on hash function with only two-round diffusion process, 2014

Norouzi and Benyamin [5] have proposed image encryption algorithm. In this paper, a novel algorithm for image encryption based on hash function is proposed. In our algorithm, a 512-bit long external secret key is used as the input value of the salsa20 hash function. First of all, the hash function is modified to generate a key stream which is more suitable for image encryption. Then the final encryption key stream is produced by correlating the key stream and plaintext resulting in both key sensitivity and plaintext sensitivity. This scheme can achieve high sensitivity, high complexity, and high security through only two rounds of diffusion process. In the first round of diffusion process, an original image is partitioned horizontally to an array which consists of 1,024 sections of size 8×8. In the second round, the same operation is applied vertically to the transpose of the obtained array.

IV. SYSTEM DIAGRAM



V. 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, I have surveyed existing work on image encryption. I conclude that all techniques are useful for real-time image encryption. Techniques describes in this paper that can provide security functions and an overall visual check, which might be suitable in some applications. So no one can access image which transferring on open network.

REFERENCES

[1] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda,‖ Image Encryption Using Advanced Hill Cipher Algorithm‖, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[2] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, ―A Novel Image Encryption Algorithm Based on Hash Function‖ 6th Iranian Conference on Machine Vision and Image Processing, 2010.

[3] Ismail Amr Ismail, Mohammed Amin, Hossam Dia ―A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps‖, International Journal of Network Security, Vol.11, No.1, PP.1 -10, July 2010.

[4] Bao, Long, et al. "A New Chaotic System for Image Encryption." 2012 International Conference on System Science and Engineering (ICSSE) (2012): n.pag. Web.

[5] Norouzi, Benyamin, et al. "A Novel Image Encryption Based on Hash Function with Only Two-Round Diffusion Process." Multimedia Systems 20.1 (2013): 45–64. Web.

[6] Ramahrishnan, S., Elakkiya, B., Geetha, R., Vasuki, P., Mahalingam, S. (2014). Image encryption using chaotic maps in hybrid domain. International Journal of Communication and Computer Technologies, 2(5), 44–48.

[7] Sesha Pallavi Indrakanti , P.S.Avadhani,‖ Permutation based Image Encryption Technique‖, International Journal of computer Applications (0975 – 8887) Volume 28– No.8, 2011.