© 2016 IJSRSET | Volume 2 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Literature Survey on Image Encryption

Kaushal T. Kevadia[*], Archana M. Nayak, Kaushik S. Patel, Brijesh U. Patel

Department of Computer Engineering, GIDC Degree Engineering College, Abrama, Navsari, Gujarat, India

ABSTRACT

Image encryption plays a paramount part to guarantee classified transmission and capacity of image over web. Then again, a real-time image encryption confronts a more noteworthy test because of vast measure of information included. This paper exhibits an audit on image encryption in spatial, frequency and hybrid domains with both full encryption and selective encryption strategy.

Keywords: Image Encryption, Domains of Image, Encryption, Full and Selective Image, Encryption Techniques, Chaotic Maps.

I. INTRODUCTION

As the data exchange in electronic way is rapidly increasing, it is also equally important to protect the confidentiality of data from unauthorized access. The breaches in security affect user's privacy and reputation. The data exchanged can be text, image, audio, video etc. Each type of data has its own features different techniques are used to protect confidential image data from unauthorized access. Hence encryption of data is done to confirm security in open networks such as the internet where the multimedia applications are ever growing. Cryptography is the study of techniques for secure communication in the presence of an adversary. It deals with problems like encryption, authentication, and key distribution to name a few. Image encryption is a technique that provides security to images by converting the original image into an image which is difficult to understand. Applications of image encryption can have extended to military communication, multimedia systems, medical science, telemedicine, internet communication etc. Generally, images are different from textual data. The idea for encryption of image is to consider a 2D image as a 1D data stream and this stream is encrypted with any textual based cryptosystem. This approach is called nave approach. For text, small bit rate audio, image and video files that can be sent over a fast-dedicated channel, this approach is suitable. Unfortunately, these encryption algorithms may not satisfy for different image data types like JPEG, PNG, BMP, etc... i.e. Traditional cryptosystems can be used to encrypt images, but it is not a good idea as image size is always much greater than the textual data. Also, the decrypted text should be equal to the original text, whereas this requirement is not necessary for image data. An image when decrypted contains small distortion and is usually acceptable because of the characteristic of human perception.

II. METHODS AND MATERIAL

A. Preliminaries

- 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.
- Cipher Text: The message that cannot be understood by anyone or meaningless 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.
- Ciphers: A cipher encrypts a single letter or group of letter as a unit, regardless of meaning.
- Codes: A code encodes a word or phrase at a time usually in a fixed way (no keys).
- Encryption: A process of converting plain text into cipher text is called as encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process

of encryption requires two things—an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

- Decryption: A reverse process of encryption is called as decryption. It is a process of converting cipher text into plain text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message (cipher text). The process of decryption requires two things—a decryption algorithm and a key. A decryption algorithm means the technique that has been used in decryption. Generally, the encryption and decryption algorithm are same.
- Key: A Key is a numeric or alpha numeric text or may be a special symbol. The key is used at the time of encryption takes place on the plain text and at the time of decryption take place on the cipher text. The selection of key in cryptography is very important since the security of encryption algorithm depends directly on it.

B. Purpose of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

- Confidentiality: Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.
- Authentication: The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity.
- Integrity: Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.
- Non-Repudiation: Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.
- Access Control: Only the authorized parties are able to access the given information.

C. Classification of Cryptography

Encryption algorithms can be classified into two broad categories - Symmetric and Asymmetric key encryption.

- Symmetric Encryption: In symmetric cryptography, the key used for encryption is similar to the key used in decryption. Thus, the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e., the key length etc. There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6, BLOWFISH. The symmetric algorithms are of two types Block ciphers &Stream ciphers.
- Asymmetric Encryption: Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access too.

D. Diffusion and Confusion

Shannon, in one of the fundamental papers on the theoretical foundations of cryptography, gave two properties that a good cryptosystem should have to hinder statistical analysis: diffusion and confusion. Diffusion means that if we change a character of the plain text, then several characters of the cipher text should change, and similarly, if we change a character of the cipher text, then several characters of the plain text should change. This means that frequency statistics of letters in the plain text are diffused over several characters in the cipher text, which means that much more cipher text is needed to do a meaningful statistical attack. Confusion means that the key does not relate in a simple way to the cipher text. In particular, each character of the cipher text should depend on several parts of the key.

E. Literature Review of Image Encryption

[1] A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. (2015) In this paper, a novel algorithm for image encryption based on the hyper-chaotic system is proposed. The algorithm consists of three main sections. In the first Section the rows and columns of the image are encrypted using a row-column algorithm. In the Second section employs masking process which is applied to each quarter of the image that is to be encrypted, using that sub-image data itself and one of the other sub-images and the average data of other quarters of image. Finally, in the last diffusion section, the four most significant bit planes will be encrypted.

[2] An image encryption scheme based on a new hyperchaotic finance system. (2015) In this paper, a new four-dimensional hyperchaotic finance system based on a chaotic finance system is presented. The chaotic sequence is generated by using Runge–Kutta method, the key sequence is generated by chaotic sequence comparison. The key sequence is used for image encryption with relation to plaintext.

[3] 2D Sine Logistic modulation map for image encryption. (2015) In this paper, introduce a new two-dimensional Sine Logistic modulation map (2D-SLMM) which is derived from the Logistic and Sine maps. To investigate its applications, they propose a chaotic magic transform (CMT) to efficiently change the image pixel positions. Combining 2D-SLMM with CMT, we further introduce a new image encryption algorithm. They use the trajectory, Lyapunov exponent, Lyapunov dimension and Kolmogorov entropy to evaluate its chaotic performance

[4] A secure transmission of 2D image using randomized chaotic mapping. (2016) Here logistic function one of the methods of chaotic map is used for encryption and decryption along with XOR function.

[5] A colour byte scrambling technique for efficient image encryption based on combined chaotic map: Image encryption using combined chaotic map. (2016) In this paper, an image encryption scheme based on colour byte scrambling technique is proposed by using Logistic map and Ikeda map. The proposed scheme is using Logistic map for generating permutation sequence to shuffle the colour bytes (confusion) and Ikeda map is used for generating masking sequence to change the value of the colour bytes (diffusion) of the 24-bit colour image.

[6] An implementation and performance evaluation of an improved chaotic image encryption approach. (2016) In this paper proposed work is the combinations of Chen Chaotic system, Hyper Chaotic system, Total Image Shuffling and Random Pixel Exchange These combinations are as follows: A) Random Pixel Exchange followed by Hyper Chaos B) Total Image Shuffling followed by Hyper Chaos C) Random Pixel Exchange followed by Chen Chaos D) Total Image Shuffling followed by Chen Chaos.

[7] Efficient image encryption with block shuffling and chaotic map. (2015) In the first step, they scramble image blocks to achieve initial encryption. In the second step, generate a set of secret matrices by a chaotic map and Arnold transform. They adopt the skew tent chaotic map for randomized secret matrix generation. Finally, encrypt each block by calculating exclusive OR operation between the corresponding elements of a random secret matrix and the image block. Note that these steps are controlled by secret keys. This is to ensure security of algorithm.

[8] A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. (2017) In this paper, they propose a hyper-chaos-based image encryption algorithm. The algorithm adopts a 5-D multiwing hyper-chaotic system, and the key stream generated by hyper-chaotic system is related to the original image. Then, pixel-level permutation and bit-level permutation are employed to strengthen security of the cryptosystem. Finally, a diffusion operation is employed to change pixels.

[9] Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences. (2016) In this paper, a hyper-chaos based image encryption algorithm is proposed. Firstly, a new hyper-chaotic system is constructed and its dynamic characteristics are analyzed. The proposed hyper-chaotic system has bigger Lyapunov exponent than many classical hyperchaotic systems. Then this system is used to generate key-streams to permute and substitute the image pixels. In the encryption algorithm, a dynamic S-box is constructed to get good confusion effect. This S-box is based on the inverse operation in

the algebraic structure Z257. Moreover, this inverse operation is embedded into an affine transformation to complicate the algebraic expression of the S-box and improve its security.

[10] A fast encryption algorithm of color image based on four-dimensional chaotic system. (2015)

This paper proposes a fast encryption algorithm of color image based on four-dimensional chaotic system. Firstly, they propose a new method of designing four-dimensional chaotic system based on the classical equations of three-dimensional chaotic system, to increase the complexity and key space of the encryption algorithm. Secondly, according to the nature of color images' pixels channel, they design a new pseudo-random sequence generator and reuse the random sequence, to improve the speed of image encryption. Finally, the methods of row-major and column-major are used to diffuse the original image and the cat map with parameter is used to scramble the image pixels, respectively, to achieve the effect of encryption.

[11] A new image cryptosystem based on 2D hyper-chaotic system. (2016): 1-22. An efficient image encryption scheme is designed based on 2D hyper-chaotic system. The confusion and the diffusion procedures of the proposed scheme are interacted on each other. In the encryption process, the position of the present pixel is influenced by the last diffused one. Then the corresponding diffused pixel makes a difference in the next pixel. The proposed cryptosystem with the interacted structure is steadier and harder to decipher. In addition, 2D hyper-chaotic systems are employed in the quicker generation of chaotic sequences in comparison to high-dimensional hyper-chaotic systems.

[12] A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution. (2016) This paper proposes a novel chaos-based image encryption scheme, in which the two-dimensional rectangular transform is employed to directly scramble the image of any rectangular size, and the dependent substitution is introduced to substitute for each pixel according to the image pixels. This scheme comprises two stages of encryption processes. Each stage provides the confusion and diffusion simultaneously in one traverse of image pixels.

[13] Digital color image encryption using RC4 stream cipher and chaotic logistic map. (2013) In this paper, they propose new secure algorithm for image encryption, which based on RC4 stream cipher algorithm and chaotic logistics map. The proposed algorithm works as follows: (i) converting the external key into initial value, (ii) using the initial value to generate a key stream using chaotic logistic map function, and (iii) processing a permutation and the result is then XOR-ed with bytes stream of digital image.

[14] An innovative image encryption scheme based on chaotic map and Vigenère scheme. (2016) In this paper, a novel image encryption scheme based on chaotic maps and Vigenère Scheme is proposed. This scheme has one round consisting of two steps: diffusion and confusion. The former step involves three stages: forward diffusion, matching process using Vigenère scheme and backward diffusion. In later part, position permutation using chaotic map is used to swap pixel positions. New type of modified logistic maps, intertwining logistic maps are used in proposed scheme.

[15] An image encryption scheme based on chaotic tent map. (2017) This paper proposes a novel image encryption scheme, which is based on the chaotic tent map. Image encryption systems based on such map show some better performances. Firstly, the chaotic tent map is modified to generate chaotic key stream that is more suitable for image encryption. Secondly, the chaos-based key stream is generated by a 1-D chaotic tent map, which has a better performance in terms of randomness properties and security level.

III. CONCLUSION

In this paper, large portions of the current essential image encryption methods have been exhibited and examined. In this review report, at first the stress have been made on officially existing image encryption algorithms in light of the fact that the most ideal method for ensuring media information like images is by method for the gullible algorithm; i.e., by scrambling the whole sight and sound bit succession utilizing a quick conventional cryptosystem. A great part of the past and momentum exploration targets scrambling just a deliberately chose piece of the image bit-stream keeping in mind the end goal to decrease the computational burden, and yet keep the security level high. Huge numbers of the proposed plans could just accomplish moderate to low level of security, which may discover applications in which quality debasement is favored over outright security. Then again, just few of the proposed strategies guarantee to attain considerable security, which is the prime prerequisite in numerous media applications. Secondly, we evaluated a wide-run of image encryption algorithms and ordered them on the premise of full and partial image encryption procedures under spatial space, frequency domain and hybrid domain categories. In the process, of this survey, a few perceptions were made, which are that full encryption plan guarantees high state of security of encoded information because of the way that they encode the whole image, however much time is used in such a procedure. On account of selective image encryption, just a locale or some piece of the image is scrambled. The time used in encoding the region of investment is less in contrast to the full encryption procedures. Hence, the partial encryption scheme is more suitable for constant applications. Therefore, partial image encryption scheme proved to be encouraging in term of encryption time, attaining an encryption procedure that adjusts security with transforming time for ongoing applications is still a challenge for researcher in image encryption. On the other hand, some key elements, for example, the sort of information to be encoded, the rate of the information that must be ensured and the measures put set up to ensure the information from cryptanalytic attack, when considered in the configuration of a continuous image encryption procedure might be a reasonable answer for ongoing image encryption issues.

IV. REFERENCES

[1] Norouzi, Benyamin, et al. "A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos." Multimedia Tools and Applications 74.3 (2015): 781-811.

[2] Tong, Xiao-Jun, et al. "An image encryption scheme based on a new hyperchaotic finance system." Optik-International Journal for Light and Electron Optics 126.20 (2015): 2445-2452.

[3] Hua, Zhongyun, et al. "2D Sine Logistic modulation map for image encryption." Information Sciences 297 (2015): 80-94.

[4] Raghuwanshi, Purvee, Jijo S. Nair, and Saurabh Jain. "A secure transmission of 2D image using randomized chaotic mapping." Colossal Data Analysis and Networking (CDAN), Symposium on. IEEE, 2016.

[5] Parvees, MY Mohamed, et al. "A colour byte scrambling technique for efficient image encryption based on combined chaotic map: Image encryption using combined chaotic map." Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on. IEEE, 2016.

[6] Suri, Shelza, and Ritu Vijay. "An implementation and performance evaluation of an improved chaotic image encryption approach." Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on. IEEE, 2016.

[7] Tang, Zhenjun, Xianquan Zhang, and Weiwei Lan. "Efficient image encryption with block shuffling and chaotic map." Multimedia tools and applications 74.15 (2015): 5429-5448.

[8] Li, Yueping, Chunhua Wang, and Hua Chen. "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation." Optics and Lasers in Engineering 90 (2017): 238-246.

[9] Liu, Ye, et al. "Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences." Multimedia Tools and Applications 75.8 (2016): 4363-4382.

[10] Tong, Xiao-Jun, et al. "A fast encryption algorithm of color image based on four-dimensional chaotic system." Journal of Visual Communication and Image Representation 33 (2015): 219-234.

[11] Yuan, Hong-Mei, et al. "A new image cryptosystem based on 2D hyper-chaotic system." Multimedia Tools and Applications (2016): 1-22.

[12] Zhang, Xuanping, et al. "A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution." Multimedia Tools and Applications 75.4 (2016): 1745-1763.

[13] Ginting, Riah Ukur, and Rocky Yefrenes Dillak. "Digital color image encryption using RC4 stream cipher and chaotic logistic map." Information Technology and Electrical Engineering (ICITEE), 2013 International Conference on. IEEE, 2013.

[14] Bansal, Ritesh, Shailender Gupta, and Gaurav Sharma. "An innovative image encryption scheme based on chaotic map and Vigenère scheme." Multimedia Tools and Applications (2016): 1-34.

[15] Li, Chunhu, et al. "An image encryption scheme based on chaotic tent map." Nonlinear Dynamics 87.1 (2017): 127-133.

[16] Hamdi, Mimoun, Rhouma Rhouma, and Safya Belghith. "A selective compression-encryption of images based on SPIHT coding and Chirikov Standard Map." Signal Processing 131 (2017): 514-526.

[17] Hamdi, Bouslehi, Seddik Hassen, and Ezzedine Ben Braiek. "Randomized poly-encryption image exploiting a new hyper-chaotic system." Advanced Technologies for Signal and Image Processing (ATSIP), 2016 2nd International Conference on. IEEE, 2016.

[18] Tang, Zhenjun, Xianquan Zhang, and Weiwei Lan. "Efficient image encryption with block shuffling and chaotic map." Multimedia tools and applications 74.15 (2015): 5429-5448.

[19] Liu, Ye, et al. "Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences." Multimedia Tools and Applications 75.8 (2016): 4363-4382.

[20] Khan, Majid, and Tariq Shah. "A literature review on image encryption techniques." 3D Research 5.4 (2014): 1-25.

[21] Xu, Lu, et al. "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion." Optics and Lasers in Engineering 91 (2017): 41-52.