Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Survey on Image Encryption, Data Hiding and Secret Fragment Visible Mosaic Image Creation Techniques

Nithya Susan Abraham[1], Priya Nair[2]
[1] *Computer Science and Engineering, Sree Buddha College of Engineering for Women, Elavumthitta, Pathanamthitta, Kerala, India,*
[2] *Computer Science and Engineering, Sree Buddha College of Engineering for Women, Elavumthitta, Pathanamthitta, Kerala, India,*

Abstract— So many skillful techniques are present for protection of confidential images from unauthorized access. Visual cryptography and data hiding are mainly used methods for secure transmission. But main problem of this method is that, during recovering stage exact image that send will not be retrieved. Small amount of distortion may occur. Some areas like medicine, military fields; small distortion of image may cause large problems. To avoid this, another secure method called secret fragment visible mosaic image is used. This paper surveys these three methods for secure image transmission. Advantage and disadvantages of these methods are pointed out. Comparisons are done to find out efficient technique that produces less distortion of image during recovery.

Keywords— image encryption; chaotic encryption; data hiding; reversible data hiding; secret fragment visible mosaic images

I. INTRODUCTION

Information transfer through internet is limited due to various attacks present in it. Areas like medical imaging, military, telemedicine etc. transfer different type of confidential images and data through internet. So it is very important to protect this type of images from different security problems. Two commonly used methods are data hiding and encryption, decryption method. Information hiding includes watermarking, anonymity and steganography. Here, data or images are securely hided inside an image so that no one can easily identify the presence other images or data. Image encryption and decryption method include conventional encryption and others such as chaotic encryption methods. Here, images are securely transfer by encrypting the whole image with a secret key. It is very difficult for an attacker to decrypt without the secret key. Due to some disadvantages of data hiding and encryption method, a new method called secret fragment visible mosaic images are developed. Mosaic image is a one type of art in which it is manufactured by generating small pieces of materials like stone, glass, tile etc. Based on this concept secret fragment visible mosaic image are created. Here, two images are present, one is secret image and other is target image in which secret image are securely hided. During the retrieving time, secret image can be obtained without any loss. In this paper, these three image protection methods are discussed.

II. IMAGE ENCRYPTION TECHNIQUE

Fast, reliable and robust, security systems is needed to store and transmit digital images used in the application like military image databases, medical imaging, confidential video conferencing, online personal photograph albums, cable TV, etc. [1]. Bulk data capacity, High Redundancy and high correlation among pixels, are the factors that differentiate Image Encryption from text Encryption. Because of the development in theory and application of chaos, now a day's many chaos algorithms have been proposed. Properties of chaotic systems are sensitively depend on initial conditions and system parameters, the density of the set of all periodic points and topological transitivity, etc. Most properties are related to requirements such as diffusion and mixing in the sense of cryptography. Therefore, chaotic cryptosystems has different useful and practical applications [2].

To improve the properties of confusion and diffusion in terms of discrete exponential chaotic maps, a paper called Image Encryption Approach Based on Chaotic Maps [2] is introduced. In this paper, it designs a key scheme for the resistance to statistic attack, grey code attack and differential attack. Since any chaotic output is based on floating-point analytical computation, the intruders can attack cryptosystems efficiently via certain basin structure. On the other hand, conventional methods called S-box transform can greatly increase the difficulty of attacks. Here, it first analyze the performance of discrete exponential chaotic map, then a permutation of the pixels of image is designed and the ‘‘XOR plus mod’’ operation is applied for the purpose of diffusion and resistance to differential attack. For resistance to entropy attack, statistic attack and grey code attack, two methods are used: one method is high precision algorithm and the other is perturbation to chaotic sequence. After that construct chaotic sequences which satisfy uniform distribution during the design of key scheme.

A novel algorithm for image encryption based on mixture of chaotic maps [3], focus on the chaotic digital encryption techniques. Symmetric key chaotic cryptography is used here. To enhance future security high-dimensional chaotic systems such as a coupled map are used. In this algorithm, a typical coupled map was mixed with a one-dimensional chaotic map and used for high degree security image encryption while its speed is acceptable. The cipher text generated and plaintext has same size. It is suitable for secure transmission of confidential information over the Internet. Here high-dimensional chaos is used as the basic structure of the cryptography, which leads to the following significant advantages of: due to the high-dimensionality and chaoticity, the output cipher text has long periodicity of computer realization of chaos, high complexity, and effective byte confusion and diffusion in many directions in the variable space. All these properties are helpful to achieve high practical security. This paper introduces the mixture mechanism of chaotic maps, which enhance the key space and security of algorithm. The proposed algorithm presented several interesting features, such as a high level of security, pixel distributing uniformity, large enough key space and an acceptable encryption speed. The high complexity of such chaotic dynamics indicates that they could be advantageously used in chaotic cryptographic techniques with enhanced security. Apparently, it can be easily used for any mixing of 1D chaotic map with 2D coupled chaotic maps. It seems that, the triple of such one dimensional maps may increase the security of crypto system in compared to the proposed cryptosystem.

Another paper called A Symmetric Chaos-Based Image Cipher with an Improved Bit-Level Permutation Strategy [4], a symmetric chaos- based image cipher with a 3D cat map-based on spatial bit-level permutation is used. Diffusion effect of this method is high because its bits are shuffled in different planes rather than within the same bit plane. Here, diffusion key stream is related to both plain image and secret key, which increases the security level. Due to the pixel value mixing effect, the number of iteration is reduced and cryptosystem performance increases. This type of chaotic system has complicated dynamical property and number of state variables. So it enhances more security. This method can resist all common attacks such as differential attacks, plaintext attack and brute force attack. Therefore it can be used for various online applications.

Now a day’s different encryption method are present and it is good in different areas. But the main disadvantage of encryption-decryption method is that, during the recovery stage original image is not recovered. Small changes in the image may cause large problems in some areas. And also, due to its randomness form causes the attackers attention [5].

III. DATA HIDING TECHNIQUE

Another method to solve disadvantage of encryption method is data hiding technique. It hides a secret message into a cover image so that no one can easily identify the presence of message. One of the main advantages of data hiding over cryptography is that it does not attract the attention of attackers themselves. Data hiding can be used in various areas like tamper proofing, ownership identification, data transmission etc. Mainly data hiding are classified as watermarking and image hiding. Watermarking is a method used to embed a distinguishable symbol into a host image to

authorize the ownership of the image. Image hiding is the method that embeds one image into the other image so that no one can easily identify the hided image easily.

Existing data hiding methods use different techniques. One of the common techniques used for data hiding is Image hiding by optimal LSB substitution and genetic algorithm [6]. In this method, data are embedding at the LSB position of the image. To increase security and obtain better embedding result an optimal LSB substitution and randomized embedding process along with data hiding by human perception model are used. To obtain optimal result, genetic algorithm is used along with it. Genetic algorithm is mainly used to solve the problem of hiding data in the rightmost k LSB bit and also to reduce the computation time when K bit is large. The main advantage of this method are: embedded data size can be large and the quality of data is not degraded very much during embedding process, data are embedded in randomized place so it appear meaningless to an attacker, due to the use of genetic algorithm embedding result become nearer to optimal and processing time is also reduced.

Another technique is hiding data in images by simple LSB substitution [7]. Advantage of simple LSB over optimal LSB is that the WMSE between the cover image and embedded image of optimal LSB is ½ that of obtained by the simple LSB. Computational cost is also low with respect to optimal LSB because optimal LSB requires huge computation cost for genetic algorithm to find an optimal substitution matrix.

In general, data hiding causes distortion in the host image. Such distortion may be very small but it is not acceptable to some application. To solve this problem, reversible data hiding method is used. Here, secret information is embedded in reversible manner so that original information can be perfectly recovered.

Different reversible data hiding techniques are present; one type is Reversible Data Embedding Using a Difference Expansion [8]. It is a reversible data embedding method in which high quality and high capacity are present. Here, first select an area for embedding and then embed payload and original value in that area. If the amount of information is larger than the embedding area, spaces saved from compression are used for payload embedding. This storage space is finding out by identifying the redundancy in the image content.

Another Reversible data hiding technique is, Reversible contrast mapping (RCM) [9] - is a simple integer transform which is applies to pairs of pixels. Even if the LSB is lost, some pair of the RCM can be invertible. Differential expansion method increases the complexity of watermarking but RCM does not need additional data compression and also its mathematical complexity is also very low.

One of the problems in data hiding method is that if the embedded data is larger than the image size then the information should be compressed and then embeds into it. This may causes distortion to the images.

IV. SECRET-FRAGMENT-VISIBLE MOSAIC IMAGE

Another new technique for secure image transmission is Secret-Fragment-Visible Mosaic Image [10], is a new type of image which is created automatically by composing small fragments of a given image to become a target image. Here secret image are divided into small fragments and they are embedded inside a target image visibly. Fragments are so tiny and random in position so that no one can easily identify the original image. The number of tile image depends on the size of the secret image. This is not in the case of traditional mosaic image, because tiles are not based on the secret image and also tiles can be repeatedly used. Information needed to recover original image are embedded into the mosaic image with a secret key and the method used is a lossless LSB scheme. Fast greedy search algorithm is used to find the similar target block to fit the secret tiled image.

One of the disadvantages of Secret-Fragment-Visible Mosaic Image [10] is the requirement of a large image database so that the generated mosaic image can be sufficiently similar to the selected target image. It takes a lot of time and also users are not free to select their own target image. By removing this weakness and keeping its merit, a new method called A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color

Transformations [5] is developed. It can transform a secret image into a secret- fragment-visible mosaic image of the same size that has the visual appearance of any freely selected target image without the need of a database. To make both images more similar, proper color transformation along with a scheme for handling overflow and underflow is used. Information needed to recover secret image are encrypted with a secret key and then embedded inside the mosaic image with the help of RCM method [9].

V. CONCLUSION

Now a day's secure transmission of information is very important. For that, different methods are used. In this paper mainly three type of secure image transmission method are surveyed. Three methods are encryption-decryption method, data hiding method and secret fragment visible mosaic image. First two methods have several advantages but its main drawback is that, during data retrieval time exact image or information is not created. Some distortion may occur and in some areas this small distortion may cause large problems. To solve this problem a new secure method called secret fragment visible mosaic image is created. It is a new technique in which it transforms a secret image into meaningful mosaic image with same size and looking like a preselected target image. The transformation process is controlled by a secret key and only with that key a person can recover the secret image from mosaic image. From the comparison, it is clear that Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations [5] is an efficient technique that produces less distortion of image during the recovery stage.

REFERENCES

[1] L. H. Zhang, X. F. Liao, and X. B. Wang, "An image encryption approach based on chaotic maps," Chaos Solit. Fract., vol. 24, no. 3, pp. 759–765, 2005.
[2] Jianjiang CUI1, Siyuan LI2 and Dingyu Xue3, "A Novel Color Image Cryptosystem Using Chaotic Cat and Chebyshev Map," IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 2, May 2013.
[3] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," Chaos Solit. Fract., vol. 35, no. 2, pp. 408–419, 2008.
[4] Chong Fu 1, Jun-Bin Huang 2, Ning-Ning Wang 1, Qi-Bin Hou 1 and Wei-Min Lei 1 ,"A Symmetric Chaos-Based Image Cipher with an Improved Bit-Level Permutation Strategy ," Entropy 2014, 16, 770-788; doi:10.3390/e16020770.
[5] Ya-Lin Lee, Wen-Hsiang Tsai, "A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations," IEEE transactions on circuits and systems for video technology, vol. 24, no. 4, april 2014.
[6] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," Pattern Recog., vol. 34, no. 3, pp. 671–683, 2001.
[7] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit.., vol. 37, pp. 469–474, Mar. 2004.
[8] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug2003.
[9] D. Coltuc and J.-M. Chassery, "Very fast watermarking by re- versible contrast mapping," IEEE Signal Process. Lett., vol. 14, no. 4, pp. 255–258,Apr.2007.
[10] I. J. Lai and W. H. Tsai, "Secret-fragment-visible mosaic image—A new computer art and its application to information hiding," IEEE Trans. Inf. Forens. Secur., vol. 6, no. 3, pp. 936–945, Sep. 2011.

