International Journal of Advanced Technology & Engineering Research (IJATER)
National Conference on Recent Trends in Science, Technology & Management (NCRTSTM-2018)

A REVIEW ON DIGITAL IMAGE ENCRYPTION TECHNIQUES

Amnesh Goel[1], Dr. Rakesh K Bhujade[2]
PhD Research Scholar[1], PhD Supervisor[2]
Department of Computer Science and Engineering, Mandsaur University, Mandsaur, MP 458001, India

Abstract

Images make an excessive contribution to conversation in this age of multimedia. When a user sends photographs through an unsecured data network, full privacy is a challenge to preserve the secrecy of images. Encryption is a way of protecting the security of images. In addition, this paper offers a brief guide to cryptography, including a detailed overview of the parameters of various elementary securities for image encryption algorithms. This thesis provides a study of different methods of image encryption and a comparison of distinct approaches to image encoding, eventually reveals a conclusion and proposes potential work. Protection is one of the most critical facets of computation. In the transmission of data, protection must be regarded as one of the approaches used to ensure the safe transfer of data. Data migration is the transfer of information from a location or host to another host or server. To provide a safe data transmission, few methods can be used, and one of them is data encryption, preparing it to be encrypted and decrypted before the data is to be used. In this section, we include literature reviews on the different techniques of image encryption.

Keywords: Image Encryption, Image security, pixel encryption, data loss etc.

1. Introduction

The Internet and information technologies are growing fast. Therefore, people use digital technology extensively in conversation. For illustration, picture, audio, and video. Images occupy a large fraction of the multimedia. Images play an important role in cooperation, for example, military, national security and diplomatic relations. Since these images which contain highly sensitive information, these images provide extreme security as users accumulate over an insecure archive. Furthermore, as people try to upload photographs over an unstable network, it becomes important to have total security. In short, a picture demands defense against a variety of security threats. The primary objective in protecting photographs is to uphold anonymity, honesty and authenticity [1]. There are various techniques available to keep photos safer, and one technique is encryption. Generally, Encryption is a technique that converts an image into a mysterious image using a key. In addition, the user can recover the original image by applying the decryption procedure to the cypher image [1], which is typically the reverse execution of the encryption operation. For example, Figure 1 represents the main image; the user performs the encryption technique and creates the hidden image; Figure 2 displays the encrypted image that is the result of the encoding process. In the other hand, when the recipient gets this secret image, the decryption process is applied, and the original information is retrieved. Figure 3 shows the recovered file.

Figure 1: Plain image

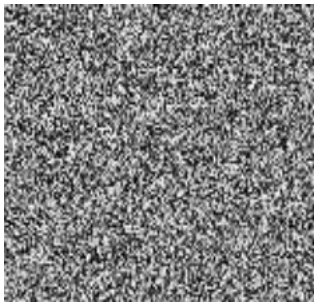

Figure 2: Encrypted Image

Figure 3: Decrypted image

With the rapid advancement of new networking methods, both information management and the defense of intellectual property are of considerable importance. This lead to a comprehensive analysis of data encryption, digital signature, authentication and watermarking methods [2]. Optical encryption techniques have drawn considerable interest as they provide the possibility of high-speed parallel processing of 2D image data, of hiding information in several different dimensions, i.e., several degrees of freedom [3]. One critical optical encryption scheme, called 'Double Random Phase Encoding (DRPE),' involves multiplying the image by random phase diffusers (masks) in both the input (space) and Fourier (space frequency) domains [4]. The encrypted picture can be seen to be a stationary white noise if the two random phases are statistically distinct white noise. Digital holography [5] offers a simple way to capture complicated encrypted images after going through optical DRPE networks. The second random step diffuser found in the Fourier domain is the secret to this encryption scheme. Following the implementation of this technique, a variety of other optical-inspired encryption approaches have been introduced in the literature, including digital optical stream cipher[6], optical XOR image encryption [7], phase-shifting interferometry [8], polarization encoding [9] and information security authentication techniques involving mutual transformation correlations [10]. The theoretical and experimental findings published suggest that the level of safety of optical encryption systems can be greatly enhanced by such approaches.

2. Literature Review

Here is the review of few image encryption algorithms that were proposed lately.

The DRPE approach has opened new areas of study in optical image and signal processing and has been the subject of several studies. There have been several variations of this method including extra degrees of freedom. The fractional Fourier Transform (FRT) and Fresnel Transform (FST) have been used in encryption algorithms and systems that implement fractional order and spread distance and function as additional keys. It has been suggested that these extra keys may boost the reliability of the optical encryption method as they create additional difficulties for system attackers. Since the Fourier transform (FT), the fractional Fourier transform (FRT) and the Fresnel transform (FST) are all special cases of linear canonical transformation (LCT), the use of the LCT has also been proposed for optical encryption techniques using a quadratic phase scheme (QPS).

In this case, the QPS transformation parameters include additional keys for the encryption scheme. The Gyrator Transform (GT), which also belongs to the linear canonical transformation class, has been used for optical encryption schemes where the rotation angle parameter gives an extra key to the encryption method. Hartley transform (HT), which is essentially a true Fourier transformation without any phase details, has also been proposed for use in optical DRPE systems. In addition, the DRPE has been investigated for use in multi-image encryption and colour image encryption. Image scrambling methods, which can be interpreted as a computer-based numerical pre-processing method, have also been used in combination with the DRPE system using Jigsaw transform (JT) and Arnold transform (ART). Recently, the computational ghost imaging technique has been suggested for encrypting and distributing information, where the encrypted image tends to be an intensity vector instead of a complex matrix in the traditional DRPE method. Another alternative form of optical imaging, i.e., diffractive imaging, has also been developed in optical encryption.

It requires the use of an iterative step extraction algorithm to decrypt the original image from the reported diffraction patterns. In addition, two-dimensional optical encryption processing has been generalized to three-dimensional space-based encryption processing, where each pixel of the image is axially perceived to be a single particle and the phase-shifting digital holography technique is applied to the diffraction of all pixels in space (particles). In the field of cryptography and cryptoanalysis, both the chosen-plaintext and the known-plaintext attacks on DRPE have been studied, as have many other attacking techniques, and the key space of the DRPE strategy itself has also been analyzed.

In this image encryption article, Long Bao and Yicong Zhou[11] proposed a new chaotic scheme that would make up three distinct one-dimensional chaotic maps. The proposed strategy uses the Logistic Map as a controller to choose a Tent Map or a Sine Map to produce random sequences. Subsequently, the imparted algorithm

uses the substitution-permutation network (SPN) structure to achieve the uncertainty and diffusion properties. This scheme uses a 240-bit key for broad key space. Mainly, this key includes all the configurations of the parameters and the original values of the current chaotic scheme, and the unnecessary vulnerability of key modifications to encryption and decryption. As a result, the proposed solution offers excellent protection against brute force attacks, as well as excessive key sensitivity and chaotic behavior.

In this picture encryption article, Saraswati D. Joshi, Dr. V.R. Udupi and Dr. D.R. Joshi[12] have put forward a technique that scans an image pixel by pixel. Subsequently, the transformation takes place on these pixels using substitution and permutation. In addition, the encoding process inserts the impurity of the converted image into a garble. This device uses two layers of encryption to achieve high-performance authentication. In addition, the imparted scheme uses the Artificial Neural Network to decode the cypher signal. The decryption process requires three steps. The method removes the added impurity at the first level. And, in the second step, the network discards the extra conjoined columns in the matrix. In addition, in the third step, the image data obtained, and the weights processed after training are used to stimulate the network. The dominance of this approach is due to the use of random coding on the sender side which prevents a key exchange. The proposed methodology therefore offers a high degree of protection. The downside is that the decryption process takes longer.

In this research article, the authors [13] proposed a picture encryption strategy based on the modified zigzag transformation. This is a 3-step process imaging technique. In the first step, the image is divided into 64 blocks. In the second step, the modified zigzag transformation is carried out. In the same step, to complicate the zigzag transformation, the authors proposed moving the first and second pixels to the second third and last positions in the image, and this is where the authors called it a tweaked zigzag transformation. In the last step, to get an image of the cypher, the XOR operation was performed on the RGB aircraft. In this case, the writers proposed using a 256-bit token, but did not explain the key details and how they were used in the encryption process. Subsequently, the writers encrypted four different images. The authors provided the histogram analysis along with the key sensitivity analysis to confirm their results. The initial key has been marginally changed and the results seen in the paper confirm that the clear image has not been returned to them. Correlation analysis is also explored in this article, which reveals that there is no correlation between adjacent pixels. A few other distinct types of research techniques are used in this article to support their findings. The authors should have specified the key information that is very necessary for any encryption process.

In this article, authors [14] proposed an image encryption algorithm that used Arnold Cat Map with Visual Cryptography to encrypt pictures. In the first stage of this encryption method, the authors separated the RGB image into three layers of Red, Green and Blue. The pixels of these Red, Green and Blue layers are then shuffled using the Arnold Cat Map for ten iterations. In the second step, the authors have created shares. Share 1 is generated randomly by the combination of RandR, RandG, and RandB. Share 2 is created by the addition of share 1. Share 3 is created by copying the odd rows of Share 1 and even the rows of Share 2 to Share 3R, 3G and 3B. In the final step, XOR is performed between the image obtained after the application of the Arnold Cat Map and the 3rd level of the share. In the end, the authors presented experimental findings showing that the PSNR of two related images is 7.63 and 7.69. Correlation analysis of two neighboring pixels was done and the value was close to 0. Histogram review reveals that the encrypted image histogram is flatter than the original image histograms. The overall quality of this paper is fine. However, the writers did not discuss the key specifics in this article.

In this article, the authors [15] explored a new approach to encrypting images using the GSVD (Generalized Singular Value Decomposition) technique, which decomposes the plain image into two parts. These two segments are then combined with an exchanged key-image to create a cypher image. In the beginning, an initial "c" key is used to produce the two matrices from the plain image. These two matrixes are then combined individually with the main image, which is then combined to produce the cypher image. This concept usually involves a key image of the same size of the matrices, and because the authors have suggested dividing the plain image into two bits, it is more difficult to hold the key to various sizes. Authors believe that this encryption scheme is very stable since there are an unlimited number of options for identifying the encryption key. With the aid of the Histogram analysis, the authors presented the data, presenting the red, green, and blue histograms of the plain image and the image they received after decryption. Results demonstrate that there is no lack of knowledge during the encryption process.

In this paper, authors [16] suggested a new image encryption algorithm that used 2 key vector methods to transfer the row and column level pixels from their location, and then ZETA was used to enter the cypher image. This is a hybrid encryption paradigm where the Rubiks Cube Theory and the ZETA function are used

together to reach a fast picture encryption approach that can be conveniently used on cell phones because of its less computational need. To initiate the encryption process, authors have generated separate keys (KR, KC) for rows and columns. These keys are in the range of 1 to 2 (n-1). Ses two keys can be used to scramble the pixels at row level and column level, respectively. The key size is not adequately addressed, but the number of rows and column shifts would depend on the key size. In addition to the ZETA function, the 1x256 row vector is determined using the sum of all row elements and the Modulo-2 of this sum is calculated to get the binary numbers. All 0 positions are used for the right circular shift and all 1s are used for the left circular shift. This is the same technique used to execute operations at the level of the column. Authors claim to run Pixel Change Rate Number (NPCR) and Unified Average Change Intensity (UACI) tests to ensure the accuracy of the encrypted file but did not address these approaches in depth. The authors further addressed the Main Sensitivity Analysis, and the related findings were applied to the article.

Authors [17] have come up with two separate encryption schemes in this article. In the first encryption scheme, the image is first separated into NxN blocks and then each block is converted into a 1D sequence using the ZigZag pattern before encrypting. Exclusive or XOR operation is done on this 1D array in a hidden key mix. Whereas, on the other hand, in the 2nd encryption scheme, the NxN size image block is first encrypted using the hidden key, then this block is XOR with the next block, and this pattern continues with all the blocks in the image. This method is called cypher block chaining (CBC) in which block encryption relies not only on the key, but also on the previous block. Histogram analysis is then conducted on a plain image vs cypher image and it has been observed that the histogram of the cypher image pixels is uniform and slightly different from the plain image histogram. Authors conducted a correlation study in which they find that the correlation between the cypher images pixels is much smaller than the plain image pixels that are strongly correlated. Authors did a Sensitivity Analysis in which they adjusted the pixel value in the plain image to see if the outcomes will be different, but I assume the Sensitivity Analysis is performed with respect to the key that the encryption process uses, not the plain image itself. In this article, the writers did not address the key specifics at a satisfactory stage, nor did they discuss the objective of maintaining two encryption schemes. Also, the authors did not discuss how the XOR operation is done or how it operates on a plain image pixel.

Authors [18] introduced a new colour picture encryption algorithm that uses chaotic map and spatial bit-level permutation (SBLP).First, use the Logistic Chaotic Series to change the location of the image pixels, then convert it into a binary matrix, and permute the bit-level matrix by scrambling the SBLP-generated mapping. Using another Logistic chaotic sequence to change the location of the current image pixels. Experimental findings show that the proposed algorithm can provide strong encryption results and low time complexity, making it ideal for securing video monitoring networks, multimedia devices and real-time applications such as cell phone services.

Authors suggested a new encryption scheme [19] to change the AES algorithm based on all ShiftRow Transformations. In this case, if the value in the first row and the first column is even, the first and fourth rows remain unchanged, and each byte in the second and third rows of the state is cyclically shifted right over the different number, otherwise the first and third rows remain unchanged, and each byte in the second and fourth rows of the state is cyclically shifted left over the different number of bytes. The experimental result reveals that MAES provides improved encryption results in terms of protection against statistical attacks and enhanced speed.

3. Conclusion

In this article, all the relevant encryption methods have been presented and reviewed to familiarize yourself with the different encryption algorithms used to encrypt the picture that has been transmitted across the network. The results of the simulation demonstrate that every algorithm has advantages and drawbacks depending on the techniques applied to the images. Based on a detailed analysis of all the research papers referred to above, the following recommendations can be made: The Chaos-based algorithm should be applied to secure multimedia content. More sophisticated and compressed algorithms can be used to provide the device with high speed and security. The modified version of different algorithms is used to increase the level of protection.

References

[1] William Stallings, Cryptography and Network Security, Principles and Practice. Fifth edition.
[2] Javidi B. Optical and digital techniques for information security. New York: Springer; 2005.
[3] Matoba O, Nomura T, Perez-Cabre E, Millan M, Javidi B. Optical techniques for information security. Proceedings of IEEE 2009;97(6):1128–48.

[4] Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. Optics Letters 1995;20(7):767–9.
[5] Javidi B, Nomura T. Securing information by use of digital holography. Optics Letters 2000;25(1):28–30.
[6] Madjarova M, Kakuta M, Yamaguchi M, Ohyama N. Optical implementation of the stream cipher based on the irreversible cellular automata algorithm.
Optics Letters 1997;22(21):1624–6.
[7] Han J-W, Park C-S, Ryu D-H, Kim E-S. Optical image encryption based on xor operations. Optical Engineering 1999;38(1):47–54.
[8] Tajahuerce E, Matoba O, Verrall SC, Javidi B. Optoelectronic information encryption with phase-shifting interferometry. Applied Optics 2000;39
(14):2313–20.
[9] Matoba O, Javidi B. Secure holographic memory by double-random polarization encryption. Applied Optics 2004;43(14):2915–9.
[10] Javidi B, Sergent A. Fully phase encoded key and biometrics for security verification. Optical Engineering 1997;36(3):935–42.
[11] Long Bao, Yicong Zhou, C. L. Philip Chen, Hongli Liu "A New Chaotic System for Image Encryption" 2012 International Conference on System Science and Engineering, June 30-July 2, 2012, pages: 69-73.
[12] Saraswati D. Joshi, Dr. V.R. Udupi, Dr. D.R. Joshi, "A Novel Neural Network Approach for Digital Image Data Encryption/Decryption", Power, Signals, Controls and Computation (EPSCICON), 2012 International Conference on 3-6 Jan. 2012, pages: 1-4.
[13] Priya Ramasamy, Vidhyapriya Ranganathan, Seifedine Kadry, Robertas Damaševi˘cius, and Tomas Blažauskas, An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent Map, Entropy 2019, 21, 656; doi:10.3390/e21070656.
[14] Reem Ibrahim Hasan, Huda Adil Abdulghafoor, "Cipher Secret Image Using Hybrid Visual Cryptography" ARPN Journal of Engineering and Applied Sciences, VOL. 13, NO. 3, FEBRUARY 2018 ISSN 1819-6608.
[15] Mohammed Abdul, Hayder Raheem Hashim, Ameer Mohammed Hussein, Hind Rustum Mohammed, "An Algorithm Based on GSVD for Image Encryption" Math. Comput. Appl. 2017, 22, 28; doi: 10.3390/mca22020028.
[16] Zaheer Abbas Balouch, Muhammad Imran Aslam, Irfan Ahmed, "Energy Efficient Image Encryption Algorithm" 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT).
[17] Omar Reyad, M. A. Mofaddel, W. M. Abd-Elhafiez, Mohamed Fathy, "A Novel Image Encryption Scheme Based on Different Block Sizes for Grayscale and Color Images", 12th International Conference on Computer Engineering and Systems (ICCES) 2017.
[18] .R. liu, X. tian "New algorithm for color image encryption using chaotic map and spatial bit level permutation "Journal of Theoretical and Applied Information Technology 15 September 2012. Vol. 43 No.1 © 2005 - 2012 JATIT & LLS.
[19] S.H. Kamali, R. Shakerian "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption" 2010 International Conference on Electronics and Information Engineering (ICEIE 2010).