International Journal of Research in Engineering, Science and Management
Volume-2, Issue-7, July-2019
www.ijresm.com | ISSN (Online): 2581-5792

A Survey on Image Encryption Techniques

N. Prathipa[1], V. Sathya[2]
[1]*PG Scholar, Dept. of Computer Science & Engineering, A.V.C. College of Engineering, Mayiladuthurai, India*
[2]*Assistant Professor, Dept. of Computer Science & Engg., A.V.C. College of Engineering, Mayiladuthurai, India*

***Abstract*: The primary goal of this paper is security management. This will provide authentication of users, and integrity, accuracy and safety of images which is traveling over the internet. Moreover, an image based data requires more effort during encryption and decryption. The intension of encrypting the images is to make images more secure. This paper presents a survey of over ten analysis papers dealing with image encryption techniques scrambled the pixels of the image and reduce the correlation among the pixels. During this paper a survey of various image encryption techniques that are existing is given. In addition, focuses on the practically of image encryption and decryption techniques. It adds a further layer to encryption. Chaos based image encryption technique using method of shuffled operations. It demonstrates a simple, secure and compact technique to cipher and decipher a color image.**

***Keywords*: Accuracy, Chaos Technique, Image Encryption, Integrity, Security.**

1. Introduction

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones. From the study of research paper, this paper concludes that there are no clarifications which type of images they are using to perform image encryption and decryption procedure. I have also analyzed that there is no clarification about the configuration of machine and platform where all the experiment are calculating. Another thing which have measured that proposed transformation table of having very complex structure and not easy to understand which is the cause of poor efficiency. From further study the observation have been done that images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the Characteristic of human perception, a decrypted image containing small distortion is usually acceptable. After the detailed study of image encryption, we presented some problem which find during study and how we can remove these with the help of our proposed work. This paper is divided in to four sections. Section – I basic introduction about image encryption and problem formulation, section-II detailed description of proposed work, section-III experiment and results comparison and section-IV conclusion and future enhancement.

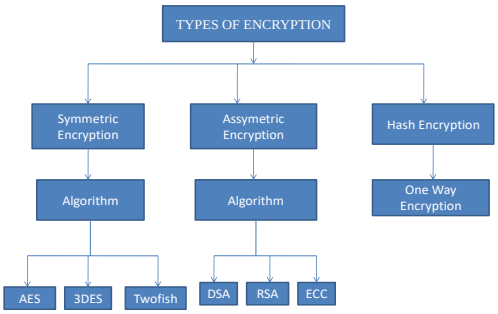

Fig. 1. Types of Encryption

2. Literature survey

A. Double image encryption based on random phase encoding in the fractional Fourier domain

Ran Tao, Yi Xin, and Yue Wang (2007) proposed that a novel image encryption method is proposed by utilizing random phase encoding in the fractional Fourier domain to encrypt two images into one encrypted image with stationary white distribution. By applying the correct keys which consist of the fractional orders, the random phase masks and the pixel scrambling operator, the two primary images can be recovered without cross-talk. The decryption process is robust against the loss of data. The phase-based image with a larger key space is more sensitive to keys and disturbances than the amplitude-based image. The pixel scrambling operation improves the quality of the decrypted image when noise perturbation occurs. The novel approach is verified by simulations.

B. An enhanced image encryption scheme using 16-byte key

Shradha Suryawanshi, Pankaj Kumar Sahu (2015) proposed that Now-a-days, security and privacy has become one of the primary issues in data storage and transmission. In the age of images are widely used in business, advertising and promotions. The protection of images from unauthorized access

is important. Image encryption plays a significant role in the field of information hiding. In this article, we introduce a chaos based image encryption technique using method of shuffled operations. This technique uses 128-bit private key for encryption. Performance of proposed image encryption scheme is compared with the existing inter pixel displacement image encryption scheme. Performance evaluation reveals that proposed scheme performs better than existing scheme in terms of entropy of encrypted image.

C. Optical encryption of gray image based on the Fourier computer generated hologram and logical modulation

Ying Wang, Qi Liu, Qiong-Hua Wang (2016) proposed that a novel optical encryption and decryption method of gray image based on the Fourier Computer-Generated Hologram (CGH) and logical modulation. Since the encryption method using the CGH or the logical modulation alone has a shortness of low security. In our encryption processing, the hologram which is gotten by Fourier transform from the original image is encrypted by logical modulation with the chaotic sequence. Simulation results and analysis show that the security and robustness of the proposed approach has a satisfactory performance.

D. Novel image encryption technique using RGB pixel displacement for color images

Shrija Somara, Mohammed Ali Hussain (2016) proposed that in the present scenario when all data is in network, cloud or some data center, security and protection of data is a major concern. Encryption is one of the techniques used for this purpose. Image encryption is applied for protecting images from different kinds of attacks. Image Encryption is possible by a kind of transposition in color images or 3D images by displacing the RGB components of the color image. This paper presents a method for encryption and decryption of Color images using RGB pixel displacement. In the proposed method the original plain image is split into its basic three components, that is the RGB components and the key image is also split into RGB Components. Further by application of XOR operation and scrambling of the three components the cipher image is generated. This method is suitable for encrypting 3D images. The algorithm is implemented in MATLAB environment and tested on various color images.

E. The color image encryption technology based on DNA encoding & sine chaos

Buhalqam Awdun, Guodong Li (2017) proposed with the increasingly fierce competition among countries, the confidential work has become an important field of a country, and the image confidentiality and deciphering is one of them. If confidential work is not done well, it would easily lead to unexpected security and economic losses. Here we research the encryption algorithm of color images by combining the DNA encoding and sine chaotic mapping to encrypt the color images. Experimental results show that the speed of encryption and decryption is greatly improved because of the advantage of parallel computation; it can against a series of attacks safely and efficiently, because the algorithm has large key space, strong attack resistance, reversible encryption methods and it also sensitive to initial value. Therefore, this method is extremely suitable for the fields which collect a large amount of image data. And it also has great potential applications in the military, medicine and other image secure communication fields.

F. Towards the growth of optical security systems for image encryption by polarized light

Wiam Zamrani, Esmail Ahouzi, Angel Lizana, Juan Campus and Maria Josefa Yzuel (2016) proposed that Motivated by recent interest in polarization encoding, we present an image encryption or decryption scheme based on polarized light which provides additional flexibility in key encryption designs, and double random phase masks. In this scheme, the primary image is encrypted relying on stokes-Mueller formalism by using two Spatial Light Modulators (SLMs). With the proposed method it is possible to control the polarization ellipse parameters and the rotation angles of the SLMs. Numerical simulation is performed for gray-scale images to demonstrate the validity of this new proposed method. The performance measurement parameters mean-square-error and Peak-signal-to-noise ratio have been calculated to verify the feasibility of the schema.

G. A novel method for encryption of images based on displacement of RGB pixels

Boddu Ramya Sri and Shrija Madhu (2017) proposed that in today's world, security of information has become a crucial part of every aspect of human-life, when data is transferred through internet. Due to the transmission of information through network, unauthorized access is possible. Image Encryption is one of the techniques to protect the images over the internet. This can be possible by displacement of RGB pixels of an image. Encryption can prevent a third party from understanding the data during the transmission. This paper sets out to contribute to the general body of knowledge in the area of cryptography application and by developing a RD algorithm for image encryption by shifting the RGB pixel values. The algorithm ultimately makes it possible for encryption and decryption of the images based on the RGB pixel. The algorithm was implemented using JAVA.

H. Image Encryption based on quantum-CNN hyper-chaos system and anamorphic fractional fourier transform

Jinqing Li1 et al. (2017) proposed that to solve the insufficient of nonlinearity in optical cryptosystems, a new scheme is proposed for optical image encryption based on Quantum Cellular Neural Network(QCNN) hyperchaotic system and Anamorphic Fractional Fourier Transform(AFrFT). The first and the second Chaos Random Phase Masks (CRPM) are generated by QCNN hyperchaotic system. The original image is combined with the first CRPM and then transformed

by AFrFT. The encrypted image is obtained by the second CRPM and the second AFrFT. Experimental simulation results show the feasibility, high security and efficiency of our scheme.

I. Optical image encryption using radon transform

A. Ritika, Y. Xiong2, and C. Quan (2017) proposed that the need to secure data and information has been increasing to prevent the unauthorized usage. Important data needs to be secured efficiently to protect it from the various security threats and attacks. The optical image encryption techniques have distinct advantage of processing complex two-dimensional information in parallel with high-speed. The optical systems with its multidimensional capabilities possess many unique characteristics such as securing information with various degrees of freedom. In this paper, we have proposed a novel optical image encryption algorithm using Radon Transform in the optical domain. Radon Transform is a mechanism which is used to express the projections of the image. It can be used in the optical encryption systems to enhance their security by increasing the security parameters of the system. It adds an additional

Table 1
Literature survey

S. No.	Title of the paper	Author	Algorithm/Technique	Advantage	Disadvantage
1	Double image encryption based on random phase encoding in the fractional Fourier domain.	Ran Tao et al. (2007).	Single image encryption algorithm.	The effects of noise perturbations on the encrypted data are also studied.	The novel approach does not have a symmetrical response on the two decrypted images when noise perturbation. .
2	An Enhanced Image Encryption Scheme using 16 Byte Key.	Shradha Suryawanshi, Pankaj Kumar Sahu (2015).	Cryptographic algorithm.	Image encryption ensures protection of images from unauthorized access.	The position of data is scrambled and easily retrieved according to randomness of elements obtained from chaotic map.
3	Optical Encryption of Gray Image Based on the Fourier Computer Generated Hologram and Logical Modulation.	YingWang et al.(2016).	Symmetric algorithm.	The encryption method based on chaotic system has some good properties in many aspects such as security, complexity, computation speed.	Even if the initial value is changed with a small deviation the information in the original image cannot be recognized from the decrypted image.
4	A Novel Image Encryption Technique using RGB pixel displacement for Color Images.	Shrija Somara, Mohammed Ali Hussain (2016).	Novel image encryption technique.	Image Encryption based on symmetric as well as asymmetric methods have been developed.	The statistical analysis of the original and encrypted images so brute force and other common types of attacks will not yield anything to the attacker.
5	The Color Image Encryption Technology Based on DNA Encoding & Sine Chaos.	Buhalqam Awdun, GuodongLi (2016).	Optical image encryption technique.	The method of solving image security problem is based on the theory of chaos.	It is impossible to regenerate, so it cannot achieve the purpose of real decryption; the chaotic signal is very sensitive to the system parameters and the initial value, and difficult to analyze, reconstruct and forecast.
6	Towards The Growth of Optical Security Systems for Image Encryption by Polarized Light.	Wiam Zamrani, et al.(2016).	(DPRE) Double Random Phase Encoding encryption technique.	Optical image encryption based on polarization of light has a great deal of attention recently, because polarization provides additional flexibility in the design of encryption keys.	The decryption is not possible if we use the wrong keys in the decryption stage.
7	A Novel Method for Encryption of Images based on Displacement of RGB Pixels.	Boddu Ramya Sri and Shrija Madhu (2017).	RD algorithm.	Image encryption technique should be designed to augment the effectiveness of the transmission and it should be protected from susceptible attacks by the illicit access.	In this approach the numerical values of an image is rearranged and displaced and finally they swapped with RGB values to get encrypted image.
8	Image Encryption based on Quantum-CNN Hyper-chaos System and Anamorphic Fractional Fourier Transform	Jinqing Li et al.(2017)	Optical image encryption technique.	In order to decrease the overload of image transmission on network, the double-image encryption by using the optical transform and chaos theory has been proposed the color image	QCNN not only have greater key space than low-dimensional chaotic system
9	Optical Image Encryption Using Radon Transform.	A. Ritika et al. (2017).	Optical image encryption technique.	The technique is reliable and can be used for secure optical communication.	To develop a cryptosystem that can be attacked easily.
10	DRPE Encryption with Chaotic Interleaving for Video Communication.	Eman et al. (2017).	Double Random Phase Encoding encryption technique.	Low-cost, simple platforms for real-time video will become essential in our daily communication and will be dominant.	The common encryption methods are not able to cope with the real-time transmission requirements.

security layer to the images and makes the encryption system difficult to be attacked. The technique is robust and can be used to transmit data securely. Simulation results are presented to validate the proposed idea. Reliability of the technique has been established by evaluating the Mean-Square Error (MSE) and Correlation Coefficient (CC) values between the decrypted and the original images.

J. DRPE encryption with chaotic interleaving for video communication

Eman M. El-Bakary El-Sayed M. El-Rabaie (2017) proposed that the need to transmit encrypted data and video securely through wireless channels, we suggest the application of the Double Random Phase Encryption (DRPE) algorithm for efficient video communication over Orthogonal Frequency Division Multiplexing (OFDM) system. Moreover, we use an efficient interleaving mechanism on the communicated data depending on chaotic Baker map to control the error level of the channel. In this paper, DRPE and chaotic Baker interleaving are used for efficient video frame transmission over OFDM. Channel equalization is implemented in the proposed scheme. Simulation results illustrate the good performance of the suggested scheme for secure video communication.

3. Proposed work

In today's world, image plays a vital role in all media secret images are transferred over the network. So, images are transferred over the network in unsecured manner. There are different encryption technique are available to provide security for these images. In this work, survey had been done in different existing image encryption techniques and these techniques are discussed in Table 1. In these technique chaos based image encryption is an efficient one because the time consumption is very less when compared to other techniques.

4. Conclusion

This internet world nowadays, the security of images is very important. This paper surveyed different image encryption techniques in the span of 10 years (2007-2017). The security for the digital images has become highly important since the communication by transmitting of digital products over the open network occur very frequently. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security. From the above review provides combined approaches of cryptography and data hiding for protection of an image. In all methods the original image and information is embedded and encrypted and then send the message to the receiver. It has found problem related to slow transfer of message and noise during embedding and to resolve this problem compression and segmentation is used but compression technique were not reversible, erasable, invertible and segmentation uses large data to embed with information and original image but due to large data the transmission takes more time.

5. Future enhancement

Hence Security is the major concern for any system to maintain the integrity, confidentiality and image authenticity. Although the cryptography is the effective method but it also face the problem in providing the security if the data in the image is more. Based on the survey of different encryption techniques it can be identified that the chaos based cryptosystem is very suitable for image encryption because of lower time consumption compared to AES (Advanced Encryption Standard) and DES (Digital Encryption Standard). In future we are going to develop a new image encryption technique based on chaos.

References

[1] L. Xinyu and Y. Wang, ``Optical encryptions and decryptions based on all-optical shift register," in Proc. IEEE Int. Conf. Opt. Commun. Netw. (ICOCN), Aug. 2017, pp. 1-3.
[2] A. Ritika, Y. Xiong, and C. Quan, ``Optical image encryption using radon transform," in Proc. IEEE Prog. Electromagn. Res. Symp.-Fall (PIERS-FALL), 2017, pp. 1235-1238.
[3] W. Zamrani, E. Ahouzi, A. Lizana, J. Campus, and M. J. Yzuel, ``Towards the growth of optical security systems for image encryption by polarized light," in Proc. IEEE Int. Conf. Comput. Syst. Appl. (AICCSA), Nov./Dec. 2016, pp. 1-6.
[4] Z. Liu, S. Li, W. Liu, Y.Wang, and S. Liu, ``Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding," Opt. Lasers Eng., vol. 51, no. 1, pp. 8_14, Jan. 2013.
[5] S. Narendra and A. Sinha, ``Optical image encryption using fractional Fourier transform and chaos," Opt. Lasers Eng., vol. 46, no. 2, pp. 117-123, 2008.
[6] Z. Nanrun and T. Dong, ``Optical image encryption scheme based on multiple-parameter random fractional Fourier transform," in Proc. IEEE Int. Symp. Electron. Commerce Secur. (ISECS), vol. 2, 2009, pp. 48-51.
[7] J. Li, X. Di, X. Liu, and X. Chen, ``Image encryption based on quantum-CNN hyperchaos system and anamorphic fractional Fourier transform," in Proc. IEEE Int. Conf. Image Signal Process., Biomed. Eng. Inform. (CISP-BMEI), Oct. 2017, pp. 1-6.
[8] R. Hui, J. Wang, and Q. Wang, ``Optical encryption of gray image based on the computer-generated hologram and logical modulation," in Proc. IEEE Int. Conf. Opt. Photon. Eng. (ICOPEN), Oct. 2017, pp. 1-6.
[9] S. Shrija and M. A. Hussain, ``A novel image encryption technique using RGB pixel displacement for color images," in Proc. IEEE Int. Conf. Adv. Comput. (IACC), Feb. 2016, pp. 275-279.
[10] H. Chen, X. Du, Z. Liu, and C. Yang, ``Color image encryption based on the af_ne transform and gyrator transform," Opt. Lasers Eng., vol. 51, no. 6, pp. 768-775, 2013.
[11] 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), International Conference on. IEEE, 2013.
[12] Khan, Majid, and Tariq Shah. "A literature review on image encryption techniques." 3D Research 5.4 (2014): 1-25.
[13] 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.