NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 4, ISSUE 2, Feb.-2017

A SURVEY ON IMAGE ENCRYPTION SCHEMES

PUNITA KUMARI
Department of computer science and engineering, College of Technology and Engineering, Maharana Pratap University of Agriculture and Technology, Udaipur, India. punitakumari13@gmail.com

KALPANA JAIN
Department of computer science and engineering, College of Technology and Engineering, Maharana Pratap University of Agriculture and Technology, Udaipur, India. kalpana_jain2@rediffmail.com

ABSTRACT
Now a day's, with the rapid increasing growth of internet and multimedia data, security is the main problem in storage and communication of images which can be solved by using different encryption and decryption techniques. With the growing multimedia and communication, encryption of text, images, audio, video etc is most important during transmission of the information securely. Apart from the encryption of data, there are various image encryption techniques which have been proposed for the security of image and confidential data from an unauthorized access over the network useful for military, government and medical applications. In this paper, a survey on different image encryption and decryption techniques has been presented. The main focus have been given on different types of image encryption and decryption schemes along with its merits and demerits so that the best secure process can be adopted for practical applications.

KEYWORDS: Cryptography, Image encryption, Diffusion, Confusion, Security measures.

INTRODUCTION

The communication system plays an important role in multimedia technology. Communication is the process in which data is transmitted from one location to another different location. During the communication process, the main and important issue arises is the security problem. Internet is one of the most useful and versatile communication media which is used for information exchange in terms of digital images, text, video, audio etc. This can also be used for storing the data in an open network in which unauthorized users can retrieve important data and information and therefore cryptography can be used to prevent it. For long time cryptography plays an important role in the field of security and is a battleground for scientists and mathematicians, starting from Shannon [1]. Several cryptographic algorithms have been proposed so far e.g. AES, DES, RSA, IDEA etc [2-4]. Cryptography is the art and science of securing the data. It is the art of converting the data into its coded form and then again decoding it into its original form. Cryptography enables in storing sensitive information and then transmitting it across the networks like the Internet so that it cannot be read or accessed by anyone except the authorized person.

Today digital image plays a crucial role in communication and multimedia technology. It becomes more important for the user's to maintain its privacy and security. Since, images can be considered one of the most useful and essential form of information, therefore privacy and security to the user for image encryption is a very important aspect to protect it from any unauthorised user. Encryptions like image, text, audio, video etc have their own uses in numerous fields such as multimedia systems, internet communication, medical imaging, Tele-medicine, military communication etc. Images are transmitted and stored in huge amount over the Internet and wireless networks due to rapid growth in multimedia and network technologies. Image encryption algorithm is different from the data encryption algorithm because of the large size of digital images and data redundancy. There are various security problems that are associated with digital image processing and its transmission. Therefore, it is important to maintain the integrity and the confidentiality of the image**.** Figure 1 shows a general image encryption scheme using image encryption algorithm and its resultant encrypted image.

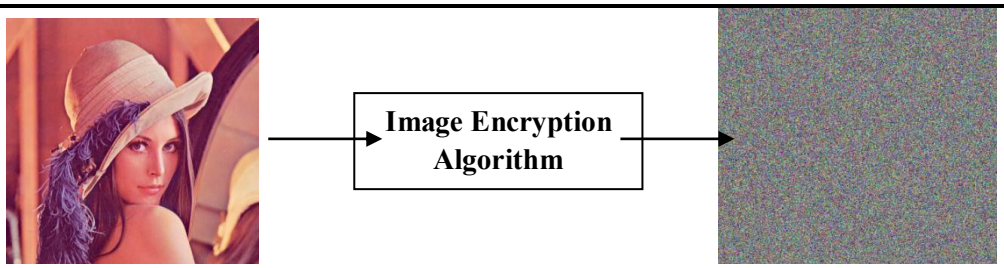

Figure 1: Image Encryption process.

In this paper, we presented literature survey on different existing techniques. In Section 4, security analysis of the image encryption techniques will be discussed in terms of statistical analysis, key sensitivity analysis, entropy etc. These parameters are essential to prove the security against the most common attacks. Finally in the Section 5, we concluded the proposed paper.

ENCRYPTION PROCESS

In real time applications, several image encryption and decryption techniques are used for secure and safe transmission of image over the internet and through wireless networks. Different image processing techniques like cryptography, stenography, watermarking etc can be used in the encryption and decryption of the images. Image encryption algorithm is used to process the original image into an encrypted image so as to keep the original image secure and confidential among different users. In other words, it is important and necessary that no-one could be able to get the content and information of the image without a key for the decryption process. Encryption is the process of encrypting the plain text data into its cipher text i.e. in code-words and the reverse process of encryption is known as decryption. It is shown below in Figure 2.

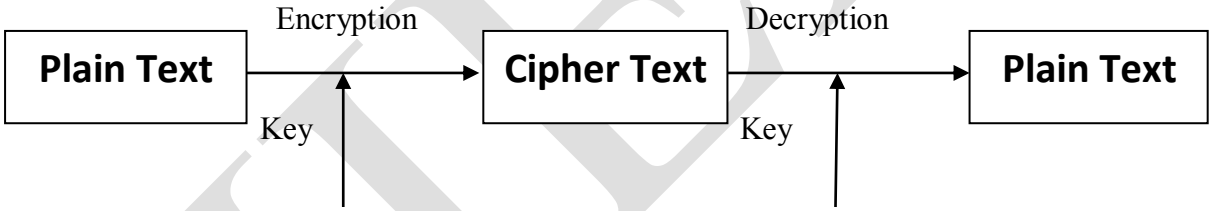

Figure 2: Block diagram of encryption and decryption process.

There are different image encryption techniques. They can be grouped into three different categories.

(i) Transposition (position permutation) techniques
(ii) Substitution (value transformation) techniques and
(iii) Visual transformation based algorithm i.e. combination of transposition-substitution technique.

In the transposition techniques/ diffusion technique, [5-7] shuffling of the pixel values position within the image itself is done and it consists of low security as there is a negligible change in the histogram of the shuffled image. In substitution techniques, there is a modification in the pixel values of the original image and has low hardware cost and low computational complexity. Next is the transposition-substitution technique, i.e. a combination of both the substitution and transposition which provides high security [8-10].

REVIEW OF IMAGE ENCRYPTION TECHNIQUES

Some of the different image encryption techniques have been categorised in Section 2. These techniques have been used by different researchers accordingly with the algorithms used. The first technique comprises of pixel permutation. Permutation-only image encryption scheme [11] was presented in which image matrix pixel values are scrambled using permutation mapping matrix. In this process i.e. permutation only image

ciphers, permutation mapping is regained completely by a chosen plaintext attack. A chosen-plaintext attack determines completely the correct plaintext elements using a deterministic i.e. non-chaos based method. When the plain-images are of size $P \times Q$ and with R different colour intensities, the number n of required chosen plain-images to break the permutation-only image encryption algorithm is $n = [\log R(PQ)]$. The complexity of the proposed attack is $O(n \cdot P\ Q)$ which indicates its feasibility in a polynomial amount of computation time. Wavelet decomposition [12] technique is used in the algorithm. High-strength chaotic encryption is applied to the process and then wavelet reconstruction and Arnold scrambling are used for diffusion process. Lastly, another wavelet decomposition and encryption round is performed to complete the encryption. Theoretical analysis and experimental results show that the algorithm has large key-space, high efficiency and satisfied security and suits for image data transmission. A novel image encryption algorithm based on chaotic system and Fractional Fourier Transform (FRFT) was introduced [13]. The image encryption process consists of two steps: firstly the image is encrypted by applying Fractional Fourier domain double random phase and then the confusion image is encrypted by using the confusion matrix which is generated by chaotic system and finally the cipher image is obtained. The security of the proposed algorithm depends on the sensitivity to the randomness of phase mask, the orders of FRFT and the initial conditions of chaotic system. Theoretical analysis and experimental results demonstrate that the algorithm was favourable.

A new loss-less symmetric image cipher based on substitution-diffusion architecture was introduced [14] which comprises of chaotic standard and logistic maps. In this technique, the initial condition and system parameters of the chaotic standard map and the number of iterations both together form the secret key of the algorithm. In the first round, substitution/confusion process is performed with the help of intermediate XO Ring keys which is calculated from the secret key. Then two rounds of diffusion process (horizontal and vertical) were performed. In the fourth round, chaotic key stream is generated in the substitution process with the help of chaotic standard and logistic maps. Analysis of the stated image encryption technique was performed using several parameters like statistical analysis, key sensitivity analysis, time analysis, key space analysis, etc. A novel permutation-substitution scheme [15] was introduced which is based on chaotic standard map. In this process all the three colour layers i.e. 3D matrix of the plain image is mixed and then is converted into a 2D matrix. Each encryption round consist of three stages i.e. permutation, substitution and then again permutation rounds. The permutation and substitution processes are done row-by-row and column-by-column to increase the speed of the encryption process. In the substitution process, the properties of rows and column pixels of several layers are mixed with the Pseudo Random Noise Sequence (PRNS). Results show that the proposed technique can be used for the real time secure image and video communication applications. Image encryption scheme [16] using a secret key of 144-bits was proposed. In the substitution process, the image is divided into blocks. Further the blocks get divided into its colour components. Each of the colour components are then modified by performing bit wise operation which depends on secret key and also a few Most Significant Bit (MSB) of its next and previous colour component. It consists of three rounds. To make cipher more robust, a feedback mechanism is applied by modifying the used secret key after encrypting each block. Then the resultant image is again partitioned into different key based dynamic sub-images which then pass through the scrambling process where pixel values of sub-image are reshuffled within itself. There were five rounds in the scrambling process. The propose scheme is simple, fast and sensitive to the secret key used in the algorithm.

A new combined chaotic system was presented [17], which shows better chaotic behaviour than the traditional ones. Applying the chaotic system to image processing, a new image encryption algorithm is proposed based on the confusion and diffusion scheme. Experimental results indicate that the proposed encryption algorithm has a higher security level and excellent performance in image encryption.

SECURITY ANALYSIS

A good encryption scheme resists against all kinds of cryptanalytic attack such as statistical and brute-force attacks. This section focuses on various parameters for analysis such as statistical analysis, information entropy, key sensitivity analysis etc and is being defined and is secure against most common attacks.

- **Statistical analysis**
  Statistical analysis consists of pixels distributions, correlation coefficient and information entropy which are given below.
  - **Pixels distributions:** In this analysis, histogram of the original image and its corresponding cipher image is taken out. Also, when the histogram analysis is done, the cipher images having RGB components have uniform distribution which is not in case of plain image which reflects its security purpose.
  - **Correlation coefficient:** The correlation coefficients between the plain and encrypted image should be very small or practically 0 so that the plain and the encrypted image are independent of each other which also resembles its security.
  - **Information entropy:** It expresses the degree of disorderness or uncertainty in the system. For an ideal case, the information entropy is 8 i.e.

    $$H(m)=8$$
- **Key sensitivity analysis:** An ideal image cipher should be extremely sensitive with respect to the secret key used in the algorithm. Flipping of a single bit in the secret key, will produce a widely different cipher image which guarantees the security of a cryptosystem against brute-force attacks.
- **Key space analysis:** Secret key used in the image cipher should be neither too long nor too short. A larger secret key decreases the encryption speed and also increases the computation power and hence is not preferred for real time image transmission whereas a choice of smaller secret key results in an easy cryptanalysis.
- **Time:** Apart from the security, the time taken to encrypt and decrypt an image in an algorithm is also an important factor for a good cipher image.

CONCLUSION

Images play an important role and are used in many applications in our day to day lives. Therefore it is necessary to protect the confidentiality and integrity of the digital image that is being transmitted. In this paper a survey on image encryption techniques has been discussed. Different encryption schemes have been studied and analysed and it is noticed that each technique is unique in its own way having their strengths and weaknesses. Everyday new techniques are evolving. This survey provides a way to realize the different aspects of image encryption and decryption techniques.

REFERENCES

1) Shannon, C. E. 1949. *Communication Theory of Secrecy Systems. Bell System of Technical Journal 28(4):656-715.*

2) Bin, L., Lichen, L., & Jan, Z. 2010. *Image encryption algorithm based on chaotic map and S-DES. IEEE 2nd International Conference on Advanced Computer Control, 5:41 – 44.*

3) Saraf, K. R., Jagtap, V. P., & Mishra, A. K. 2014. *Text and image encryption decryption using advanced encryption standard. (IJETTCS) International Journal of Emerging Trends and Technology in Computer Science, 3(3):118-26.*

4) Noura, H., El Assad, S., & Vlădeanu, C. 2010. *Design of a Fast and Robust Chaos-Based Cryptosystem for image encryption. IEEE 8th International Conference on Communications (COMM), pp. 423 – 426.*

5) Zhou, J., Liu, X., Au, O. C., & Tang, Y. Y. 2014. *Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation. IEEE transactions on information forensics and security, 9(1):39-50.*

6) Jun, Z., Jinping, L., & Luqian, W. 2010. *A new compound chaos encryption algorithm for digital images. IEEE International Forum on Information Technology and Applications (IFITA), 1:277-279.*

7) Huang, M. Y., Huang, Y. M., & Wang, M. S. 2010. *Image Encryption Algorithm Based on Chaotic Maps. IEEE International Computer Symposium (ICS), pp. 154 – 158.*

8) Zhao, J., Guo, W., & Ye, R. 2014. *A Chaos-based Image Encryption Scheme Using Permutation Substitution Architecture. International Journal of Computer Trends and Technology (IJCTT), 15(4):174-185.*

9) Feng, Y., Li, J., Han, F., & Ahmad, T. 2011. *A novel image encryption method based on invertible 3d maps and its security analysis. In IECON 37th Annual Conference on IEEE Industrial Electronics Society. pp. 2186-2191.*

10) Ye, R., & Guo, W. 2013. *A chaos-based image encryption scheme using multi modal skew tent maps. Journal of Emerging Trends in Computing and Information Sciences, 4(10):800-810.*

11) Jolfaei, A., Wu, X. W., & Muthuk kumar asamy, V. 2016. *On the security of permutation-only image encryption schemes. IEEE Transactions on Information Forensics and Security, 11(2): 235-246.*

12) Yu, Z., Zhe, Z., Haibing, Y., Wenjie, P., & Yunpeng, Z. 2010. *A chaos-based image encryption algorithm using wavelet transform. IEEE 2nd International Conference in Advanced Computer Control (ICACC), 2:217-222.*

13) Lai, J., Liang, S., & Cui, D. 2010. *A Novel Image Encryption Algorithm Based on Fractional Fourier Transform and Chaotic System. IEEE International Conference on Multimedia Communications, pp. 24 – 27.*

14) Patidar, V., Pareek, N. K., & Sud, K. K. 2009. *A new substitution–diffusion based image cipher using chaotic standard and logistic maps. Communications in Nonlinear Science and Numerical Simulation, 14(7):3056–3075.*

15) Patidar, V., Purohit, G., Sud, K. K., & Pareek, N. K. 2010. *Image encryption through a novel permutation-substitution scheme based on chaotic standard map. IEEE International Workshop on Chaos-Fractal Theory and its Applications (IWCFTA), 5(3):164 – 169.*

16) Pareek, N. K. 2012. *Design and analysis of a novel digital Image encryption scheme. International Journal of Network Security & Its Applications (IJNSA), 4(2):95-108.*

17) Chen, C. P., Zhang, T., & Zhou, Y. 2012. *Image encryption algorithm based on a new combined chaotic system. IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 2500-2504.*