National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

A Survey on Image Encryption Techniques

Vishwas C.G.M[1], Dr. R Sanjeev Kunte[2]
[1]Assistant Professor Department of IS&E, J.N.N College of Engineering, Shivamogga, Karnataka, India
[2]Professor, Department of CS & E, J.N.N College of Engineering, Shivamogga, Karnataka, India

ABSTRACT

Security of data/images is one of the important aspects and it is still an expanding domain of digital transfer. Encryption of images is one of the well known mechanisms to preserve the secrecy of images over the Internet. This medium is vulnerable to attacks and hence efficient encryption algorithms are necessary for securely transmitting the data. Various techniques have been proposed in literature to cope up the ever growing need of security. This paper is an effort to compare the most popular techniques available for image encryption.

Keywords : Encryption, Decryption, Cryptography.

I. INTRODUCTION

With the increasing growth of multimedia applications, security is an important issue in transmission of multimedia data. The main aim of image encryption is to transmit the image securely over the network so that no unauthorized user can be able to decrypt the image. Therefore the information has to be protected while transmitting it. Important information such as credit cards and banking transactions need to be secured. For this reason, many techniques exist which are Image encryption, video encryption, chaos based encryption that have their have applications in many fields including the medical imaging, internet communication, transmission, military communication, tele-medicine etc. Encryption techniques are very useful tools to protect secret information. In this paper we survey on different techniques for image encryption.

This paper is organized as follows. In Section 1; we present general guide line about cryptography. In

We Survey on already existing work. Finally, we conclude in section 3.

Encryption is defined as the conversion of plain text into a form called a cipher text that cannot be read by others without decrypting the encrypted text. Decryption is the reverse process of encryption which is the process of converting the cipher text into its original plain text, so that it can be read [1]. In order to fulfill such a task, many image encryption methods have been proposed in the literature.

There are two main types of cryptography: 1.Secret key cryptography and 2.Public key cryptography. Secret key cryptography is also known as symmetric key cryptography. Here, both the sender and the receiver have the information regarding the same secret key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

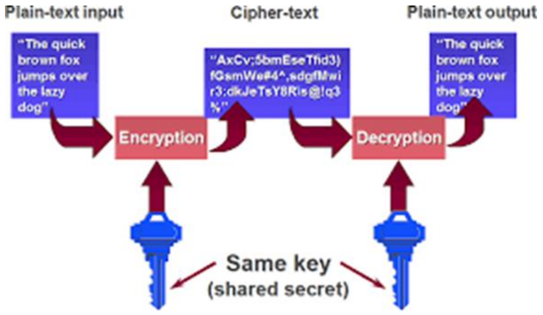
Plain-text input
Cipher-text
Plain-text output
"The quick brown fox jumps over the lazy dog"
"AxCv;5bmEseTfid3) fGsmWe#4^,sdgfMwi r3:dkJeTsY8Ris@!q3 %"
"The quick brown fox jumps over the lazy dog"
Encryption
Decryption
Same key
(shared secret)

Fig 1. A simple model of symmetric key encryption

Fig 1 shows the process of symmetric cryptography. Both parties agree on the secret key that both of them will use in this connection. Sender starts sending its data encrypted with the shared key. On the other hand, receiver uses the same key to decrypt the encrypted message.

Public key cryptography, also called asymmetric key cryptography, uses a pair of keys for encryption and decryption as shown in Fig. 2. Where as in public key cryptography, keys work in pairs of matched public and private keys.

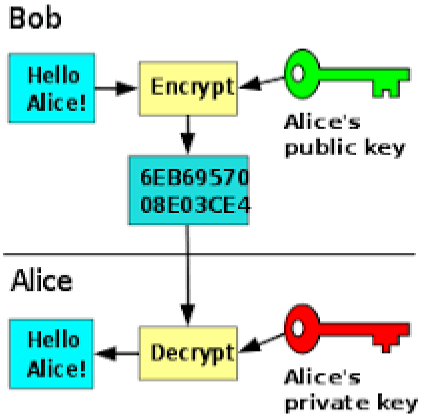

Fig 2. Asymmetric encryption

Nowadays when sensitive information is stored on computers and transmitted over the Internet, safety and security of information must be ensured. Considering this, image is also an important part of information. Therefore it is very important to protect the image from unauthorized access.

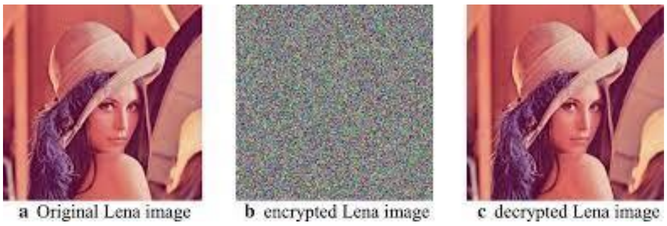

Fig 3. Image encryption process

Fig 3 shows a general image encryption process using any image encryption algorithm and the resultant encrypted image. Decryption is the reverse process of encryption which gives back the original image. There exists many algorithms in the literature to protect image from unauthorized access which is described in the next section.

II. LITERATURE SURVEY

Aloka Sinha and Kehar Singh [2] proposed the digital signature based image encryption scheme. First the original image is encoded and digital signature is added to the original image. Bose- Chaudhuri Hochquenghem (BCH) type of code is used for encoding of the image. After the decryption of the image, digital signature is used for authentication of the image and digital signatures are created and verified by means of cryptography. One-way hash function was used to produce the digital signature of an image. Standard digital image algorithms were used to convert a message of any length into a fixed length message digest which is usually 128 bits long. MD2, MD4, MD5 and Secure Hash Algorithm (SHA) are the standard techniques for creating hash. This encryption technique provides three layers of security.

S.Vani Kumari and G.Neelima [3] proposed the image encryption by using Chaotic Logistic Map and Arnold Cat Map. In this scheme, first block based shuffling is performed using Arnold cat transformation. After block based shuffling, pixel shuffling is performed by using certain number of iterations of Arnold cat map. The Arnold cat map is used to change the positions of the blocks/pixel values of the original image. The shuffled image contain the same pixel values as that of the original image. To encrypt the pixels of an image, eight different types of operations are used and which operation should be used is decided by the logistic map. It is concluded that chaos-based image encryption technology is very useful for real-time secure image.

Mohammad Ali Bani Younes and Arnan Jantan [4] proposed an image encryption using block-based transformation algorithm. A block-based transformation algorithm along with blowfish algorithm is used for encryption and decryption. First the original image is divided into blocks and then it is rearranged into a transformed image using a transformation algorithm. Later, blowfish algorithm is used for encryption. It is observed that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy. Experimental results showed that a direct relationship exists between number of blocks and entropy. And an inverse relationship exists between number of blocks and correlation.

A Combination of Permutation Technique for image encryption was proposed by Mohammad Ali Bani Younes and Aman Jantan [5]. This approach depends on the concept that, in natural images the values of the neighboring pixels are strongly correlated. This means that the value of any given pixel can be reasonably predicted from the values of its neighbors. It is necessary to disturb the high correlation among image pixels to increase the security level of the encrypted images. Here, a new permutation technique is introduced based on the combination of image permutation and an encryption algorithm called RijnDael. Here the original image is divided into 4 pixels × 4 pixels blocks, which are then rearranged into a permuted image by using a permutation process. The permutation process is defined as the operation of dividing and replacing an arrangement of the original image. The results show that the correlation between image elements is significantly decreased by using the combination technique which leads to higher entropy. This technique enhances the security level of the encrypted images by reducing the correlation among image elements and increasing its entropy value by decreasing the mutual information among the encrypted image variables.

Bibhudendra Acharya et.al.[6] proposed an Image encryption using Advanced Hill Cipher Algorithm. The available Hill cipher algorithm is classified as a symmetric key algorithm. The proposed advanced Hill (AdvHill) encryption technique uses an involuntary key matrix which overcomes the problem of encrypting the images with homogeneous background. It also overcomes the drawback of using a random key matrix in Hill cipher algorithm for encryption, where if the key matrix is not invertible then it may not be possible to decrypt the encrypted message. Also, as it is not required to find inverse of the matrix for decryption, the computational complexity can be reduced.

Sesha Pallavi Indrakanti and P.S.Avadhani [7] proposed Permutation based Image Encryption Technique in which image encryption based on random pixel permutation exists. In this technique, first for image encryption, image is split into blocks, later permutation is applied based on random number. Next, in the key generation phase, a key is built by using the values used in the encryption process. The last stage is where the identification process is involved in the numbering of the shares which are generated from the secret image. These shares and the key are then sent to the receiver. The key is generated with valid information about the values used in the encryption process which is a unique one from others. A new image encryption technique based on a new chaotic system by adding two chaotic systems: the Lorenz chaotic system and the Rössler chaotic system was proposed by Qais H. Alsafasfeh and Aouda A. Arfoa [8]. The main strength of this technique is that it provides stronger security. Data encryption standard (DES) is not useful for image encryption because of the special storage characteristics of an image. Experimental analysis shows that the image encryption algorithm has the advantages of high speed, large key space, high- level security and high obscure level.

Ibrahim S I Abuhaiba and Maaly A S Hassan [9] describe an Image Encryption using Differential Evolution Approach in Frequency Domain. This scheme employs magnitude and phase manipulation using Differential Evolution (DE) approach. First the two dimensional keyed discrete Fourier transform is performed on the original image. Then Crossover is performed between two components of the encrypted image, which are selected based on Linear Feedback

Shift Register (LFSR) index generator. Keyed mutation will be performed on the real parts of a certain components selected based on LFSR index generator. In this process, shuffling of the positions of image pixels is done. Final encrypted image is found to be fully distorted increasing the robustness of the said scheme.

Nidhal Khdhair El Abbadi et.al., [10] proposed new image encryption algorithm based on Diffie- Hellman and Singular Value Decomposition. In the proposed work, they have suggested a new way to encrypt image based on three main steps: the first one aims to scrambling the image values by using Fibonacci transform. The second step focuses on generating public and private key based on Diffie - Hellman Key Exchange which are used encrypt the diagonal matrix that is created by Singular Value Decomposition (SVD) in third step. The experimental results show that the proposed image encryption system has a very large key space. Also the proposed image encryption algorithm analysis proves better in case of the security, robustness, correctness and effectiveness.

S.S. Maniccam and N.G. Bourbakis [11] have presented a novel approach which based on two works: lossless compression and encryption of binary and gray-scale pictures. The compression and encryption methods are based on the SCAN methodology which is a formal language-based 2D spatial-accessing methodologies that generate a wide range of scanning paths or space filling curves.

Chang-Mok Shin et.al.,[12] proposed an algorithm which was multilevel form of image encryption using binary phase exclusive OR operation and image dividing technique. The same grey level multi-level image is divided into binary images. Then binary pictures are regenerated to binary phase encoding.Then these images are encrypt with binary random phase images by binary phase XOR operation.

Huang-PeiXiao and Guo-ji Zang [13] describe an algorithm using two chaotic systems . One chaotic system generates a chaotic sequence, which changes into a binary stream using a threshold function. The other chaotic system is used to construct a permutation matrix. Firstly, using the binary stream as a key stream, randomly the pixel values of the images is modified. Then, the modified image is encrypted again by the permutation matrix.

Amitava Nag et.al, [14] introduced a novel approach using affine transform which is based on shuffling the image pixels. This method is a two phase encryption decryption algorithm. Firstly using XOR operation, the image is encrypted. Then, the pixel values are redistributed to different locations with 4 bit keys using the affine transformation. The transformed image is then divided into 2 pixels x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The result proves that the correlation between pixel values was significantly decreased after the affine transform.

A mirror like algorithm is presented by Jiun-In Guo and Jui-Cheng Yen [15]. There are 7 steps in this algorithm. At first, 1-D chaotic system is determined and its initial point x (0) and set k = 0. Then, from the chaotic system, the chaotic sequence is generated. After that, the binary sequence is generated from chaotic system. Image pixels are rearranged in the last four stages using swap function according to the binary sequence.

Seyed Mohammad Seyedzade, et.al., [16] proposed a novel algorithm based on SHA-512 hash function. The algorithm had two sections. Firstly, it does pre-processing operation to shuffle one half of image. Then the hash function is applied to generate a random number mask. Then, the mask is XORed with the other part of the image that is to be encrypted.

Ismail Amr Ismail et.al.,[17] proposed a chaos- based stream cipher which composes of two chaotic logistic maps and it also consists of an external secret key for encryption of image. In this scheme, an external secret key of 104 bit and two chaotic logistic maps are used to differentiate between the plain image and the encrypted image. Further, the secret key is modified after encrypting of each pixel of the plain image which makes the encrypted image more robust in nature. There is also a feedback mechanism which increases the robustness of the said scheme.

Rasul Enayatifar and Abdul Hanan Abdullah [18] proposed a novel scheme for image encryption based on a hybrid model composed of a chaotic function and a genetic algorithm. In this scheme, with the help of the chaotic function, first a number of encrypted images are constructed using the original image. In the next stage, these encrypted images are employed as the initial population for starting the operation of the genetic algorithm. Then, as much as possible, the genetic algorithm is used to optimize the encrypted images. In the end, the best cipher-image is selected as the final encryption image.

Kuldeep Singh and Komalpreet Kaur [19] compared four chaotic maps i.e., Henon, Logistic, Cross chaotic and Ikeda map and noise effects are observed on the image. First, the image encryption algorithm is used to convert the given original image to encrypted image. Then they apply noise on the encrypted image and then decrypt cipher image with noise back to original image. The conclusion is that the cross chaotic map shows best results than the other three chaotic maps.

III. CONCLUSION

In today's digital world, the security of digital images has become more important. In this paper, we have surveyed existing work on image encryption. We also give the general guide line about cryptography. The techniques that are described in this paper can provide security functions which might be suitable in some applications so that no one can carry unauthorized access on the image while transferring the image on the open network. In general, a well-suited, fast and secure conventional cryptosystem should be chosen so as to provide high security.

IV. REFERENCES

[1]. John Justin M, Manimurugan S, "A Survey on Various Encryption Techniques", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[2]. Aloka Sinha and Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203), 229- 234.

[3]. S. Vani Kumari and G. Neelima, "An efficient Image Cryptographic Technique By Applying Chaotic Logistic Map and Arnold Cat Map", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 9, 2013.

[4]. Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, 35, 2008.

[5]. Mohammad Ali Bani Younes and Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique

[6]. Followed by Encryption", IJCSNS International Journal of Computer Science and Network Security, VOL.8 , April 2008.

[7]. Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", International Journal of Recent Trend in Engineering, Vol. 1, No. 1, May 2009.

[8]. Sesha Pallavi Indrakanti, P.S.Avadhani, "Permutation based Image Encryption Technique", International Journal of Computer

Applications (0975 – 8887) Volume 28– No.8, 2011.

[9]. Qais H. Alsafasfeh , Aouda A. Arfoa, “Image Encryption Based on the General Approach for Multiple Chaotic Systems”, Journal of Signal and Information Processing, 2011.

[10]. Ibrahim S I Abuhaiba , Maaly A S Hassan, “Image Encryption Using Differential Evolution Approach In Frequency Domain” Signal & Image Processing: An International Journal(SIPIJ) Vol.2, No.1, March 2011.

[11]. Nidhal Khdhair El Abbadi, Samer Thaaban Abaas, Ali Abd Alaziz “New Image Encryption Algorithm Based on Diffie-Hellman and Singular Value Decomposition”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016, pages: 197-201.

[12]. S.S.Maniccam, N.G. Bourbakis, “Lossless image compression and encryption using SCAN”, Pattern Recognition 34(6): 1229-1245 2001.

[13]. Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, “Multilevel Image Encryption by Binary Phase XOR Operations”, IEEE Proceedings, 2003.

[14]. Huang-Pei Xiao Guo-Ji Zhang, “An Image Encryption Scheme Based On Chaotic Systems”, IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006.

[15]. Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, “Image Encryption Using Affine Transform and XOR Operation ”,International Conference on Signal

[16]. Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).

[17]. Jiun-In Guo, Jui-Cheng Yen, “A new mirror-like image Encryption algorithm and its VLSI architecture”, Pattern Recognition and Image Analysis, vol.10, No.2, pp.236-247, 2000.

[18]. Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, “A Novel Image Encryption Algorithm Based on Hash Function”, 6th Iranian Conference on Machine Vision and Image Processing, 2010.

[19]. Ismail Amr Ismail, Mohammed Amin, Hossam Diab ,”A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps”, International Journal of Network Security, Vol.11, No.1, pp.1 -10, July 2010.

[20]. Rasul Enayatifar , Abdul Hanan Abdullah, “Image Security via Genetic Algorithm”, International Conference on Computer and Software Modeling IPCSIT Vol.14, 2011.

[21]. Kuldeep Singh, Komalpreet Kaur, “Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it”, International Journal of Computer Applications (0975 – 8887) Volume 23– No.6, June 2011.

Cite this article as :

Vishwas C.G.M, Dr. R Sanjeev Kunte, "A Survey on Image Encryption Techniques", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 165-170, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194731