ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

A Survey on Different Image Encryption Techniques

Tejaswini B. Ghanwat[1], Gayatri R. Vidhate[2]

Assistant Professor, Dept. of EE, Karmaveer Bhaurao Patil, College of Engineering , Satara, Maharashtra, India[1]

Assistant Professor, Dept. of EE, KIT's, College of Engineering, Kolhapur, Maharashtra, India[2]

ABSTRACT: In present times, the protection of multimedia data is becoming very important which can be done with encryption. Due to growth of multimedia application, security becomes an important issue of communication and storage of images. There are various techniques which are discovered from time to time to protect secret image from unauthorized access. In this paper a Survey of different Encryption Techniques that are existing is given.

KEYWORDS: Asymmetric key cryptography, Decryption, Encryption, Image encryption, Symmetric key cryptography.

I. INTRODUCTION

With the increasing growth of multimedia applications, security is an important issue in transmission of images. Encryption is one the way to ensure security. Image encryption techniques convert original image to another image which is hard to understand. Also reliable security in storage and transmission of digital images is needed in many applications, such as online personal photograph album, medical systems, confidential video conferences, military communications etc. In order to fulfil such a task, many image encryption methods have been proposed. Encryption is the process of encoding messages or information in such a way that only authorized parties can able to read it using the decryption key. An authorized person can easily decrypt the message with the key provided. Somebody who is not authorized can be excluded, because he or she does not have the required key, without which it is impossible to read the encrypted information.

II. LITERATURE SURVEY

Image encryption using digital signature, 2003

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

Applying Chaotic Logistic Map and Arnold Cat Map for Image Cryptography, 2013

S.Vani Kumari, G.Neelima proposed the image encryption by using *Chaotic* Logistic Map and Arnold Cat Map. Here first Block based shuffling was 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 was used to change the positions of the blocks/pixel values of the original image. Shuffled image contain the same pixel values as that of 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 outcome of logistic map. It is concluded that chaos-based image encryption technology is very useful for real-time secure image.

A Modified AES Based Algorithm for Image Encryption 2007

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki proposed the AES based algorithm for Image Encryption. In this paper, we analyze the Advanced Encryption Standard (AES), and we add a key stream generator(A5/1, W7) to AES to ensure improving the encryption performance. It is observed that average time required

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

by AES for image encryption is much lesser as compared to three existing image encryption algorithms; “VC”, “MIE”, “N/KC”.

TABLE I
ENCRYPTION TIME USING DIFFERENT ALGORITHMS WITH LENA AS TEST IMAGE

Algorithm	Encryption (s)
MIE	0.27
VC	0.98
N/KC	0.15
AES	0.03175

Using Block-Based Transformation Algorithm for Image Encryption 2008

Mohammad Ali Bani Younes and Arnan Jantan proposed an Image Encryption Using Block-Based Transformation Algorithm. Here a block-based transformation algorithm and Blowfish algorithm was used for encryption and decryption. First the original image was divided into blocks; it is then rearranged into a transformed image using a transformation algorithm and then the Blowfish algorithm was used for encryption. It was 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 between number of blocks and entropy and an inverse relationship exists between number of blocks and correlation.

An Image Encryption Approach Using a Combination of Permutation Technique, 2008

Mohammad Ali Bani Younes and Aman Jantan proposed an Image Encryption Approach Using a Combination of Permutation Technique. In natural images the values of the neighbouring pixels are strongly correlated. This means that the value of any given pixel can be reasonably predicted from the values of its neighbours. It is necessary to disturb the high correlation among image pixels to increase the security level of the encrypted images. In this paper, a new permutation technique is introduced based on the combination of image permutation and an encryption algorithm called RijnDael. Here the original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process. The permutation process is the operation of dividing and replacing an arrangement of the original image. The results showed that the correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved. This technique enhances the security level of the encrypted images by reducing the correlation among image elements, increasing its entropy value by decreasing the mutual information among the encrypted image variables.

Image Encryption Using Advanced Hill Cipher Algorithm, 2009

Bibhudendra Acharya, Saroj K Panigrahy, Sarat K Patra, and Ganapati Panda Proposed an Image encryption using Advanced Hill Cipher Algorithm. The Hill cipher algorithm is symmetric key algorithms. They proposed an advanced Hill (AdvHill) encryption technique which uses an involuntary key matrix. This scheme overcomes problems 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 we may not be able to decrypt the encrypted message. Also the computational complexity can be reduced, as it is not required to find inverse of the matrix for decryption.

Permutation based Image Encryption Technique, 2011

Sesha Pallavi Indrakanti and P.S.Avadhani proposed Permutation based Image Encryption Technique. Image encryption algorithms are mostly complex and compromise on the quality of the image. This paper proposes image encryption based on random pixel permutation. It also maintains the quality of the image. In this technique, first for image encryption, image is split into blocks. Then permutation is applied based on random number. In key generation phase, a key is build by using the values used in the encryption process. The last stage is the identification process which involves the numbering of the shares which are generated from the secret image. These share and key are then send to receiver. In this proposed technique, the key is generated with valid information about the values used in the encryption process which is unique one from the others.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Image Encryption Based on the General Approach for Multiple Chaotic Systems, 2011
Qais H. Alsafasfeh, Aouda A. Arfoa proposed new image encryption technique based on new chaotic system by adding two chaotic systems: the Lorenz chaotic system and the Rössler chaotic system. This technique 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 large key space, high speed and high-level security, high obscure level.

Image Encryption Using Differential Evolution Approach in Frequency Domain, 2011
Ibrahim S I Abuhaiba and Maaly A S Hassan proposed an Image Encryption Using Differential Evolution Approach in Frequency Domain. This method 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. Also, keyed mutation is performed on the real parts of a certain components selected based on LFSR index generator. The process shuffles the positions of image pixels. Final encrypted image is found to be fully distorted increasing the robustness of the proposed work.

Image Encryption and Decryption Using Blowfish Algorithm in Matlab, 2013
Pia Singh and Prof. Karamjeet Singh proposed an Image Encryption and Decryption Using Blowfish Algorithm in Matlab. Bruce Schneier designed blowfish in 1993 as an encryption algorithm. It is consider as one of the strongest encryption algorithms. The Blowfish algorithm has many advantages. It is suitable for hardware implementation and no license is required. The algorithm has two parts, key expansion and data encryption. Blowfish is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits (14 bytes).Blowfish can be considered as an excellent standard encryption algorithm.

Fast Image Encryption based on Random Image Key, 2016
Abdulrahman Dira Khalaf Proposed Fast Image Encryption based on Random Image Key. In this paper a new algorithm is proposed to encrypt color image using symmetric key which is generated from the same image. The block cipher and stream cipher are two types of cryptosystem. Stream ciphers are different to block ciphers; they do not transform blocks of data to another block of data instead based on a key. In this paper, a new algorithm is designed to generate image key from the same image. Here an image key is generated by rotating the origin image to three directions. Then four images are cut and scrambled randomly and then XOR logic is used to generate image key. Also it is possible to encrypt partial image instead of full image encryption.

New Image Encryption Algorithm Based on Diffie-Hellman and Singular Value Decomposition, 2016
Nidhal Khdhair El Abbadi, Samer Thaaban Abaas, Ali Abd Alaziz proposed new image encryption algorithm based on Diffie-Hellman and Singular Value Decomposition.This paper 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, while the second step focus on generating public and private key based on Diffie -Hellman Key Exchange, these keys used to encrypt the diagonal matrix which created by Singular Value Decomposition (SVD) in third step. The experimental results showed 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, correctness, effectiveness and robustness.

III. RESULT AND CONCLUSION

The security for the digital image has become highly important since the communication by transmitting of digital products over the open network occur very frequently. In this paper I have surveyed different image encryption and decryption techniques. We conclude that all techniques are useful for real-time image encryption. Techniques describes in this paper can provide security and an overall visual check, which might be suitable in some applications. 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

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

REFERENCES

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

[2] 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 I 9, Sep-2013.

[3] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, ― "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology 27 2007.

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

[6] 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.

[7] Sesha Pallavi Indrakanti , P.S.Avadhani, "Permutation based Image Encryption Technique", International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, 2011.

[8] Qais H. Alsafasfeh , Aouda A. Arfoa, " Image Encryption Based on the General Approach for Multiple Chaotic Systems", Journal of Signal And Information Processing, 2011.

[9] 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.

[10] Pia Singh, Karamjeet Singh, "Image Encryption and Decryption Using Blowfish Algorithm in MATLAB", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013, pages:150-154.

[11] Abdulrahman Dira Khalaf, "Fast Image Encryption based on Random Image Key", International Journal of Computer Applications, Volume 134 – No.3, January 2016, pages: 35-43.

[12] 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.

[13] Nadeem, Aamer; "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.

[14] 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.

[15] William Stallings, Cryptography and Network Security, Principles and Practice. Fifth edition.

[16] D. R.Stinson, Cryptography, Theory and Practice. Third edition: Chapman & Hall/CRC, 2006.