International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-4, April 2014

A Review: Image Encryption Techniques and its Terminologies

Ambika Oad, Himanshu Yadav, Anurag Jain

Abstract— In today's environment, security becomes an important issue in communication. For secure transmission of data in open network, encryption is very important methodology. Though encryption we can prevent our data from unauthorized access during transmission. In recent years many image encryption methods have been proposed and used to protect confidential data. In this paper, we survey on existing work which is used different techniques for image encryption and we also give general introduction about cryptography.

Index Terms— Cryptography, Image Encryption, Decryption, Security.

I. INTRODUCTION

In the current trends, the technologies have been advanced. Most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the internet. There are many possible ways to transmit data using the internet like: via e-mails, sending text and images, etc. In the present communication world, images are widely in use. However, one of the main problems with sending data over the Internet is the 'security' and authenticity. Data security basically means protection of data from unauthorized users or attackers. Encryption is one of the technique for the information security. Image encryption is a technique that convert original image to another form that is difficult to understand. No one can access the content without knowing a decryption key. Image encryption has applications in corporate world, health care, military operations, and multimedia systems. Encryption is the process of encoding plain text message into cipher text message whereas reverse process of transforming cipher text to plain text is called as decryption[1]. Cryptography consists of encryption and decryption techniques. In this paper we have discuss about the various encryption terminologies, purpose of cryptography and its types.

1. Basic Terms Used in Cryptography

1.1 Plain Text: The original massage that the person wishes to communicate with the other is defined as plain text. In cryptography the actual message that has to be send to the other end is given a special name as plain text [2].

1.2 Cipher Text: The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message [3].

Manuscript published on 30 April 2014.
* Correspondence Author (s)
Ambika Oad*, CSE department, RITS, Bhopal, India.
Himanshu Yadav, CSE department, RITS, Bhopal, India.
Anurag Jain, CSE department, RITS, Bhopal, India.

1.3 Encryption: A process of converting Plain Text into Cipher Text is called as Encryption[1]. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

1.4 Decryption: A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption[4]. Generally the encryption and decryption algorithm are same.

1.5 Key: A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it.

2. Purpose of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography[5].

2.1 Confidentiality: Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

2.2 Authentication: The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

2.3 Integrity: Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

2.4 Non Repudiation: Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

2.5 Access Control: Only the authorized parties are able to access the given information.

3. Classification of Cryptography

Cryptography technique is used when secret message are transferred from one party to another over a communication line. There are two main types of cryptography [5]:

1. Symmetric *key* cryptography
2. Asymmetric *key* cryptography

3.1 Symmetric *key* cryptography:

With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e. the key length etc.

3.2 Asymmetric *key* cryptography:

It used encryption and decryption algorithm pair. With public key cryptography, keys work in pairs of matched public and private keys.

II. LITERATURE REVIEW

A. A New Combined Symmetric Key Cryptography CRDDBT Using – Relative Displacement (RDC) and Dynamic Base Transformation (DBTC) 2013.

This paper [21] focused a new technique of encryption without a predefined key. The input string is fragmented into several parts, with each part encrypted using a different algorithm. On the whole, three unique algorithms have been applied to encrypt the fragmented string on the basis of its orientation. For higher security levels, the key is derived from the two differently determined keys. The salient feature of this algorithm is that, a part of string is manipulated using base conversion, second part of string is deformed by interchanging position and increasing number of repetitions. time taken for encryption time taken for encryption.

B. New Image Encryption Technique Based On Combination of Block Displacement and Block Cipher Technique 2013.

In this paper [20], a new image encryption algorithm is proposed. It is already known that security of the algorithm is depended on the length of the key that mean longer key length will always support to good security feature and proposed algorithm used 128 bits key length which is provided too much security for the proposed algorithm. To access original key or crypto analysis of the proposed key is required 2^{128} time to break the key which is almost impossible for any hacker. There is no chance to generate floating point error because no such types of mathematical formula have applied on the proposed algorithm. The correlation co-efficient as well as their entropy values for the proposed algorithm was calculated.

C. Image Encryption based on the RGB PIXEL Transposition and Shuffling 2013.

This paper [19] proposed a technique of transposition and reshuffling of the RGB values of the image in steps has proven to be really effective in terms of the security analysis. The extra swapping of RGB values in the image file after R G B component shifting has increased the security of the image against all possible attacks available currently.

D. Enhanced Color Visual Cryptography 2012.

In this paper [18] a new algorithm is proposed. For image encryption by using sorting of pixels as per their RGB values and arranging them group-wise which helped to reduce the correlation between pixels and increased entropy value. Experimental results were taken out on Matlab 6.0.1 and this is a lossless image encryption algorithm with results. Histogram of plain image and cipher image is also carried out. Further inter pixel algorithm can be used with another confusing property to result in better image encryption technique.

E. Image Encryption Based on Explosive Inter-pixel Displacement of the RGB Attributes of a Pixel, 2011

This paper [17] was proposed in 2011 which focused in manipulation of RGB values of pixel and its displacement as per the predefine key. Circular shift applied on the three component of pixel with different key so that R, G and B values of pixel inter mix with the R, G, B value of other pixel which is also terms as explosive inter-pixel displacement.

F. Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices, 2011.

This paper [16] was proposed in 2011 which was further extension of work of Inter-Pixel displacement of the RGB attributes of a Pixel by making the 4 slices and shuffling of those slices before encryption. Slices were made from the centre of image and these four slices were diagonally inter exchanged before doing actual image encryption.

G. Permutation based Image Encryption Technique, 2011.

Sesha Pallavi Indrakanti and P.S.Avadhani [15] introduced an algorithm on the basis of random pixel permutation with the motivation to maintain the quality of the image. It had three phases in the process of encryption. The phase one was the image encryption. The phase two was the key generation phase. And the phase three was the identification process. This provides confidentiality to color image with less computations.

H. Digital image encryption algorithm based on chaos and improved DES, 2009

Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan and Dai Wei-di [14] researches on the combination of image encryption algorithm like chaotic encryption, DES encryption etc. In their algorithm, for making the pseudo-random sequence, logistic chaos sequencer was used, it carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement DES. This algorithm had high security and the encryption speed.

I. Image Encryption Using Block-Based Transformation Algorithm, 2008

Mohammad Ali Bani Younes and Aman [13] introduce a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, and using the transformation algorithm it was rearranged, and then the Blowfish algorithm is used for encrypting the transformed image their results showed that the correlation between image elements was significantly decreased. Their results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

J. An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption, 2008.

RijnDael was introduced by Mohammad Ali Bani Younes and Aman Jantan [12] using the combination of image permutation.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process, and then RijnDael algorithm was applied on the generated image for encryption. Their results showed that the correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved.

K. Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm, 2008

Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jena [11] present image encryption technique using the Hill cipher. They are generating self-invertible matrix for Hill Cipher algorithm. Using this key matrix they encrypted gray scale as well as color images. Their algorithm works well for all types of gray scale as well as color images except for those images which have background of same gray level or of same color.

L. Image encryption using chaotic logistic map,2006

N.K. Pareek, Vinod Patidar introduce a image encryption method using chaotic logistic map [10]. In this paper image encryption scheme, an external secret key of 80-bit and two chaotic logistic maps are employed. The initial conditions for the both logistic maps are derived using the external secret key by providing different weightage to all its bits. Further, in the encryption process, eight different types of operations are used to encrypt the pixels of an image and which one of them will be used for a particular pixel is decided by the outcome of the logistic map. To make the cipher more robust against any attack, the secret key is modified after encrypting each block of sixteen pixels of the image. The results of several experimental, statistical analysis and key sensitivity tests show that the image encryption scheme provides an efficient and secure way for real-time image encryption and transmission.

M. A Technique for Image Encryption using chaos technique, 2006.

Huang-PeiXiao , Guo-ji Zang [9] proposed scheme using two chaotic systems based on the thought of higher secrecy of multi-system. One of the chaotic systems is used to generate a chaotic sequence. Then this chaotic sequence was transformed into a binary stream by a threshold function. The other chaotic system was used to construct a permutation matrix. Firstly, the pixel values of a plain image have been modified randomly using the binary stream as a key stream. Secondly, the modified image was encrypted again by permutation matrix.

N. New Chaotic Image Encryption Algorithm , 2004

Zhang Han, Wang Xiu Feng [8], Firstly permutation transform and then nonlinear map to circularly iterate pixel values. Failure of encryption owing to self-similarity and visional psychological characteristics of image.

O. Technique based on T-matrix, 2004

M.-R. Zhang, G.-C. Shao and K.-C. Yi [7] used a T matrix for image scrambling. The T-matrix has a simple conformation and a period twice of the Arnold matrix. This can be applied to image encryption and pre-processing in image processing such as image watermarking algorithms and etc.

P. A Technique for Image Encryption using multi level and image dividing technique, 2003

Chang- Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha- Wmn Lee, and SmJmng Kim [6] proposed the multi-level image encryption by using binary phase exclusive OR operation and image dividing technique. The multi-level image can be divided into binary images that have same gray levels. They converted binary images to binary phase encoding and then encrypt these images with binary random phase images by binary phase XOR operation. Encrypted gray image was then obtained by combining each binary encrypted images.

III. CONCLUSION

In this paper, various important encryption techniques have been presented and analyzed in order to make familiar with the other encryption algorithms used in encrypting the image which has been transferred over network. The results of the simulation show that every algorithm has advantages and disadvantages based on their techniques which are applied on images. I conclude that all techniques are good for image encryption and give security so that no one can access the image which is in the open network.

IV. ACKNOWLEDGMENT

I would like to say thanks to my Head of Department (HOD) “Prof. Anurag Jain” and guide “Mr. Himanshu Yadav” who gives their knowledge and time in order to complete this paper. This paper will never complete without the support of faculty member of Computer Science and Engineering (CSE) department of Radharaman Institute of technology and science (RITS) Bhopal.

REFERENCES

[1] http://en.wikipedia.org/wiki/Encryption
[2] http://en.wikipedia.org/wiki/Plaintext
[3] http://en.wikipedia.org/wiki/Ciphertext
[4] http://en.wikipedia.org/wiki/Decryption
[5] http://en.wikipedia.org/wiki/Cryptography
[6] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, “ Multilevel Image Encryption by Binary Phase XOR Operations “, IEEE Proceeding in the year 2003.
[7] M.-R. Zhang, G.-C. Shao and K.-C. Yi, — T-matrix and its applications in image processingl, IEEE Electronics Letters 9th December 2004 Vol. 40 No. 25
[8] Wang Ying, Zheng DeLing, Ju Lei, et al., —The Spatial-Domain Encryption of Digital Images Based on High-Dimension Chaotic Systeml, Proceeding of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, pp. 1172-1176, December. 2004
[9] Guosheng Gu ,Guoqiang Han “An Enhanced Chaos Based Image Encryption Algorithm”, IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) in 2006.
[10] N.K. Pareek, Vinod Patidar, "Image encryption using chaotic logistic map", Elsevier, Image and Vision Computing 24 (2006) 926–934.
[11] Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jen, Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm 1st t International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008
[12] 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.
[13] Mohammad Ali Bani Younes and Aman Jantan ImageEncryption Using Block-Based Transformation Algorithm IAENG International Journal of Computer Science, 35,2008.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

[14] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan , Dai Wei-di, Digital image encryption algorithm based on chaos and improved DES, IEEE International Conference on Systems, Man and Cybernetics, 2009.

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

[16] Amnesh Goel, Reji Mathews & Nidhi Chandra, "Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices", International Journal of Computer Applications (0975 – 8887), Volume 36– No.3, December 2011.

[17] Reji Mathews, Amnesh Goel, Prachur Saxena & Ved Prakash Mishra, "Image Encryption Based on Explosive Inter-pixel Displacement of the RGB Attributes of a PIXEL", Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, 2011, San Francisco, USA. ISBN: 978-988-18210-9-6.

[18] S.Bosu Babu & S.S.P Kumar "Enhanced Color Visual Cryptography" Engineering Science and Technology: An International Journl, , ISSN: 2250-3498, Vol.2, No. 5, October 2012

[19] Quist-Aphetsi Keste," Image Encryption based on the RGB PIXEL Transposition and Shuffling" I.J.Computer Network and Information Security, 2013,7, 43-50,2013.

[20] Keerti Kushwah, Sini Shibu "New Image Encryption Technique Based On Combination of Block Displacement and Block Cipher Technique," International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 61 - 65

[21] Nehal Kandele, Shrikant Tiwari "A New Combined Symmetric Key Cryptography CRDDBT Using - Relative Displacement (RDC) and Dynamic Base Transformation (DBTC)", International Journal of Engineering Research & Technology, Vol.2 - Issue 10 (October - 2013)(2278-0181)