A Survey on Existing Image Encryption Techniques

Er. Ramandeep Kaur
M. Tech. Research Scholar
Department of Computer Engineering
Yadavindra College of Engineering, Talwandi Sabo, Punjab, India

Er. Sumeet Kaur
Assistant Professor
Department of Computer Engineering
Yadavindra College of Engineering, Talwandi Sabo, Punjab, India

Abstract

In today's technical World people always concern with security of data before sending it over the internet. Security of data provides protection to data from unauthorized access. There is large no. of algorithms are available to secure the data. Cryptography plays a key role in data security. In modern cryptographic system encryption techniques are most widely in use. It provides security to data so that it can be used in confidential area like military, net banking, online transactions, medical, scientific etc. In this paper we mainly focus on some existing encryption techniques. Every technique comes with its good and bad features. It gives a brief review to researcher to choose a particular type of encryption scheme for some selected type of data so that it can be efficient and more secure.

Keywords: Authentication, Basic Cryptography, Decryption, Encryption, Encryption Types

I. INTRODUCTION

Providing the security to data is becomes the most challenging task for data communication and IT engineers. Security related to online data is known as cyber security. As the Internet grown up today, more and more data is used in every field of life and we become so dependent on that data or information. Advancement in technology has good as well as bad effects. It is too easy to share information from a corner of world to another end. The information may be any image, text, binary data, audio, video etc. But the fact is also true the data hacking is also become so easy. The hackers can use the technology for their own intentions. So we can say that data security is most important today.

Encryption is a technique used for security purpose of data. It is a subpart of Cryptography. It can be applied on various form of data like text, image, audio etc. with increase in online applications the popularity of also got increased. A large no. of encryption techniques exists that prevent data from illegal access. Image encryption, video encryption has many application areas like banking, multimedia, military, medical and tele- medicine. Every day a new method is discovered on the basis of encryption.

Encryption is a process that changes the data form a readable format to unreadable format to prevent it from read by anyone and send it from sender to receiver via a communication channel.

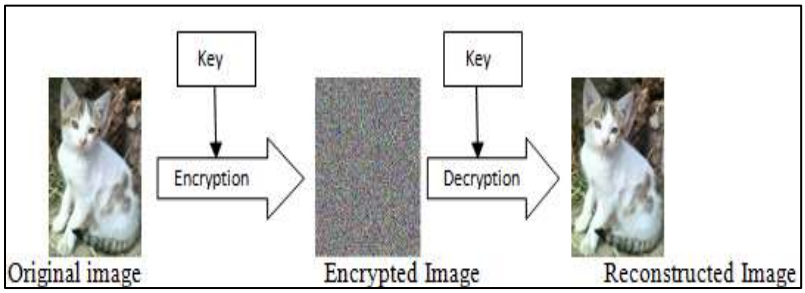

Fig. 1: Encryption Process

The original data is known as plain text which is readable. The senders change the data into some other non-readable format using an encryption key and send this encrypted data to the receiver. The receiver receives the data and decrypts it by using a key into its original readable form. The data after encryption is called cipher text. Changing process cipher text into plain text is known as decryption. Key is a crucial part of an encryption scheme. Security of algorithm depends upon the length of key.

There is large no. of encryption algorithms are available for encryption like AES, RSA, DES ,Blowfish etc but most of these used for text and binary data encryption. We cannot use them directly for complex type of data because in multimedia data high degree of redundancy is found and fast interaction is needed. Some method provide security to a great extent but slow in speed while some provide speed but less efficient. The whole existing algorithm cannot provide the entire feature in one algorithm so strictly need an encryption algorithm which has attack tolerance.

The paper is organized into 3 Phases.

- Basics of Cryptography

- Existing Techniques on image encryption
- Conclusion

A. Cryptography

It is a mechanism to enciphering and deciphering a message from sender to receiver and vice versa. Encryption is a subpart of cryptography.

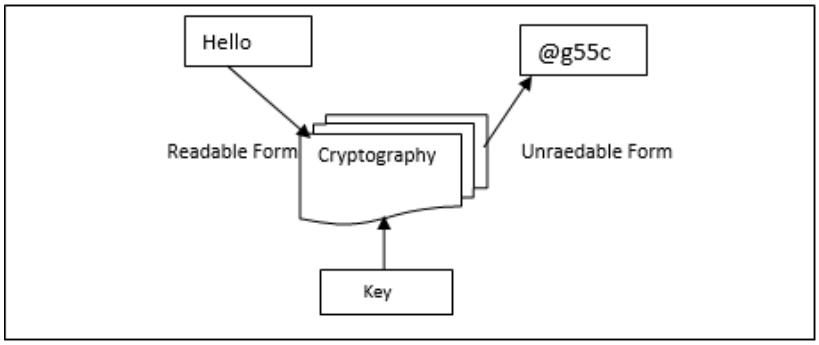

Fig. 2 Cryptographic System

It sends the data with security. Cryptography attains the following objectives

- Authentication
- Privacy
- Integrity
- Non-Repudiation
- Access Control

1) Authentication*:* It assures the identity of sender that the information coming from sender is really an authorized sender or not.
2) Privacy: It support the confidentiality of information by assuring that the only authenticate user can access the information rather than anyone else.
3) Integrity: It cheeks the massage length before sending and after receiving so that there is not any change or alteration of message. Alteration of message can be performed only by authorized sender.
4) Non.-Repudiation: Ensure that both sender and receiver cannot deny about sent content.
5) Access control: Only the authenticate media can access the information.
6) Encryptio*n*: the process of converting plaint text is called encryption.
7) Decryption: The process of converting cipher text again into plain text is called decryption.
8) Key: Key plays a very important role in cryptography. Key is just a piece of information that is used to encrypt or decrypt the data. Various algorithms use different keys. The size of key is also depending upon algorithm because different algorithm uses different size of key. The security of algorithm depends upon the length of key.

Cryptography can be fall under three categories

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Hash Function

1) Symmetric Key Cryptography: In this cryptography only a single key is used for encryption as well as decryption. Before encrypt the message key is send to intended receiver and then sender encrypt the message with key and send it over transmission media. Now receiver receives the encrypted message and decrypts it with the same key. It is also known as Secret Key Cryptography.
2) Asymmetric Key Cryptography: This type of cryptography two different keys used for encryption and decryption. Every sender and receiver has pair of keys known as public and private keys. Private Key is not shared with anyone while public key is shared with sender. Sender encrypts the message with its public key and sends to receiver. The receiver receives the message and decrypts it with its private key. This technique is also known as public key.
3) Hash function: The Hash function provides the integrity of message. Rather than key only fixed length of Hash function is used. The length of Hash function is decided by plain text. It checks the damage of message

II. RELATED WORK

In this phase we are briefly describing the research work of some researcher in the same area.

A. Akanksha Mathur" An ASCII value based data encryption algorithm and it Comparison with other symmetric data encryption algorithms" 2014 [1]

This paper purposed an encryption algorithm based on ASCII values of plaint text. It calculates the ASCII values for data that is to be encrypted. The algorithm uses a single key for both encryption and decryption. The key is modified and change into other string and then changed key is used for both purposes.

The special thing about this algorithm is that the length of plain text and length of key should be same which a limitation in this method is.

B. Daundkar Anita Mohan, Pratima Bhati"Improving Image compression system by Random Permutation" 2014 [2]

The given method encrypts and compresses the images. It deals with three phases: image encryption, compression and decryption. In this first image is encrypt using random permutation and then compression is done by using arithmetic coding.

It can be consider for both lossless and lossy compression.

C. Pratibha S.Ghode, Abha Gaikwad"A keyless approach to lossless image encryption" 2014 [3]

The algorithm provides lossless encryption of image. The method follows SST (Sieving, Shuffling and Transformation) approach for encryption. The input image is divided into pixels and every pixel got encrypted using SST Technique. It gave good quality of output image. It is a secure and efficient technique in image encryption.

D. Jiantao Zhou, Xianiming Liu, Yuan Yan Tang "Designing an efficient image encryption then compression system via prediction error clustering and random permutation" 2013 [4]

In this paper they design an efficient algorithm for encryption and compression of an image. The technique they have developed can be used for both lossless and lossy compression. It provides a high level of security by predicting the error domain. They did both the encryption and compression simultaneously. They used arithmetic coding and random permutation to prepare a solid and high security algorithm.

E. Ci-Lin Li, Chih-Yang Lin, and Tzung-Her Chen "Efficient compression-Jointed Quality Controllable scrambling method for H.264/SVC" 2014 [5]

In this study, a quality controllable encryption scheme is proposed. This scheme shows that the computation and compression overheads are negligible since only the sensitive data, including motion vector difference, the intra prediction mode, and the residual coefficients, are encrypted. According to this, the proposed encryption scheme provides high security, low computational cost, low bit-rate overhead, and smooth compatibility. The encrypted H.264/SVC can transmit the suitable bit stream to appropriate users on a heterogeneity network.

F. Amit Pande, Prasant Mohapatra, Joseph Zambreno," Using Chaotic Maps for Encrypting Image and Video Content" 2011[6]

This paper focus on a novel scheme to efficiently secure variable length coded (VLC) multimedia bit streams. The proposed scheme employs code word diffusion and content based shuffling techniques to achieve security. The main idea of this encryption scheme is to make the decoding of the VLC codes in the bit streams computational infeasible in the absence of a private key. Here the contents are divided into random size blocks. Within each block, a few bits are flipped such that the correlation present among codeword is diffused. Next the blocks are randomly shuffled.

G. M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki," A Modified AES Based for Image Encryption" 2007 [7]

A brief introduction of AES algorithms is presented in this paper. With the AES algorithm of video encryption, a novel algorithm classification is discussed. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits

H. Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data" 2012 [8]

In this study cryptography based Blind image watermarking technique presented that can embed more number of watermark bits in the gray scale cover image without affecting the imperceptibility and increase the security of watermarks. By using watermark nesting we can embed more number of bits in the cover image as compare to without watermark nesting. Due to nesting feature we can embed some metadata about watermark also.

I. Kalyani G. Nimbokar, Dr. M.V.Sarode" Clustering and Permutation Based Image Encryption and Compression System" 2015 [9]

In this paper they design an algorithm for encryption and compression. Image encryption can be done using random permutation and combination. It is useful in compressing the encrypted data. They study both ETC and CTE here.

J. 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" 2000 [10]

They present a method of image encryption using a combination of no. of image encryption algorithms. Chaotic and RGB methods used to prepare the image and then 2 times encryption is done using modified DES.It give high level of security and posses a good speed.

K. Shuqun Zhang and Mohammed A. Karim, "Color image encryption using double random phase encoding" 1999 [11]

The paper introduces a technique for image encryption using a combination of image transformation and encrypted technique. It uses image shuffling and minimizes correlation. After this step double encryption is performed.

L. Mohammad Ali Bani Younes and Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" 2008 [12]

They purposed an algorithm used to encrypt color images. First the color image converted into grey scale image and then encoding is performed. Encoding can be done in 2 phase mask-input plain and Fourier plain. At decryption grey images again changed into RGB format.

M. K.C. Ravishankar, M.G. Venkateshmurthy "Region Based Selective Image Encryption" 2006 [13]

The proposed method helps to encryption of image at a selective level. It encrypts only the selected portion of image not whole image, for encryption the image is divided into fixed size blocks or regions. These regions processed independently. Similarly decryption is also performed on only that portion which is encrypted rather than whole image. It is good choice to save the encryption time and reduce complexity.

N. Riyaz Sikandar Kazi, Prof.Navnath Pokale"Secure image transfer using Clustering and permutation based approach" 2015 [14]

In this paper the image encryption and compression using permutation. In this approach, the input image is divided into small boxes. These boxes are generating by using clustering method. After this step encryption is applied on selected cluster. At the end compression is performed efficiently.

O. Parveen Kumar, Maitreyee Dutta"Image encryption using prediction error K-mean clustering and cyclic permutation" 2015 [15]

This paper purposes encryption of image using K-mean clustering and cyclic permutation. It is a fast and easier method to provide a good level of security.

III. CONCLUSION

In this paper many algorithms are given to perform the encryption on images. Encryption is a sub part of cryptography. Using encryption we can secure our data transmission. Different algorithm has different performance. Some gives good speed but not efficient and some provide efficiency but low level of security. Every algorithm has its own merits and demerits.

On studied the all research paper we can conclude that the selection of particular algorithm can be made on the basis of various data types because every algorithm works on some special type of data. For security complex algorithms should be used while chaos based scheme can be use for multimedia data.

REFERENCES

[1] Jiantao Zhou, Xianiming Liaoyuan Yan Tang,(2014).Designing an efficient image encryption then compression system via prediction error clustering and random permutation, IEEE, transaction on information forensic and security vol.9.no.1.january 2014.
[2] Daundkar Anita Mohan, Pratima Bhati,(2014).Improving Image compression system by Random Permutation, International Journal of advanced Research in Computer Science and software and Engineering, ISSN : 2277 128X, Vol. 4,Issue 11, Nov 2014
[3] Pratibha S.Ghode, Abha Gaikwad,(2014.)A keyless approach to lossless image encryption International Journal of advanced Research in Computer Science and software and Engineering, ISSN : 2277 128X, Vol. 4,Issue 5, may 2014
[4] Akanksha Mathur, (2012).An ASCII value based data encryption algorithm and its compression with other symmetric data encryption algorithms, International Journal on Computer Science and Engineering, ISSN: 0975-3397, Vol. 4 No. 09 Sep 2012
[5] Ci-Lin Li, Chin-Yang Lin, and Tzung-Her Chen,(2011). "Efficient compression-Jointed Quality Controllable scrambling method for H.264/SVC, international Journal of network security Vol.16, 2014
[6] Amit Pande, Prasant Mohapatra, Joseph Zambreno,(2011). Using Chaotic Maps for Encrypting Image and Video Content, IEEE, International Symposium on Multimedia, 2011
[7] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki,(2006). A Modified AES Based for Image Encryption, World Academy of Science, Engineering and Technology, 2007
[8] Preeti Gupta, (2012). Cryptography based digital image watermarking algorithm to increase security of watermark data, International Journal of Scientific & Engineering Research, Vol. 3, and September 2012.

[9] Kalyani G. Nimbokar,Dr. M.V.Sarode,(2015).Clustering And Permutation Based Image Encryption And Compression System, international journal of research in advent technology,ISSN:2321-9637,march 2015
[10] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan , Dai Wei-di,(2009).Digital image encryption algorithm based on chaos and improved DES,IEEE,international conference on system, man and cybernetics,2009
[11] Shuqun Zhang and Mohammed A. Karim,(1999).Color image encryption using double random phase encoding ,microwave and optical technologies Letters Vol. 21, No. 5, 318-322 , June 5 1999
[12] Mohammad Ali Bani Younes and Aman Jantan,(2008).“An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption ,international journals of computer science and network security,vol.8,april 2008
[13] K.C. Ravishankar, M.G. Venkateshmurthy, (2006).Region Based Selective Image Encryption, 1-424-0220-4/06 ©2006 IEEE
[14] Riyaz Sikandar Kazi,Prof.Navnath Pokale,(2015).Secure image transfer using Clustering and permutation based approach,International Journal of advanced Research in Computer engineering and technology, ISSN : 2378-1223, Vol. 4,Issue 6, June 2015
[15] Parveen Kumar,Maitreyee Dutta,(2015).Image encryption using prediction error K-mean clustering and cyclic permutation “international journal of advance research in computer science and management studies” ISSN : 2321-7728, Vol. 3,Issue 4, April 2015