Study of Image Based Cryptography Techniques and Security Facilities

Swati[1] Reecha Sharma[2]
[1]M.tech student [2]Assistant Professor
[1,2]UCOE, Punjabi University, Patiala(Pb)

Abstract— Network security in today's world is an important issue among all who share their important images via internet. This security is possible by cryptography. Cryptography, a word with Greek origin means "secret writing". Cryptography is an art of hiding data and transforming messages or images to make them secure and immune to attacks. Cryptography mangles the images. This can be done by so many methods and techniques. Cryptography offers many types of security facilities to send data on insecure channel. Basically, this paper proposing the techniques of cryptography of images which have been used till and security services offered by cryptography.

Key words: cryptography, services, cryptography techniques.

I. INTRODUCTION

Secured data transfer in real world is still a major challenge. Nowadays, mostly data is sent through internet which means open sharing of data through wireless channel. Therefore, it is more threat to data that it can be leaked or moved to any wrong user. Data confidentiality is necessary in almost all type of communication fields like military, space communication, etc. Images sent must be secured and it can be done by using cryptography. Cryptography is an art of hiding data and transforming images to make them secure and immune to attacks. Cryptography of images is more difficult due to high correlation between the pixels of an image.

Cryptography is completed in two steps i.e. encryption and decryption. Original or plain text is converted into cipher text via encipherment or encryption. The reverse process of converting ciphertext into plain text is called decipherment or decryption. Encryption and decryption is done with the help of key which is like password[1].

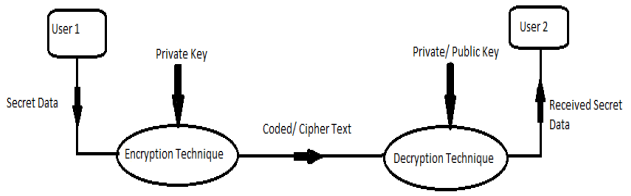

Fig. 1: Basic Cryptographic Model

II. CRYPTOGRAPHIC TECHNIQUES

There are many methods or techniques by which cryptography is done.

A. According to key used[6]:

1) Symmetric Key Cryptography:

It is also called secret/ private key cryptography in which only one key is used for encryption and decryption both means key is shared.

2) Asymmetric Key Cryptography:

It is also called public key cryptography. Two keys private key and public keys are used for encryption and decryption. Sender announced the encryption key in public and used different key called private key for decryption. But symmetric key cryptography is more used for longer messages than asymmetric because of its efficiency.

3) Hash function:

it is also called one way encryption technique. This method is used to preserve the integrity of message. Hash function is an encrypted algorithm which convert original message to compressed image called message digest and message digest needs to kept secret.

B. According to Ciphers:

1) Traditional Ciphers[6]:

These are character oriented and having types

Substitution Ciphers: In this, one pixel value is replaced by another different pixel value. If one pixel value is replaced always to same value in each time of occurrence then it is called mono pixel. If each pixel is replaced with different pixel in each time of occurrence then it is called polypixel cipher.

Transposition Cipher: In this, locations of pixels will be changed but the values remain same. Reordering of pixels is done in such a way to render the image unreadable without knowing how to reorder the letters.

Permutation Cipher:In this type of cipher, key length has to be chosen which is denoted as 'n' and permutation of numbers 1,2……,n Suppose if n=4 and permutation would be 3 2 4 1.

Plain text: myna meisasha

Cipher text: nyamiesmhsaa

In each block of 4, we place 3rd plaintext character 1st in cipher text and so on

2) Modern Ciphers[6]:

These are bit oriented and of many kinds like

XOR ciphers: this is also called one time pad. In this, plaintext and key is xored and size of input image, key and cipher text are all same.

Rotation Cipher: In this, bits are left or right rotated and it can be keyed or keyless

Block Encryption: It is a method of encryption text in which key is applied to block of data at a time rather than one bit at a time

C. According to Existing Cryptographic Standard[5],[6]:

1) RSA(Rivest Shamir and Adleman:

It is asymmetric key algorithm so uses one private and one public key. It chooses prime large numbers as private and public key and calculates the ciphertext and then decipher the code by RSA algorithim. RSA is very slow if the message is long so suitable only for small messages.

2) DH(Diffie Hellman):
It was designed for key exchange. In this, two parties create a symmetric session key to exchange data without storing the key for future use. Two parties create secret key in three parts and first part is public and other two parts are added by two parties secretly to complete the session key. DHA was good algorithim but the main drawback is lack of authentication between two parties. Due to absence of this authentication, man in the middle attack occurs and the message can be changed by middle attacker by changing the key. This is known as Bucket Brigade Attack.
3) DES(Data Encryption Standard):
It is a symmetric key technique. DES is a conventional cryptosystem means one key is used for encryption and decryption. It is a 64 bit block cipher method which explain that 64 bit data encrypted at a time rather than single bit. But it was easily breakable technique for brute force attack due to its small size. It is based on Fiestal block cipher.
4) AES(Advanced Encryption Standard):
It is an advanced technique of DES and it was designed because DES is very small. AES encrypt the 192 and 256 bits of data at a time. AES is secure enough to protect information means had intense security.
5) Blowfish:
Blowfish is symmetric key based block cipher algorithim used for encryption of data. It works on 64 bit block size and uses variable length key from 32 bits to 448 bits. Blowfish is basically a Feistel Network means it transform any function into permutation. Blowfish uses 16 round Feistel Network. Each round contains a key dependent permutation and key dependent substitution. Blowfish is suitable where key change does not needed oftenly[1].
6) SHA(Secure Hash Algorithim):
It is used to create a message disget of any size input message so it is only one way cryptography. It has many types like SHA0, SHA1, SHA2, SHA3 etc. according to the the output bits size. For example, SHA0 change input message to 160 bit message digest and SHA2 changes to 256 and 512 bits message digest with different block size also.

D. According to Decryption of images:

1) Lossless Cryptography:
In this type of technique, when decryption is done then any type of distortion or change in input image is not tolerable and decrypted image is vulnerable to distortion. It preserve each and every single detail of an image.

2) Lossy Cryptography:
In this type of encryption technique, decrypted image is distorted in some manner and this kind of technique is used in applications where high image details are not required.

III. SECURITY FACILITIES BY CRYPTOGRAPHY[7]

Cryptography has several applications in security in almost all filed of communication. Cryptography provides many security services or facilities including:

(1) Authentication: Authentication means confirming to reality and therefore worthy of trust of the claimed source means receiver should be sure of sender's identity.
(2) Data Confidentiality: Cryptography offer this facility in which the data will be protected from unauthorized user means it should only understood to the receiver. For all other, it should be garbage.
(3) Integrity: This service guarantees that message is received in the same form as it is sent. There should be no kind of change or manipulation in data.
(4) Non Repudiation: By this facility, receiver or sender cannot deny of receiving or sending of messages.
(5) Access Control: This will limit the access only to authorized user that any unauthorized usercan't access the sent data.
(6) Availability: This service should guarantees that all services are always available when needed.

IV. CONCLUSION

In this paper, various types of exsistingcryptographic techniques are studied and showed there comparison in terms of performance and security services offered by cryptography are discussed.

REFERENCES

[1] TaranjitKaur and Reecha Sharma, " Voluminous Amount of Cryptographic Methods and Cryptographic Attacks" , International Journal of Engineering Sciences and Emerging Technologies, vol. 6, Issue. 1, pp: 113-119, August 2013.

[2] Gamil R.S Qaid and Sanjay N. Talbar, " Encryption and Decryption of Digital Image Using Color Signal", IJCSI, vol.9, Issue 2, March 2012.

[3] TaranjitKaur and Reecha Sharma, " Image Cryptography by TJ-SCA: Supplementary Cryptographic Algorithim for Color Images" , International Journal of Scientific & Engineering Research, vol. 4, Issue.7, July 2013.

[4] Ki-Hyun Jung, Keum-Sook Ha and Kee Young Yoo, " Data Hidong In Binary Images by Pixel value Weighting" , International Confrence on Convergence and Hybrid Information Technology, 2008

[5] Lini Abraham and Neenu Daniel, " Secure Image Encryption Algorithim: A Review" , International Journal of Scientific & Technology Research, vol.2, Issue. 4, April 2013.

[6] Behrouz A. Forouzan, " Data Communication and Networking", Genuine Tata McGraw Hill, 2nd edition.

[7] TaranjitKaur and Reecha Sharma, " Security Definitive Parameters for Image Encryption Technique" , International Journal of Emerging Technology and Advanced Engineering, vol.3, Issue. 5, May 2013.

[8] Komal D Patel and SonalBenali, " Image Encryption using Different Techniques: A Review" , International Journal of Emerging Technology and Advanced Engineering, vol.1, Issue.1 , pp: 30- 34, November 2011.

[9] Brain Candler and Hervey Allen, " Cryptographic Methods".

[10] MohiniChaudhari and Dr. KonakSaxena, " Fast and Secure Data Transmission using Symmetric Encryption and Lossless Compression", IJCSMC, vol.2, Issue.2, pp: 58-63, February 2013.

[11] Pascal Lafour Cade, " Security and Cryptography just by Images", 2009

[12] Chih-Hsu Yen and Bing-Fei Wu, " Simple Error Detection Methods for Hardware Implementation of Advanced Encryption Standard" , IEEE Transactions on Computers, vol. 55, No. 6, June 2006.

[13] Kevin Allison, Keith Feldman and Ethan Mick, " Blowfish".

[14] Michael Pace, "DSS: Digital Signature Standard and DSA Algorithim".

