ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

A Survey On: Reversible Data Hiding and Image Hiding Using Encryption Technique

Pradnya Mandlik[1], Samruddhi Mhatre[2], Samiksha Niwal[3], Priti Mithari[4]

B.E, Dept. of Computer Engineering, Dr.D.Y.Patil Institute of Engineering &Technology Ambi, Pune, India[123]

Dept. of Computer Engineering, Dr.D.Y.Patil Institute of Engineering &Technology Ambi, Pune, India[4]

ABSTRACT: Nowadays, with the speedy development of information technology more images and data are available on the internet. Hence there is a need to have some kind of authentication to that data. Data is information that is translated into a form that is more convenient to move or process, so we can secure the transmission of data with the help of cryptography. Data hiding phenomena is defined as a scheme that allows complete and blind restoration of the original host data. Steganography is the act of secreting information in approximately else. Steganography is favourable over encryption because encryption only hides the meaning of the information; steganography hides the very existence of the information. Steganography and watermarking take a variety of very important techniques how to hide important information in an undetectable and immovable way in audio and video data. Steganography and watermarking are main parts of the fast developing area of information hiding.

KEYWORDS: Data Hiding, Cryptography, Steganography, Linear Feedback Shift Register (LFSR), Watermarking.

I. INTRODUCTION

Data is extracted from and image by using Reversible Data Hiding techniques while data, is extracting from image after get image as it is without looking its original features for data hiding use stenography also, but in most case some distortion occur and if cannot be restored back to its original media. Reversible Data Hiding (RDH) provides the exact image after extraction of data and improved that image into original form. If user wants to send an image through internet them he has to encrypt that image before sending through net. Reversible data embedding can be used as information. As the difference between the embedded image and original image is almost invisible from human eyes, reversible data embedding could be assumed as a hidden communication channel. By embedding its message verification code, reversible data embedding provides a true identity verification order, without the use of metadata. Reversible Data embedding it is also Called Lossless Data Embedding. Cryptography, Steganography, Linear Feedback shift Register (LFSR) are the most powerful technology for hiding data.

Cryptography is a technique of embedding and decoding the messages, so that they cannot be understood by anybody except the sender and intended recipient. Cryptography having mainly two types a) Secret key Encryption b) Private Key Encryption. Linear Feedback Shift Register (LFSR) is constructed using D-type flip-flops and OR gate. While providing security key at the time of encrypting image security of that key is very less, so to improve the security of the key uses LFSR. LFSR is a pseudo random number generator. The Random no generated through LFSR code repeat itself 2n-1. With the help of LFSR we can generate good Key stream. Steganography is the process of privately embedding information into a data source in such a way its very existence is covered. The main goal of steganography is to hide a message in various audio or video data, to form new data. Steganography methods usually do not need to provide strong security against eliminating or variation of the hidden message. It is also often said that the goal of steganography is to cover a message in one-to-one communications.

Watermark is a “secret message” “hide message”. Digital watermark is an obvious or perfectly unobvious, identification code that is permanently embedded in the data and always present within the data after any decryption process. A digital signal or pattern executed on a digital document such as text, graphics, multimedia presentations, etc. Watermarking having some of techniques as follows:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

1. Text – Varying spaces after punctuation, distances in between lines of text, spaces at the end of sentences, etc.

2. Audio – Low bit coding, random.

3. Images / Video – Least-significant bit, random.

Today security is the major concern in the Internet as the information contained within the packets that are forwarded over the network are more likely to be hack by the hackers.

II. RELATED WORK

While embedding data some distortion is get created so this optimal balance between the amount of an information and the induced distortion get studied in [3] in this Reversible Data Hiding (RDH) technique use with the help of RDH remove the distortion of data.

1. *Data:* -Data is nothing but collection of information that has been translated from source to destination using secure network.

2. *Data Hiding:* -Data Hiding is concept in which the information of any message is hided for security purpose using different techniques like Reversible Data Hiding (RDH), Cryptography, Steganography, Linear Feedback Shift Register (LFSR), and Watermark. In Fig. Data Hiding With the help of Encryption shows that the Sender sends a input message to the receiver and hides the contents of that messages with the help of encryption. The messages are encrypted with the help of encryption key for receiving that encrypted message receiver has to decrypt messages by using decryption key and recovered the original message. Data hiding provides assurance of content integrity and proves of copyright [3]. Technique used for data hiding depends on quantity of data being hidden. Data hiding is nothing but the class of processes used to embed data[8]. The embedded data should not be visible to human observer. To maintain the integrity of data error correction coding should be used. Data Hiding is used for Copyright Protection, Content Authentication, Labeling and monitoring, secret communication, Error protection.

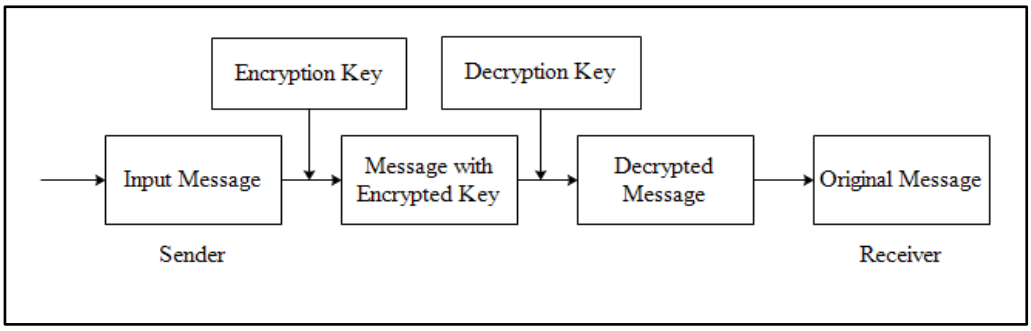

FIG.1. DATA HIDING WITH THE HELP OF ENCRYPTION

3. *Cryptography:*-Cryptography hides the contents of the message from an attacker, but not the existence of the message. Cryptography is a technique of encrypting and decrypting image so that it is invisible to other user except sender. Encryption is nothing but the encoding of message. Sender sends the message in the form of plain text by using method of encryption plain text is converted into cipher text. That cipher text travels through the network. When it reaches to the receiver it decodes that message this process is called as Decryption [2]. Cryptography having mainly two types of schema:- Secret key Encryption and Public Key Encryption.

Symmetric key Encryption is a secret key encryption. Only one key is used for encryption and decryption. This approach is used by Data Encryption Standard (DES). Key agreement and distribution are the disadvantages of cryptography. Public key Encryption is multiple key encryptions. Different key are used for

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

encryption and decryption, one of the two keys known as a public key and other key is private.Cryptography was used to assure only secrecy.

4. *Steganography:* - The process of secretly coding information into a data source in such a way its very existence is covered. Steganography bring a variety of very important techniques how to hide important information in an undetectable and immovable way in audio and video data. The goal of steganography is to hide a message in one-to-one communications. Steganography even hide the very existence of the message in the communicating data. Steganography provides potential capability to hide the existence of confidential data attaching stegano file to an image Steganography is used for confidential communication and secret data storing, Protection of data alteration for digital content distribution and media database system.Steganography is one such pro-security innovation in which secret data is embedded in a cover

5. *LFSR (Linear Feedback Shift Register):- LFSR* is string key generated. LFSR generate pseudo random number generated using LFSR we can provide more security by using LFSR rather than other Galois field. The LFSR code is additional information to our data. Data hiders have to hide LFSR code into the data. LFSR is easy to construct and implement. It consists of shift register and linear feedback function. LFSR are used for Data Encryption Standard (DES) cracker, generating pseudo random number generator.

6. *Watermark:* - Watermark is a "secrete message" that is embedded into a "cover message". The purpose of watermarking is to hide the data in one-to-many communications [5]. Watermark is used for various purposes like copyright protection, source tracking, broadcast monitoring, video authentication, software clipping etc.
Attacks on Watermarking are: Unintentional and Intentional.

1. *Unintentional:* -All image handlings commonly used to prepare images for print publication.For example: Resizing, rotation, sharpening, contrast modification, compression, etc.

2. *Intentional:* -All the well-known intentional attacks include: changing, embedding new watermark, etc.

Intentional Watermark Attacks:-

1. *Active Attacks:* - An attack in which hacker attempts to make some changes on the data. Hacker tries to remove the watermark or make itinvisible. Applying Geometric transformation: rotation, scaling, translation, change aspect ratio.
For example: - Active attacks are masquerade attacks, session replay attack.

2. *Passive Attacks:* -In passive attack system observe and scan for the open ports and gain information on the data. Hacker tries to break the system individually. These attacks very difficult to find out because there is no alteration of the data.
For example:-A passive attack on a cryptosystem.
3. *Collusion Attacks:* -In this attack there is an agreement between two or more parties, some time that agreement may be faulty. So that attack is nothing but the collision attack.
For example: - Collision attacks on cryptography hash that tries to find to inputs and calculate separate result for that inputs.

III. CONCLUSION

The concept of data hiding concludes that how to hidden confidential data from the hackers or unauthorized person. With the help of cryptography by using the concept of encryption and decryption information of secret messages are hidden. LFSR is good key stream generation, so provide more security to data. In LFSR technique receiver must know encryption as well as data hiding key. So receiver extracts the knowledge from encrypted image. Cryptography shows how to encrypt and decrypt the data by using secret and private key. Large attacks takes place over multimedia, using watermarking technique those attack will be avoided. Steganography and cryptography provides one to one communication between sender and receiver for hiding the data. Steganography is a high security technique for the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

large data transmission. Steganography is used for transmitting large amount of data. Active attacks, Passive attacks and Collusion attacks can be sort out by using watermarking.

ACKNOWLEDGEMENT

The authors would like to thank the publishers, researchers for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure support. Finally, we would like to extend heartfelt gratitude to friends, family members.

REFERENCES

[1] Kede Ma, Weiming Zhang, XeianfengZhao,"Reversible data hiding in encrypted images by reserving room before encryption" IEEE Trans. On information forensic and security, March 2014.
[2] Meng Zhang, AnandRaghunathan ,Niraj K. Jha, "Trust worthiness of Medical Devices and Body Area Networks" , August 2014.
[3] W. Zhang, B. Chen, and N. Yu, Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans. Image Process, 2012.
[4] W. Zhang, B. Chen, and N. Yu, Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding (IH'2011), LNCS 6958, 2011, pp. 255-269, Springer-Verlag.
[5] L.Luoet al., "Reversible image watermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.
[6] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Mar. 2007
[7] Xinpeng Zhang, "*Reversible Data Hiding in Encrypted Image*", IEEE Signal Processing Letters, vol.18, No.4, April 2011.
[8] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.
[9] Xiaolong Li, Bin Yang and Tie yongZeng, "Efficient Reversible Watermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection", IEEE Transaction on Image Processing, Dec 2011.

BIOGRAPHY

.

Pradnya P. Mandlikis a B.E student in the Computer Engineering Department, Dr. D. Y.Patil Institute of Engineering and Technology, Ambi, Talegoan, Pune, SavitribaiPhule Pune University

Samruddhi S. Mhatreis a B.E student in the Computer Engineering Department, Dr. D. Y. Patil Institute of Engineering and Technology, Ambi, Talegoan, Pune, SavitribaiPhule Pune University.

Samiksha M. Niwalis a B.E student in the Computer Engineering Department, Dr. D. Y. Patil Institute of Engineering and Technology, Ambi, Talegoan, Pune, SavitribaiPhule Pune University.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Priti M. Mithari, received M.E. in Computer Engineering from Computer Department of RMD Sinhgad School of Engineering, Warje, Pune. from Pune University (2014). She is also working as an Assistant Professor in the department of Computer Engineering in Dr. D. Y. Patil Institute of Engg. & Technology Ambi, Pune, India from Pune University (2015).