ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)
Vol. 2, Issue 1 (Jan. - Mar. 2015)
International Journal of Advanced Research in Education Technology (IJARET)

Literature Survey on Several Data Hiding Techniques

[I]Shreya M S, [II]Sandeep Kumar S
[I]M.Tech Student, [II]Assistant Professor
[I,II]Dept. of CSE, Mangalore Institute of Tech. and Engg., Mangalore, Karnataka, India

Abstract
Nowadays digital communication has become an essential part of infrastructure. A lot of applications are internet-based and it is important that communication will be made secret. As a result, the security aspect of information passed over an open channel has become a fundamental issue and hence, the confidentiality and data integrity are required to protect against unauthorized access and use. This has led to an unstable growth in the field of information hiding. Cryptography and steganography are the two popular methods available to provide security. Using cryptography, the data is transformed into some other gibberish form and then the encrypted data is transmitted. In steganography, the data will be embedded in an image and that image will be transmitted. In this paper the focus on different techniques that are existing, for steganography and comparative study all the techniques together as a literature survey. This paper will also propose a new method for embedding the data inside the image and the advantages of this technique over the previous existing techniques.

Keywords
Cryptography, Feedback shift, MLSB, Ordinal Virtual Embedding, Reversible Data Hiding, Steganography, Separable Reversible Data Hiding.

I. Introduction

Computer and the internet are major communication media that connect different parts of the world as one global virtual world in this modern era. As a result, people can exchange information easily and distance is no longer a barrier to communication. Perhaps, the safety and security of long-distance communication will be an issue. This is indeed important in the case of confidential data. The solution for this problem has led to the development of steganography schemes.

Steganography is a very powerful security tool that provides a higher level of security, in particular when it is combined with encryption. Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Cryptography scrambles a message so that it cannot be understood; the Steganography hides the message so it cannot be seen. Even though both the techniques provide security, a research is made to combine both cryptography and Steganography methods into one system for better confidentiality and security.

A. Cryptography and Steganography

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and the receiver have, whereas public-key systems that use two keys, a public key which will be known to everyone and a private key that only the recipient of messages uses [1]. Commonly used terminologies in cryptography are: 1.Plain text 2.Cipher text 3.Encryption 4.Decryption 4.Key.

The word steganography comes from the Greek Steganos, which mean secret or covered and graphy means writing or drawing. Hence, steganography means, covered writing. The aim of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. There exist two types of materials in steganography they are message and the carrier. Message will be the secret data that will be hidden and the carrier will be the material that will take the message in it.

Watermarking and fingerprinting related to steganography are typically used for protection of the intellectual property. A digital watermark is a type of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is normally used to identify ownership of the copyright of such signal. The embedded information in a watermarked object is a signature that refers the ownership of the data in order to ensure copyright protection. In fingerprinting technique, different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it will be easy for the property owner to find out such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups.

B. Reversible Data Hiding

Reversible Data Hiding is a technique that hides data in digital images for secret communication. It is a technique used for hiding additional message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. Traditionally, the data hiding technique is used for secret communication of data. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analyzed to reveal the presence of the embedment of data. Other applications could be for when the owner of the carrier might not want the other person, including the data hider, to know the content of the carrier before data hiding is actually performed, such as confidential medical images or military images. Here, the content owner has to encrypt the content before passing to the data hider for data hiding. The receiver can extract the embedded message and recover the original image which was used as cover image. Many reversible data hiding methods have been proposed recently.

Encryption is an effective and popular means for providing privacy. In order to securely share a secret image with other person, a content owner will encrypt the image before transmission. It may be also expected that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. Hence a reversible data hiding scheme for encrypted image is desirable.

Data hiding is referred to as a process to hide data (representing

some information) into cover media. The data hiding process links two types of data, one a set of the embedded data and another set of the cover media data. In several cases of data hiding, the cover media will be distorted due to data hiding and cannot be inverted back to the original media. Means, cover media has permanent distortion even after the hidden data have been removed. In some applications, like medical diagnosis and law enforcement it is desired that the original cover media can be recovered efficiently with no loss. The techniques satisfying this requirement will be referred to as lossless, reversible, invertible, distortion-free or data hiding techniques [2].

C. Separable Reversible Data Hiding

As the name indicates that it is the reversible data hiding technique but which is separable. The separable means that the information hidden can be separated using suitable criteria. The activities that can be separated are extraction of original cover image and extraction of original data which was embedded. This separation exists based on the keys available. At the receiver side, three different cases are encountered viz., if encryption key is available, get the original image, if data extraction key is available, get the original data and if both the keys are available, get both data and the image. Hence it is called as Separable Reversible Data hiding.

II. Steganography Overview

Depending on the cover media steganography can be divided into 5 types [3]. They are

1. Text Steganography: Hiding information in text file is the most common method of steganography.
2. Image Steganography: Images are used as the popular cover medium for steganography. A secret message is embedded in a digital image using an embedding algorithm, using the secret key and sent to the receiver. On the other side of the communication system, it is processed by the extraction algorithm using the same key.
3. Audio Steganography: Audio steganography is concerned with embedding information in an innocuous cover speech in a secure and robust manner. Existing audio steganography software can embed messages in WAV and MP3 sound files.
4. Video Steganography: It is a technique to hide any find of files in any extension into a carrying Video files.
5. Protocol Steganography: The term protocol steganography is to embedding information within network protocols such as TCP/IP. Information is hidden in the header of a TCP/IP packet in some fields that can be either optional or are never used.

Steganographic techniques that modifies the image for hiding information includes following techniques or the domains: [4,5,6]

1. Spatial Domain
2. Transform Domain
3. Distortion Techniques
4. Statistical
5. Cover Generation

III. Related Work

A. Xiaoping Liang [7]

This author has proposed a reversible watermarking scheme for image authentication based on histogram modification in integer wavelet transform (IWT) domain. Proposed RAW (Reversible Authentication Watermarking) scheme utilizes the space-frequency localization of IWT, and combining a bi-level image and hashes on IWT coefficients to discern and localize tamper originally done in spatial or frequency regions. Proposed method also uses the statistical property of coefficients in high frequency sub-bands of IWT to ensure enough reversible embedding capacity. In the proposed method verification is performed before reconstruction of the original image. The proposed RAW scheme is practical and effective, and can be applied to strict content integrity authentication system in law, commence, defense, and journalism.

B. Vivek Jain, Lokesh Kumar, Madhur Mohan Sharma, Mohd Sadiq, Kshitiz Rastogi [8]

This paper proposed a technique to implement steganography and cryptography to hide the data inside the image. Here the original data will be encrypted by the stego key which is generated and shared by using Diffie Hellman key exchange protocol. Using the same stego key, some pixels are selected for hiding the encrypted data. From the selected pixel its LSB is taken for hiding the data. At the receiver side the shared stego key will be used to select the pixels where the data is embedded. Then extract the data which is encrypted using the key. Here based on the key shared the pixels will be selected. So if any intruder gets the stego image without the key will not know which pixel will be selected for data embedding. Thus it will ensure more security to the embedded data.

C. Divyani UdayKumar Singh, Kasturi Mohan Padwal, Madhura Pundlik Jadhav [9]

In this the authors proposed a new method for embedding the data into the image. Here sender will encrypt the data using AES algorithm, hides encrypted data in the image using LSB technique and then the system will auto generate the hide key. Sender will send the file with the help of mailing system. Receiver can retrieve the data based on the keys available. If he has only data hiding key then he can get only the original image. If he has the data hiding key and decryption key then he can get original data. All operation is done by proper login process. The system will generate fake data when unauthorized user tries to login. This proposed system will provide high security by providing access to only authenticated users and generating a fake data for the unauthorized users.

D. Guorong Xuan, Chengyun Yang, Y. Q. Shi, Yizhan Zheng, Zhicheng Ni [10]

This paper presents a reversible data hiding method based on wavelet spread spectrum and histogram modification. Using the spread spectrum scheme, the data is embedded in the coefficients of integer wavelet transform in high frequency sub-bands. Here pseudo bits are also embedded which will enhance data hiding efficiency. To prevent overflow and underflow an efficient histogram modification method is developed and it is used. Performance in terms of data embedding capacity and visual quality of marked image was high when compared to existing method.

E. C.Anuradha, S.Lavanya [11]

This paper presented a new secure and authenticated discrete reversible data hiding in cipher images deals with security and authentication. Here the content owner will encrypt the image with encryption key. The data hider may compress the LSB of the encrypted image for creating a space for embedding the data. The data hider can then embed the data in the allocated space

by using the data hiding key. At the receiver based on the keys available he can get the data or the image. Here only the intended user with particular key can get the particular information. Here both image and data will be useful information. So the security of both image and data will be maintained.

F. Chaithu V Kumar [12]

In this paper the author proposed a novel secure Reversible Data Hiding for encrypted image by conforming space before encryption for embedding the data. In existing system, the data is embedded by reversibly vacating room after the encryption of the cover image, which may make some error in data extraction and/or the restored image. Here the room for data hiding is reserved before encryption and the data is reversibly embedded in the encrypted image. Hence the image recovery and data extraction can be performed without error. In the proposed method the data is also encrypted using data encryption key and during data embedding another key will be used that is data embedding. Here it provides the separation of data extraction from image decryption thus improves the quality of marked image.

G. Naseem, Ibrahim M. Hussain, M. Kamran Khan, Aisha Ajmal [13]

In this paper an algorithm called Optimum Intensity Based Distributed Hiding (OIBDH) was proposed for hiding the secret data inside the image. The OIBDH algorithm is the improvement of Bit Plane Splicing LSB technique. Here the pixel value of the image will be represented using the planes where the lowermost plane will contain the MSB bit of the pixel and highest plane will contain the LSB of the pixel. Movement towards the LSB plane will decrease the information contained in it. In the proposed algorithm the secret data bits are hidden in the LSB plane based on the color intensity of the pixel. Here two ranges of pixel intensity are chosen for embedding the data. In this algorithm the data is hidden in the non-sequential manner and it is dynamic in nature and it is more effective in terms of visual degradation of the cover image and data hiding capacity.

H. Mazen Abu Zaher [14]

In this paper the author proposed a new method for representing the data that will be embedded inside the cover image. Generally, characters of the data will be represented using 8 bits, but the MLSB technique will represent the characters of the data using 5 bits and then the 5 bits can be embedded in to the image using LSB method. Control symbols will be used to indicate the small, capital, number and space and even the control symbols are represented using 5 bits. By doing this a large amount of data can be embedded inside the cover image and the security also will be increased by performing data encryption.

Most of the previous related work has focused on embedding the data inside the image either by transforming the image or using the LSB's of the pixels of the image or changing the statistical properties of the image. So in the existing methods there will be some changes done to the cover image.

In the proposed method a new technique called Ordinal Virtual Embedding will be used where embedding will be done virtually on the encrypted image by extracting the ordinals of pixels who's LSBs match with each bit of the data to be embedded and thus will not modified the encrypted image. It will use the techniques like Separable Reversible Data Hiding [11] and Modified Least Significant Bit (MLSB) [14] along with the proposed algorithm. The proposed method will also be highly secure because the RSA algorithm will be used for key exchanging and when the histogram of the encrypted image and image after embedding the data into it will remain the same.

IV. Conclusion

In this paper, discussion is made on what is cryptography, steganography, reversible data hiding, separable reversible data hiding different. Several Steganographic techniques for embedding the data inside the image are discussed. The Table 1 shows the highlights of related work. But all the related work papers proposed the methods where the cover image will be modified while embedding the data into it. This paper also provides an overview of a new data embedding technique called Ordinal Virtual Embedding which will not perform actual embedding and will proved high security for both data and the image as well.

Table 1: Highlights of the related work

SL. No	AUTHOR	METHOD USED	HIGHLIGHTS
1	Xiaoping Liang[7]	Histogram modification in integer wavelet transform domain	High Embedding capacity, Reversibility, Stream cipher with secret key and hashes are used to improve security
2	Jain, Lokesh Kumar, Madhur Mohan Sharma, Mohd Sadiq, Kshitiz Rastogi[8]	Embedding done on the LSB's of the selected pixels by using the shared key	Diffie Hellman key exchange protocol, data is encrypted using the key, selected pixels are used for embedding
3	Divyani UdayKumar Singh, Kasturi Mohan Padwal, Madhura Pundlik Jadhav [9]	Data is encrypted using AES and is embedded using LSB technique	Encrypt data using AES algorithm, fake data generation if unauthorized access
4	Guorong Xuan, Chengyun Yang, Y. Q. Shi, Yizhan Zheng, Zhicheng Ni [10]	Reversible data hiding method based on wavelet spread spectrum and histogram modification.	Embed data in coefficient of IWT in high frequency sub-band, pseudo bits are embedded for efficient data hiding, high visual quality of marked image

5	C.Anuradha, S.Lavanya [11]	Data embedding ad image encryption based on the key available	For authentication SHA-1 algorithm is used, based on the key available the receiver can get the information, it also has low computational complexity
5	Chaithu V Kumar [12]	Reversible Data Hiding for encrypted image by conforming space before encryption for embedding the data.	Data extraction and image recovery can be done without any error because space for embedding the data will be allocated before encryption which reduce data hiding effort, for secure communication AES and SHA-1 is used, data is also encrypted
6	Naseem, Ibrahim M. Hussain, M. Kamran Khan, Aisha Ajmal[13]	Secret data bits are hidden in the LSB plane based on the color intensity of the pixel	Has low absolute entropy difference compared to Bit Plane Slicing LSB technique, less image degradation
7	Mazen Abu Zaher [14]	Character of data is modified from 8 bit to 5 bit.	Increase the amount of data hiding using LSB, convert data from 8 bit to 5 bit, because of the conversion built-in encryption will take place.

V. Acknowledgment

I am very thankful to my guide Mr. Sandeep Kumar S Assistant Professor, Department of Computer Science and Engineering, Mite for his cordial support, valuable information and guidance, to prepare this paper and also thankful to Prof. Dr. Nagesh H R, Head of the Department, Computer Science and Engineering, for his valuable and constructive suggestions during the planning and development of this work.

References

[1] *E Thambiraja, G. Ramesh, Dr. R. Umarani," A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X.*

[2] *Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, Wei Su, " Reversible Data Hiding", IEEE Transactions On Circuits And Systems For Video Technology, Vol. 16, No. 3, March 2006.*

[3] *Masoud Nosrati, Ronak Karimi, Mehdi Hariri, "An introduction to steganography methods", World Applied Programming, Vol (1), No (3), August 2011. 191-195, ISSN: 2222-2510.*

[4] *Jasmeet Kaur, Nitika Kapoor, Harish Kundra, "LITERATURE SURVEY: Steganography Using Redundant Bit Replacement By Neural Network", International Journal of Computer Science and Communication Engineering Volume 3 issue 1(February 2014 issue).*

[5] *Masoud Nosrati ,Ronak Karimi, Hojat Allah Hasanvand, " Spatial and Transform Domains RDH Methods", World Applied Programming, Vol (2), Issue (6), June 2012. 373-376, ISSN: 2222-2510.*

[6] *Dipalee Borse, Shobhana Patil, "Review and Analysis of Multifarious Spatial Domain Steganography Techniques", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, Vol. 4, Issue 01, January-2015.*

[7] *Xiaoping Liang," Reversible Authentication Watermark for Image", World Congress on Engineering and Computer Science, October 22 - 24, 2008.*

[8] *Vivek Jain, Lokesh Kumar, Madhur Mohan Sharma, Mohd Sadiq, Kshitiz Rastogi," Public-Key Steganography Based On Modified Lsb Method", Journal of Global Research in Computer Science, Volume 3, No. 4, April 2012.*

[9] *Divyani UdayKumar Singh, Kasturi Mohan Padwal, Madhura Pundlik Jadhav," Separable Reversible Data Hiding in Image Using Advanced Encryption Standard with Fake Data Generation", International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 3469-3473.*

[10] *G. Xuan, C. Yang, Y. Zheng, Y. Q. Shi and Z. Ni, "Reversible data hiding based on wavelet spread spectrum," IEEE International workshop on multimedia signal processing (MMSP2004), Sept. 2004, Siena, Italy.*

[11] *C.Anuradha, S.Lavanya,"Secure and Authenticated Reversible Data Hiding in Encrypted Image", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.*

[12] *Chaithu V Kumar," Secure RDH for Encrypted Images by Conforming Space before Encryption", International Journal of Research in Advent Technology, Vol.2, No.2, February 2014.*

[13] *M. Naseem, Ibrahim M. Hussain, M. Kamran Khan, Aisha Ajmal, "An Optimum Modified Bit Plane Splicing LSB Algorithm for Secret Data Hiding", International Journal of Computer Applications (0975 – 8887) Volume 29– No.12, September 2011.*

[14] *Mazen Abu Zaher," Modified Least Significant Bit (MLSB)", Computer and Information Science, Vol. 4, No. 1; January 2011.*

Authors Profile

Shreya M S completed the Bachelor's Degree in Computer Science & Engineering from Visvesvaraya technological University (VTU). Currently pursuing M.Tech degree in Computer Science & Engineering at Mangalore Institute of Technology, Karnataka,India.

Mr. Sandeep Kumar S received Master Degree in computer science and engineering from Canara Engineering College Mangalore. He is currently an Assistant professor in the department of Computer Science and Engineering, Mangalore institute of Technology and Engineering Mangalore, Karnataka India. His research interest area includes Image Processing, Network Security, information Security.