IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 94-98
www.iosrjournals.org

Stegnography Approach in Frequency and Spatial Domain for Secure Communication

Jesmy John[1], Aparna M[2], Dhanya Winson[3]
[1]*(PG Scholar, Embedded System, Sahrdaya College of Engineering & Technology, India)*
[2]*(PG Scholar, Embedded System, Sahrdaya College of Engineering & Technology, India)*
[3]*(PG Scholar, Embedded System, Sahrdaya College of Engineering & Technology, India)*

ABSTRACT: *most recently, significant attention has been given to issues surrounding digital multimedia. With the digital multimedia being transmitted via the Internet, some area have become more important, including copyright protection, modification, multimedia broadcast security, interception, forgery, etc. With the quick development of information and communication technology, transmitting data by the Internet is very capable and convenient. However, it is very dangerous to transmit private information through the Internet without any security. Protecting information while transmitting over the internet has become a very significant issue. A variety of techniques have been proposed to deal with this problem. Nowadays, data hiding techniques are increasingly common for Internet privacy, for instance steganography, watermarking, fingerprinting, and so on. Among this image steganography seems to have a higher hiding capability and it is also visually imperceptible to the human visual system. The goal of stegnography is to hide secret information via some cover media. So that no one can be understood the presence of secret data. In this paper, different approach to stegnography and the necessity of secret communication is explained.*

Keywords—*Cryptography, Distortion profile, steganalysis ,Stegnography, ,stego medium*

I. INTRODUCTION

Steganography is a method of covering key information behind a medium. It is taken from Greek word “STEGANOS” which means “Covered” and “GRAPHIE “which mean “Writing”. So, Steganography is a technique of covering chief information behind a medium [11].It is the art and science of hiding communication; a steganographic system thus embeds hidden content in unexceptional cover media. . Sending secret data under cover-object by using a steganographic method reduces the chance of raising attacks. The information-hiding process in a steganographic system starts by identifying a medium’s redundant bits that can be made to order without destroying that medium’s integrity. When we are modifying the cover medium it will change its statistical features, so eavesdroppers can detect the distortions in the resulting stego medium’s statistical properties. The process of finding these distortions is called statistical steganalysis.so it is the technique to discover the existence of hidden information.

It serves as an improved way of securing information than cryptography which only conceals the content of the message not the existence of the information [12]. The intended secret message does not attract attention to itself as an object of scrutiny. This is the advantage of steganography over cryptography. Cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. Steganography includes the concealment of information within computer files. Cryptography focuses on maintenance the contents of a message secret, but steganography focuses on keeping the existence of a message secret [13]. Both are to protect secret data from others. When the presence of hidden information is exposed, the purpose of steganography is partly defeated. Steganography strength can be enlarged by combining it with cryptography. Other technologies that are closely related to this are watermarking and fingerprinting.

Data hiding has a long history. Messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves in olden days. It has been in use for centuries for fun by children and students. The Microdot technique was developed by the Germans during Second World War. Nowadays steganography is typically used on computers with digital data being the carriers and networks being the high speed delivery channels.

II. IMPLEMENTATION OF STEGANOGRAPHY

Modern steganography uses the chance of hiding information into digital multimedia files and also at the network packet level. It requires following elements; the cover media(C) that will hold the hidden data, the secret message (M), may be plain text, cipher text or any type of data ·The stego function (Fe) and its inverse (Fe-1).An optional stego-key (K) or password is second-hand to hide and unhide the message. The stego function operates over cover media and the message (to be hidden) along with a stego-key (optionally) to create a stego media (S)[12].

The ordinary current technique of steganography exploits the property of the media itself to express information. These are the candidate for digitally embedding message.

- Plaintext
- Audio
- Video ·
- Image
- IP datagram units and Protocols

2.1. Hiding a Message inside a Text

The secrets within plain text have in common. Many techniques involve the modification of the layout of a text, rules like using every n-th character of the amount of whitespace after lines or between words. The final technique was effectively used in practice and even after a text has been printed and copied on paper for ten times, the secret message could still be retrieved. Another possible way of storing a secret within a text is using a publicly available cover source, a book or a newspaper, and using a code which consists. No information stored inside the cover source will lead to the hidden message. Discovering it relies solely on gaining awareness about secret key.

2.2. Images

Hiding information within images is a popular technique nowadays. An image with a secret message inside can easily be spread over the world wide web. The use of steganography in newsgroups has been researched by German steganographic expert, who made a scanning cluster which detects the presence of hidden messages inside images that were posted on internet. After checking one million images, no hidden messages were found, so the practical use of steganography seems to be limited. In order to hide a message within an image without changing its visible properties, the cover source can be altered in noisy areas with many colour variations, so less attention will be drawn to the modifications. Most common methods are usage of the least-significant bit or masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of JPEG files [5].

2.3. Audio and Video

Hiding information inside audio files can be done in many ways. Using the least-significant bit is possible, as modifications will usually not create audible changes to the sounds. An additional method involves taking advantage of human limitations. It is not impossible to encode messages using frequencies that are inaudible to the human ear. Using any frequencies above 20.000 Hz, messages can be hidden in sound files and will not be detected by human. Also, a message can be encoded using musical tones with the substitution scheme.

III. PROPOSED SCHEME: FREQUENCY DOMAIN

Proposed scheme attempts to insert the secret image into multi-stage compressed images and to find the hidden secret images progressively from the multi-stage decoded images. Two procedures are using: the secret embedding and the secret extraction.

3.1. The Embedding Procedure

To progressively identify the hidden secret image, the secret image is also encoded with multi-stage in which the smaller and extra important secret data will encode in the earlier encoding stages and the mass and less important secret data are encoded in the final encoding stages [6].According to its importance the secret image again set. The refined bit stream generated in each encoding stage must be first detected in order to insert the rearranged secret image into multi-stage compressed images. In the case of multi-stage encoding, a coefficient is marked as a significant node if its magnitude is greater than or equals to the encoding threshold.

The most significant bit (MSB) of the significant node encoded in this encoding stage. The remaining bits will be programmed in the following encoding stages for refining this significant node. Since the refined bit stream is extracted from significant nodes, embedding secret image into refined bit stream can be preserve good stego-image imperceptibility. A progressive secret revealing scheme based on a set combination theory is presented. The set combination theory was applied to indicate the relationship among the refined bit stream and subset distribution. The number of modification bits in each embedded block is limited to less than or equal to one [6].Embedding the secret image into multistage programmed bit stream was happening here.

A great amount of data with high security, no loss of secret message and a good invisibility can be achieved using DWT (Discrete Wavelet Transform). The basic idea to hide information using DWT is to alter the magnitude of the DWT coefficients of three sub-bands, HH, HL, and LH of cover image [14].

3.2. The Extraction Procedure

The extraction procedure is same as to the embedding procedure. The pattern P used in the embedding procedure ought to be known. To extract the secret image, the stego-image bit stream will be received and the refined bit stream, which hides the secret image, will be detected according to the embedding threshold = 64. The detected refined bit stream is also partitioned into blocks B———————————— with the same size as P. Then, the relationship of elements between B———————————— and P is computed and summed. The LSBs of computational result shows the hidden secret data. From that, hidden secret is extracted. The extracted secret data are similar as the embedded one. Since the stego-image is encoded with multi-stages, the secret image can be extracted more and more by decoding the threshold higher to inferior. The decoding threshold determines the number of extracted secret bits. This produces a higher quality secret image [6].

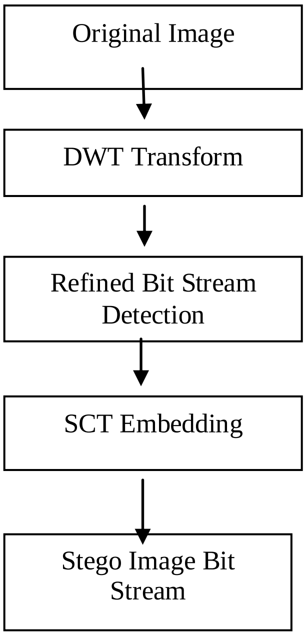

Fig a: Embedding Procedure

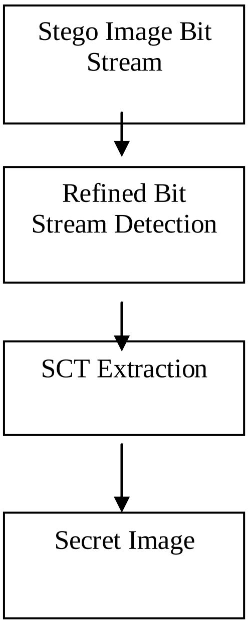

Fig b: Extraction Procedure

3.3. Performance

In a data hiding scheme, some tradeoff between hiding capacity and stego-image quality can be visualize. Hiding capacity and the stego-image quality are determined by the embedded block size and the number of refined bits. Variable embedded block sizes may be used to deal with the tradeoff between the hiding capacity and stego-image quality. Regarding to security consideration, the pattern can be randomly permuted to improve the hiding security. Also, the embedded block extracted from the refined bit stream and the secret data can be encrypted by using encryption systems, such as DES, RSA before the embedding procedure is performed [6]. The experimental results showed that multi-stage secret revealing was achieved.

IV. PROPOSED METHOD: SPATIAL DOMAIN

It represents an adaptive steganographic method based on just noticeable distortion (JND) profile measurement. The method considers four different impact factors to compute how much information can be embedded and what the stego-pixel value will be. The JND value of the target pixel, difference values that represent the correlation between neighboring pixels, the contents of various lengths secret data bits, a predefined embedding capacity control factor have to be considered. The proposed method embeds more secret data bits within complex areas and a few data bits in smooth areas. The difference between the target pixel and the stego-pixel values is restricted, as far as possible, to less than or equal to the JND value of the target pixel.

The stego-image maintains good imperceptible property. The embedded secret data can be extracted from the stegoimage without referencing the original image and the JND profile. The experimental results show that this method improves stego-image quality and conspicuously improves the embedding capacity at the same time [7].

V. APPLICATIONS

- To have secure secret communications where cryptographic encryption methods are unavailable.
- To have secure secret communication where strong cryptography is impossible.
- In some cases like military applications, even the knowledge that two parties communicate can be of large importance.
- The health care, and especially medical imaging systems, may very much benefit from information hiding techniques.
- It is used in modern printers, alleged use by intelligence services, distributed stegnography, online challenge etc

VI. CONCLUSION AND FUTURE SCOP

Steganography is the technique to hide information under cover media. This is the most popular and efficient technique nowadays. The paper basically explained the stegnography approach both in frequency domain and spatial domain. The spatial domain study shows good stego image quality and improved embedding capacity. It can also be used to implement watermarking. It is also possible to simply use steganography to store information on a location. This technique combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The most important use of steganographic techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials.

REFERENCES

[1]. N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” IEEE Computer, vol. 31, no. 2, pp. 26–34, Feb. 1998.

[2]. X. Zhang and S.Wang, “Steganography using multiple-base notational system and human vision sensitivity,” IEEE Signal Process. Lett., vol. 12, no. 1, pp. 67–70, Jan. 2005.

[3]. H. Noda, J. Spaulding, M. N. Shirazi, and E. Kawaguchi, “Application of bit-plane decomposition steganography to jpeg 2000 encoded images,” IEEE Signal Process. Lett., vol. 9, no. 12, pp. 410–413, Dec. 2002.

[4]. D.-C. Wu and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognit. Lett., vol. 24, pp. 1613–1626, 2003.

[5]. R. Chandramouli, M. Kharrazi, and N. Memon, “Image steganography and steganalysis: Concepts and practice,” in Proc. Int. Workshop Digital Watermarking 2003, 2004, vol. 2939

[6]. Hsiu-Lien Yeha, Shu-Tsai Gueb, Piyu Tsaib, Wei-Kuan Shiha, “Wavelet bit-plane based data hiding for compressed images”, Int. J. Electron. Commun. 67 (2013) 808– 815, Publisher:Elsevier

[7]. Ju-Yuan Hsiao, Chieh-Tse Chang, “An adaptive steganographic method based on the measurement of just noticeable distortion profile” Image and Vision Computing 29 (2011) 155–166, Publisher:Elsevier

[8]. Chin-Feng Lee ,Hsing-Ling Chen , Shu-Hua Lai , “An adaptive data hiding scheme with high embedding capacity and visual image quality based on SMVQ prediction through classification codebooks”, Image and Vision Computing 28 (2010) 1293–1302, Publisher:Elsevier

[9]. Mr . Vikas Tyagi*1, Mr. Atul kumar2, Roshan Patel3, Sachin Tyagi4, Saurabh Singh Gangwar5:”Image Steganography Using Least Significant Bit With Cryptography”, Journal of Global Research in Computer Science , Volume 3, No. 3, March 2012

[10]. Mihir h Rajyaguru:"Crystography-Combination of Cryptography and Steganography With Rapidly Changing Keys”, International Journal of Emerging Technology and Advanced Engineering,www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 10, October 2012)329

[11]. Deepali:”Steganography With Data Integrity”,International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue.7

[12]. [12] Arvind Kumar Km. Pooja;” Steganography- A Data Hiding Technique”; International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010

[13]. Komal Patel1,, Surendra Vishwakarma2, Hitesh Gupta3: "Triple Security of Information Using Stegnography and Cryptography"

[14]. International Journal of Emerging Technology and Advanced Engineering ,Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 10, October 2013)

[15]. Dr. MAHESH KUMAR, MUNESH YADAV" Image Steganography Using Frequency Domain"; International Journal Of Scientific & Technology Research Volume 3, Issue 9, September 2014

[16]. NamitaTiwari, Dr. Madhu Sandilya, Dr. Meenu Chawla ,"Spatial Domain Image Steganography based on Security and Randomization" (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 5, No. 1, 2014.