International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

General View on Techniques Used In Image Steganography

Jayshree V. Ingle[1], M. M. Bartere[2]

[1]Student of Master of Engineering in (CSE), G. H. Raisoni college of Engineering and Management, Amravati, India
[2]Guide, Assistant professor Department of (CSE), G.H Raisoni college of Engineering and Management, Amravati, India

Abstract: ***The Steganography is getting its importance due to the increase in secret communication of computer users over the internet. It can also be express as an invisible communication that actually deals with the ways of hiding the presence of the secrete message from the image. Generally that data embedding is achieved in the communication, text, image, multimedia, voice content for copyright, military communication, authentication and for many other purposes. In the image Steganography, secret communication is achieved to hide a message into the cover image.The secret message is embedded inside the cover image in encrypted format by using some hiding algorithm and it send to a receiver over a network. The receiver then it decrypted the message by applying the reverse process on the cover data and reveal the secret data. Steganography means is not to vary the structure of secret message, but hides it inside a carrier-object (cover object). After hiding process cover object and stego-object (object which contain secrete information) are similar. This paper is about to showthe two different techniques that is used in the image steganography. There are two techniques that we study in this paper are Wavelet Transform and spread spectrum***.

Keyword: Cover-Image, Message, Stego-Image

1. Introduction

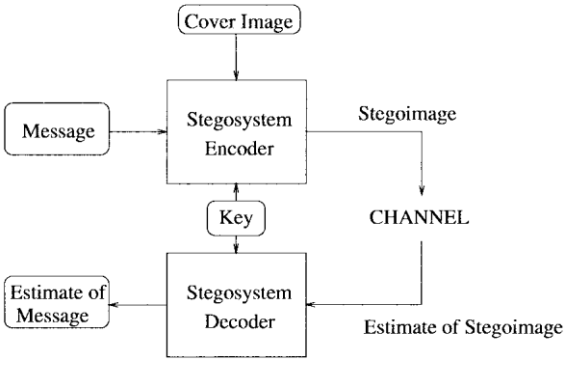
As the world moving, need for technology increased. Everyone has its secret's, which he wants to hide from the world. If anyone wants to share a secret massage with someone at that time image steganography is very useful. Many years ago, there are so mediums that are used for hiding secret message. One of the oldest recorded use of steganography technique was dates back to the time of Herodotus, is about 2000 years ago. In his one story, Herodotus ordered of a Persian soldier that shaved the head of one of his slaves and then tattooed a secret message on his head (scalp). Then once the slave's hair grew again, the man sent him to his predetermine place with such order that, shave his head that it revealing a plan to incite a revolt against the Persians.

Steganography Equation: 'Stego-medium = Cover medium + Secret message + Stego key'

The embedded data is the data that one wants to send secretly. It is actually hidden in an cover message and is referred to as a cover-image, making the stego-object or other stego-text. The purpose of stego-key to controlling the hiding process so that it restrict the detection and also used for recovering of the secret data to reciever who know the stegno key. The Pure steganography in which there is no` stego key is present. It works on the assumption that no other party is aware of the communication.

In the secret key steganography in which thestego key is exchanged before the communication. It is the most suspectible to interception. And in the Public key steganography in which a public key and a private key is used for a secure communication.Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. The use of steganography in newsgroups has been researched by German steganographic expert NielsProvos, who created a scanning cluster which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited. To hide a message inside an image without changing its visible properties, the cover source can be altered in "noisy" areas with many color variations, so less attention will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image file.

Actually image steganography is method of data hiding into cover-image and create a stego-image. This stego-image then sent to the person by any known medium, where the third persondoes not know that this stego-image has hidden message. When the person receives stego-image, hidden message can simply be extracted with or without stego-key (depending on embedding algorithm) by the receiving end. Basic structure of image steganography is shown in Figure.



without stego-key, where embedding algorithm required a cover image with message for embedding procedure. Output of embedding algorithm is a stego-image which simply sent to extracting algorithm, where extracted algorithm unhide the message from stego-image.

To hide a message inside an image without changing its visible properties, the cover source can be altered in ”noisy” areas with many color variations, so less attention will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image file

There are some Steganographic methods:

1. Substitution
2. Transform
3. Domain
4. Spread Spectrum
5. Statical

- The substitution methods in which the substitute redundant parts of a cover with a secret message (spatial domain).
- The transform domain techniques hides secret data in a transform space of the signal (frequency domain)
- The spread spectrum techniques accepted the ideas from spread spectrum communication.
- The Statistical methods which encode data by changing several statistical properties of a cover and then use hypothesis testing in the extraction process.
- The Distortion techniques which stores data by signal distortion and then measure the deviation from the original cover in the decoding step.
- A Cover generation methods which encodes the data in the way a cover for secret communication is created.

2. Classification of Steganographic Categories

Steganography is classified into 3 categories,

- Pure steganography where there is no stego key. It is based on the assumption that no other party is aware of the communication.
- Secret key steganography where the stego key is exchanged prior to communication. This is most suspectible to interception.
- Public key steganography where a public key and a private key is used for secure communication.

Image Steganography Classifications

Actually image steganography is categorized in following aspects.

High Capacity: Maximum size of information can be embedded into image.

Perceptual Transparency: After hiding process into cover image, perceptual quality will be degraded into stego-image as compare to cover image.
Robustness: After embedding, data should stay intact if stego-image goes into some transformation such as cropping, scaling, filtering and addition of noise.

Temper Resistance: It should be difficult to alter the message once it has been embedded into stego-image.

Computation Complexity: How much expensive it is computationally for embedding and extracting a hidden message?

Now, let us study about the two different techniques of image steganography. These two 1`techniques are spread spectrum and wavelet transform.

3. Spread Spectrum

Spread Spectrum Image Steganography Technique **[SSIS]**

Today’s present invention for information hiding or secret communication steganographic system isSpread Spectrum Image Steganography (SSIS) which uses digital image as a cover medium. Spread spectrum gives that the ability that hides a significant quantity of data bits within cover image while avoiding detection by other person. The secret data is recovered with having lowest error probability because the use of error control coding. Spread spectrum image steganography in which payload is at a minimum, an order of magnitude greater than of existing watermarking techniques. The cover image is not needed to decode the secret message. The receiver needs only having a secret key which is used to decode the secret message. The presence of secret data is virtually undetectable by human and also computer. Spread spectrum provides resiliency to transmission noise, such as which is found in the wireless environment and the low levels of compression.

The applications for techniques that embed data within digital images. The reveal of secret messages is an obvious function, but today’s technology stimulates even more subtle uses. In the movie subtitles, captioning is one such use of text information can be easily embedded within the cover image. The ability to deposit image creation and revision information within the image provides a form of revision tracking as another possible application of digital steganography. This avoids the need for maintaining two separate media, one containing the image itself and one containing the revision data. The embedded signal estimation performs better for the images that have significant smooth areas.

Embedded such as the Ulm and LAV-25 images. This is reflected in the low embedded signal BER and correspondingly of low steganography SNR. Signal BER which is used for embedding purpose permits the use of the rate 1/6 convolutional code, which has a threshold (the level at which the code can typically correct all errors equal to and less than BER) of 0.22 BER. Images that have regions of high frequency require a strong embedded signal power, which providing a lower steganography

SNR that yields a higher embedded signal BER and requiring an error-correcting code that can correct more errors. Error-correcting code that is capable of correcting the embedded signal BER can be used. If higher rate codes can be used, the payload amount will increase.

4. Wavelet Transform

The traditional steganography system's security depends on the encoding system's secrecy. Thus such a system might work for a particular time, once it is known by someone, it is simple enough to know the entire received media passing by to check for secret messages at last, and such a steganography system fails. The newsteganography system, attempts to be detectable only if he knows the secret key, then and then he will get the secret data. In such case, cryptography method should be used, which holds the cryptographic system's security that should rely solely on that key material. The steganography those to be remain undetected by other person, the unmodified cover image that must be kept in secret, because if it is known by other person, who creates problem because the comparison between the cover image and the stego image can immediately reveals the changes.

Wavelet Transform: A Wavelet is a small wave which contains energy is concentrated in time that is use to give a tool for the analysis of transient, non-stationary or time-varying phenomena. It is improving very quickly. Wavelets is used very effectively as a powerful tool in many different fields, including approximation theory, signal processing, physics, astronomy, and image processing.

Many practical tests are done to use the wavelet transform domain in the steganography because there are many advantages that can be obtained by using this wavelet transform. The use of such wavelet transform will mainly points the robustness and capacity of the data hiding system features. The hierarchical nature of it that represents allows multi-resolution detection of the secret message, it is a Gaussian distributed random vector that added to all the high pass bands in the wavelet domain. It is given that when subjected to distortion from compression, the secret message can still be correctly access in each resolution in Discrete Wavelet Transform (DWT) domain.

The signal can be better analyzed if it is given as a linear decomposition of sums of products of coefficient and the functions. A two-parameter system is to be constructed that one has a double sum and coefficient with two indices. The set of the coefficients are called the DWT of a signal. In this wavelet transform, the original signal (1-D, 2-D, 3-D) is transformed by using already define wavelets.

The DWT is implemented using the function that is present in MATLAB to simplify the analysis and reduce development time.

The wavelet is divided into two decompositions,

One-Dimensional Wavelet Decomposition

A single- level one- dimensional Wavelet decomposition is done with respect to either a particular Wavelet or particular Wavelet decomposition filters.

A Starting from a signal s, there present2 sets of coefficients are computed: approximation coefficients *cA1*, and the detail coefficients *cD1*. The vectors can be extracted by convolving *s* with the low-pass filter *Lo_D* for approximation and with the high-pass filter *Hi_D* for detail; it is followed by dyadic decimation. For each filter the length is equal to *2N*. Then If *n* is the length of s, the signals *F* and *G* are of length *n + 2N - 1*, and then the coefficients *cA1* and *cD1* are of length *[(n-1)/2] +N*.

Multilevel 2-D Wavelet Decomposition

An algorithm similar to the one-dimensional (for image) this is also possible for two-dimensional Wavelets and then we can obtain scaling function from one-dimensional ones by tensor product. The kind of two-dimensional DWT is to be decomposed of approximation coefficients at the level *j* in 4 components: the approximation at level *j+1*, and the detailed in 3 orientations are that are vertical, diagonal, horizontal.

5. Conclusion

This paper explains about the general view of spread spectrum and the wavelet transform. When any stego images are decoded, by using spread spectrum and wavelet transform the text messages are completely recoverable. And also the system is able to cope with added noise and compression of the stegoimage has been exhibited.

An intruder or illegal person will be unable to decode the hidden information without having the perfect keys even though he knows system methodology. The wavelet transform is dividing into two, one dimensional and multi-dimensional. The ability of Wavelet transforms to compress data and introducing sparsity, hence it increases the capacity or payload of the steganography process.

References

[1] Bilgin A., Sementilli J., Sheng F., and Marcellin W., "Scalable Image Coding Using Reversible Integer Wavelet Transforms," *Computer Journal of Image Processing IEEE Transactions*, vol. 9, no. 4, pp. 1972 - 1977, 2000.
[2] Walker S., *A Premier of Wavelets and Their Scientific Applications*, CRC Press, 1999.
[3] F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *IEEE Computer Mag.*, pp. 26–34, Feb. 1998.
[4] B. Pfitzmann, "Trials of traced traitors," R. Anderson, Ed. Berlin, Germany: Springer-Verlag, 1996, vol. 1, pp. 49–64.
[5] J. R. Smith and B. O. Comisky, "Modulation and information hiding in images"

[6] Johnson N. and Jajodia S., "Steganography: Seeing the Unseen," *IEEE Computer Magazine*, vol. 25, no. 4, pp. 26-34, 1998.
[7] Lee K. and Chen H., "A High Capacity Image Steganographic Model," *in IEEE Proceedings on Vision Image and Signal Processing*, China, pp. 288-294, 2000.
[8] Lin T. and Delp J., "A Review of Data Hiding in Digital Images," *in Proceedings of the Image Processing, Image Quality, and Image Capture Conference*, Georgia, pp. 274-278, 1999.
[9] Lo Y., Topiwala S., and Wang J., "Wavelet
[10] Based Steganography and Watermarking," *Wavelets Reports*, Cornell University, http://dukiedoggie.tripod.com/cornell/wavelets/report.html, 1998.
[11] Lu S., *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*, Idea Group Publishing, 2005
[12] Microsoft Press, *Fundamentals of Network Security*, Microsoft Official Curriculum, 2003.
[13] L. M. Marvel and C. G. Boncelet, Jr., "Capacit of the additive steganographic channel," submitted for publication.
[14] R. van Schyndel, A. Tirkel, and C. Osborne, "A digital watermark," in *Proc. IEEE Int. Conf. Image Processing*, 1994, vol. *Image Processing*, Lausanne, Switzerland, Sept.1996, vol. 111, pp. 219–222.
[15] R. Machado, http://www.fqa.com/romana/romanasoft/stego.html