International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 6, June-2014, pp: (241-245), Impact Factor: 1.252, Available online at: www.erpublications.com

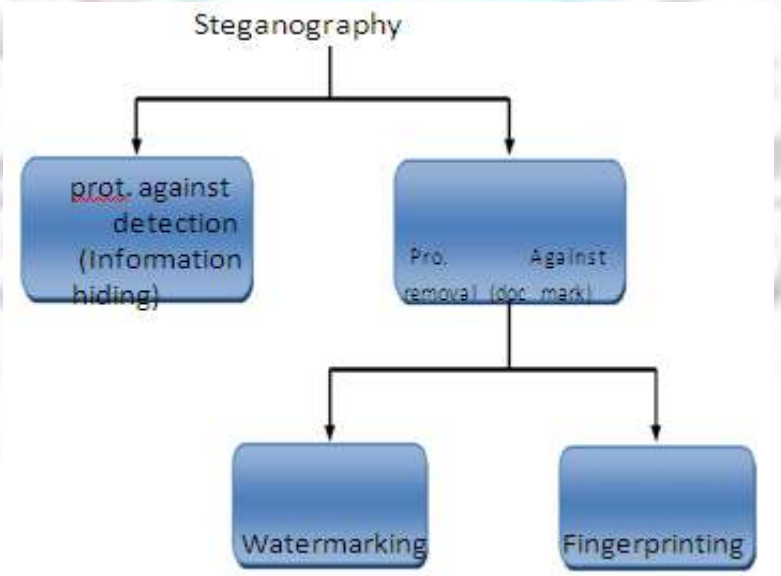
Steganography and Its Various Techniques

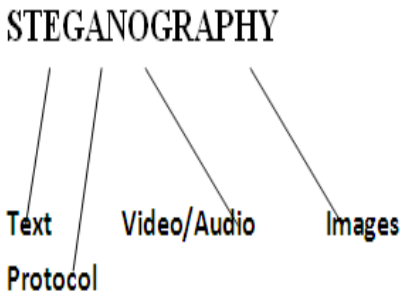
Sarita Nain[1], Sunil Kumar[2]
[1]M. Tech (ECE), PDMCE, Bhadurgarh, Haryana, India
[2]Asst. Prof., PDMCE, Bhadurgarh, Haryana, India

Abstract: Communication is in progress since many years. Internet expeditious development and information technology made it is easy and fast to receive and send messages, pictures, video etc. With this transmission privacy and authentication became very important and this leads to the development of more and enhanced secure data hiding techniques. To achieve secure communications, the cousins cryptography and steganography are used. Steganography provide a secure form of communication. Many different image file formats exist, most of them for specific applications. Here different types of techniques for data hiding and securing information are described with their advantages and disadvantages.

Keyword: Steganography, cryptography.

INTRODUCTION





DATA TYPES OF STEGANOGRAPHY

The word steganography is derived from Greek words, "stego" means to "cover" and, "grafia" means "writing" so Steganography means to cover/hide information. The art of hiding information in any other information and also hiding the fact that communication is taking place is known as steganography. For this there exist a large number of techniques some are complex and some are easy and all these have their respective advantages and disadvantages.

HISTORY

After deriving the term many researchers used it for thousands of years in different ways [10]. During the 5th century BCE, the Greek tyrant Histiaeus was taken as a prisoner by King Darius in Susa. Histiaeus needed to send an abstruse message to his son-in-law, Aristagoras, who was in Miletus and in order to do this, Histiaeus shaved a slave's head and tattooed the message on his scalp. As soon as the slave's hair grew sufficiently to conceal the tattoo, he was sent to Miletus with the message [11].In ancient Greece, another method was to peal the wax off a wax-covered tablet, then write a message and to have the application of the wax again. The one in charge to receive the message would simply need to get rid of the wax from the tablet to see the message. Invisible ink was another popular form of Steganography. Ancient Romans had their way in writing between the lines by using invisible ink, and by using substances such as fruit juice, urine, and milk. Using Invisible ink, though seems harmless, a letter might reflect a very different message written between the lines. Invisible ink was used as recently as World War II .

In addition to invisible ink, the Germans used the Microdot technique during the Second World War. Information, particularly photographs, was made so small that they were very difficult to detect [13]. In 1550, Jerome Cardan, an Italian mathematician, proposed a scheme of secret writing where a paper mask with holes is used. The user of such papers all what he needs is to write his secret message in such holes after placing the mask over a blank sheet of paper. The next step is to remove the mask to fill in the blank parts of the page and in this way the message appears as innocuous text [14]. This technique, Steganography, is now highly used in computers files with digital data as the carrier and networks are considered as high-speed dispatch channels. The sections that follow illustrate the taxonomy of Steganography techniques for image files, including an overview of the most important Steganography techniques for digital images .

CLASSIFICATION OF STEGANOGRAPHY TECHNIQUES

Here provide the necessary background required for this paper. In section 2.1 discuss briefly some of the existing Steganography techniques .

Existing Steganography Techniques: The Steganography algorithms proposed in literature can broadly be classified into two categories:

1. Spatial Domain Techniques
2. Transform Domain Techniques

Each of these techniques are covered in detail in the next two subsections. Though there are three more categories in which these are techniques can be classified, these are:

1 Spread Spectrum 2 Statistical Method 3 Distortion Technique

Spatial Domain

These techniques use the pixel gray levels and their color values directly for encoding the message bits. These techniques are some of the simplest schemes in terms of embedding and extraction complexity. The major drawback of these methods is amount of additive noise that creeps in the image which directly affects the Peak Signal to Noise Ratio and the statistical properties of the image. Moreover these embedding algorithms are applicable mainly to lossless image compression schemes like TIFF images. For lossy compression scheme like JPEG, some of message bits get lost during compression step.

The most common algorithm belonging to this class of techniques is the Least Significant Bit (LSB) Replacement technique in which the LSB of the binary representation of the pixel gray levels is used to represent the message bit. This kind of embedding leads to an addition of a noise of 0:5p on average in the pixels of image where p is the embedding rate in bits/pixel. This kind of embedding also leads to an asymmetry and a grouping in the pixel gray values (0,1);(2,3);. . . (254,255). This asymmetry is exploited in the attacks developed for this technique as explained further in section 2.2. To overcome this undesirable asymmetry, the decision of changing the least significant bit is randomized i.e. if the message bit does not match the pixel bit, then pixel bit is either increased or decreased by 1. This technique is popularly known as LSB Matching. It can be observed that even this kind of embedding adds a noise of0:5p on average. To further reduce the noise, [2] have suggested the use of a binary function of two cover pixels to embed the data bits. The embedding is performed using a pair of pixels as a unit, where the LSB of the first pixel carries one bit of information, and a function of the two pixel values carries another bit of information. It has been shown that embedding in this fashion reduces the embedding noise introduced in cover signal.

According to [20], "For a given medium, the Steganography algorithm which makes fewer embedding changes or adds less additive noise will be less detectable as compared to an algorithm which makes relatively more changes or adds higher additive noise." Following the same line of thought Crandall [7] have introduced the use of an Error Control Coding technique called "Matrix Encoding". In Matrix Encoding in a group of 3 pixels while adding a noise of 0:75 per

group on average. The maximum em- LSB replacement technique has been extended to multiple bit planes as well. Recently [3] has claimed that LSB replacement involving more than one least significant bit planes is less detectable than single bit plane LSB replacement. Hence the use of multiple bit bedding capacity achievable is 2=3 = 0:67 bits/pixel. F5 algorithm [17] is probably the most popular implementation of Matrix Encoding planes for embedding has been encouraged. But the direct use of 3 or more bit planes leads to addition of considerable amount of noise in the cover image. [8] and [9] have given a detailed analysis of the noise added by the LSB embedding in 3 bit planes. Also, a new algorithm which uses a combination of Single Digit Sum Function and Matrix Encoding has been proposed. It has been shown analytically that the noise added by the proposed algorithm in a pixel of the image is0:75p as compared to 0:875p added by 3 plane LSB embedding where p is the embedding rate. One point to be observed here is that most of the approaches proposed so far are based on minimization of the noise embedded in the cover by the algorithm. Another direction of Steganography algorithm is preserving the statistics of the image which get changed due to embedding.

Transform Domain

These techniques try to encode message bits in the transform domain coefficients of the image. Data embedding performed in transform domain is widely used for robust watermarking. Similar techniques can also realize large-capacity embedding for Steganography. Candidate transforms include discrete cosine Transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT). By being embedded in the transform domain, the hidden data resides in more robust areas, spread across the entire image, and provides better resistance against signal processing. Eg: we can perform a block DCT and, depending on pay-load and robustness requirements, choose one or more components in each block to form a new data group that, in turn, is pseudo randomly scrambled and undergoes a second-layer trans-formation. Modification is then carried out on double transform domain coefficients using various schemes. These techniques have high embedding and extraction complexity. Because of robustness properties of transform domain embedding, these techniques are more applicable to "Watermarking" aspect of data hiding.

F5 [17] uses the Discrete Cosine Transform coefficients of an image for embedding data bits. F5 embeds data in the DCT coefficients by rounding the quantized coefficients to the nearest data bit. It also uses Matrix Encoding for reducing the embedded noise in the signal. F5 is one the most popular embedding schemes in DCT domain Steganography, though it has been successfully broken in [42]. The transform domain embedding does not necessarily mean generating the transform coefficients on a blocks of size 8 8 as done in JPEG compression techniques. It is possible to design techniques which take the transforms on the whole image [10]. Other block based JPEG domain and wavelet based embedding algorithms have been proposed in [11] and [25] respectively.

Spread Spectrum

Spread spectrum transmission in radio communication transmit message below level of noise frequency. In Steganography it deals either with cover image as noise or tries to add as pseudo-noise in the cover image.
Cover Image As Noise: A system that treats the cover image as noise can add a single value to that cover image. This value must be transmitted below that noise level. This means that the channel capacity of the image changes significantly. Thus, while this value can be a real number, in practice, the difficulty in recovering a real number decreases the value to a single bit. To permit the transmission of more than one bit, the cover image has to be broken into sub images. When these sub cover images are tiles, the technique is referred to as direct-sequence spread spectrum Steganography. When the sub cover images consist of separate points distributed over the cover image, the technique is referred to as frequency-hopping spread-spectrum Steganography. These techniques require searching the image for the carrier in order to then retrieve the data. These techniques are robust against gentle JPEG compression and can be made more robust through the pre-distortion of the carrier.

Pseudo-noise: This technique shows that the hidden data is spread throughout the cover image and that is why it becomes difficult to detect [37]. Spread spectrum image Steganography (SSIS) described by Marvel et al., combined spread spectrum communication, error control coding, and image processing to hide information in images, is an example of this technique [38]. The general additive embedding scheme can be described as follows:

$$Y_i = X_i + \gamma W_i \quad \text{for } i = 1, 2, \ldots\ldots, N \quad (5)$$

Where X_i is a sequence of the original data from the cover, Wi is a pseudo-random sequence generated from a pseudo-random number generator (PRNG) initialized by a secret stego key, γ is an embedding strength parameter (gain factor), and Yi is a sequence of possibly altered data.

STATISTICAL METHODS

Also known as model-based techniques, these techniques tend to modulate or modify the statistical properties of an image in addition to preserving them in the embedding process. This modification is typically small, and it is thereby able to take advantage of the human weakness in detecting luminance variation [17].Statistical Steganography techniques exploit the existence of a "1-bit", where nearly a bit of data is embedded in a digital carrier. This process is done by simply modifying the cover image to make a sort of significant change in the statistical characteristics if "1" is

transmitted, otherwise it is left unchanged [45]. To send multiple bits, an image is broken into sub-images, each corresponding to a single bit of the message.

Distortion Technique

It require original cover image during decoding process where decoder functions to check for differences between original cover image and distorted cover image in order to restore secret message. Encoder, adds a sequence of changes to cover image. So, information is described as being stored by signal distortion .Using this technique, a stego-object is created by applying sequence of modifications to cover image. This sequence of modifications is selected to match secret message required to transmit [45]. Message is encoded at pseudo-randomly chosen pixels. If stego-image is different from cover image at given message pixel, then message bit is a "1." Otherwise, message bit is a "0." Encoder can modify "1" value pixels in such manner that statistical properties of image are not affected (which is different from many LSB methods).

TABLE 1

	LSB	Transform Domain	Spread Spectrum	Statistical Techniques	Distortion Techniques	File and Pallet Embedding
Imperceptibility	High*	High	High	Medium*	Low	High*
Robustness	Low	High	Medium	Low	Low	Low
Payload Capacity	High	Low	High	Low*	Low	High

CONCLUSION

In this paper various options for hiding data are addressed for both lossy and lossless image format such as JPEG and BMP. We revisited information theoretic and practical approach proposed to increase capacity and security. However there are many different techniques used for stag image based on requirement and capacity and security they are used, table1 shows comparison between different techniques. Above an overview of different techniques is given. From above study it can be concluded that still capacity and security of the system can be increased by improving some factors.

REFERENCES

[1]. Yu-Chiang Li, Chia-Ming Yeh, Chin-Chen Chang, " Data Hiding Based On The Similarity Between Neighboring Pixels With Reversibility" October 24, 2009.
[2]. Yuan-Yu Tsai, Du-Shiau Tsai, Chao-Liang Liu, "Revesible Data Hiding Scheme Based On Neighboring Pixel Differences" September 12, 2012.
[3]. Szymon Grabski, Krzysztof Szczypiorski, "Steganography in OFDM Symbols of Fast IEEE 802.11 n Networks" 2013.
[4]. Ching-Te Wang, Ching-Lin Wang, Lin-Chun Li and Sheng-You Guo, "The Image High Capacity And Reversible Data Hiding Technique Based On Pixel Frequency Of Block" 2011.
[5]. Graeme Bell and Yeuan-KuenLi, "A Method For Automatic Identification Of Signatures of Steganography Software" June 2, 2010.
[6]. I.J. Cox, M.L. Bloom, J.A. Fridrich, and T. Kalkert. Digital watermarking and Steganography. USA: Morgan Kaufman Publishers, 2008, pp. 1-591.
[7]. N.F. Johnson and S. Jajodia. (1998, Feb.). "Exploring Steganography: seeing the unseen." IEEE Computer Journal. [On line]. 31(2), pp. 26-34. Available: http://www.jjtc.com/pub/r2026.pdf [Jun. 2011].
[8]. A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). "Digital image Steganography: survey and analysis of current methods." Signal Processing Journal. [On line]. 90(3), pp. 727-752. Available: http://www.abbascheddad.net/Survey.pdf [Aug. 2011].
[9]. M. Fortrini, "Steganography and digital watermarking: A global view." University of California, Davis. Available: http://lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/fortini/project.pdf.[June2011].
[10]. N. Provos and P. Honeyman. (2003, Jun.). "Hide and seek: An introduction to Steganography." IEEE Security and Privacy Journal. [On line], 1(3), pp. 32-44.

ABOUT AUTHOR

The Author have completed her B.TECH. (ECE) from MDU, Rohtak, Haryana and currently pursuing M.TECH. (ECE) from PDMCE, Bhadurgarh, Haryana. Her area of interest is "hiding the secret data in images" that is Steganography.

E-mail: nainsarita2@gmail.com