E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

A REVIEW OF VIDEO STEGANOGRAPHY METHODS

Richa Khare[1], Dr. Kuldeep Raghuwanshi[2]
[1]*M.Tech. IV SEM (CSE)*
[2]*HOD of CSE Dept*
[1,2]*Oriental College of Sc & Tech Bhopal*
[1]*richa.khare28@gmail.com*, [2]*drkuldeepraghuwanshi@oriental.ac.in*

ABSTRACT:
Steganography is the art and science of sending covert messages such that the existence and nature of such a message is only known by the sender and intended recipient. Steganography has been practiced for thousands of years, but in the last two decades Steganography has been introduced to digital media. Attacks, misuse or unauthorized access of information is of great concern today which makes the protection of documents through digital media is a priority problem. It is the art of hiding message inside a multimedia block. Data hiding can be done in different medias like text, images and audio valid data or not. This urges the researcher's to devise new data hiding techniques through Steganography principle to protect and secure the data of vital significance. This paper we focus simple review Steganography methods.

Keywords: Steganography, Data hiding, NN (Neural Network).

1. INTRODUCTION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity [9]. The word Steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphing meaning "to write". Steganography is the technique of hiding the message in a chosen carrier such that no one except the intended recipient is aware of its existence [1]. Block diagram of Steganography mechanism is shown in Figure 1.

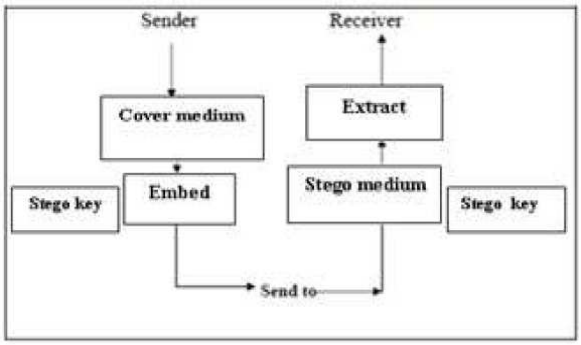

Figure1. Block diagram of Steganography scheme

Here a secret data is being embedded inside a cover image to produce the stego image. A key is often needed in the embedding process. The proper stego key is used by the sender for the embedding procedure. The same key is used by the recipient to extract the stego cover image in order to view the secret data. The stego image should look almost identical to the cover image.

A Steganography system, in general, is expected to meet three key requirements, namely, imperceptibility of embedding, accurate recovery of embedded information, and large payload (payload is the number of bits that

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

get delivered to the end user at the destination) [1]. In a pure Steganography framework, the technique for embedding the message should be unidentified to anyone other than the sender and the receiver. An effective Steganography should posses the following characteristics:

Secrecy: Extraction of hidden data from the host medium should not be possible without the knowledge of the proper secret key used in the extracting procedure.

Imperceptibility: After embedding the data in the medium, it should be imperceptible from the original medium.

High capacity: The maximum length of the hidden message that can be embedded can be as long as possible.

Resistance: The hidden data should be able to survive when the host medium has been manipulated, for example lossy compression scheme.

Accurate extraction: The extraction of the hidden data from the medium should be accurate and reliable.

There are mainly three basic data embedding techniques for images in practice, namely Least Significant Bit (LSB) Method, Masking and filtering and Transform based [11]. The primitive method is embedding in LSB. Although there are several disadvantages to this approach, the relative easiness to implement it makes it a popular method. In this method we embed information in the LSB of pixels colours. The changes of LSB may not be noticeable because of the imperfect sensitivity of the human eyes. On an average, only half of the bits in an image will need to be modified to embed a secret message using the maximal cover size. While using a 24-bit image gives a relatively large amount of space to hide messages, it is also possible to use an 8-bit image as a cover source. Because of the smaller space and different properties, 8-bit images require a more careful approach. Where 24-bit images use three bytes to represent a pixel, an 8-bit image uses only one. Changing the LSB of that byte will result in a visible change of colour, as another colour in the available palette will be displayed. Therefore, the cover image needs to be selected more carefully and preferably be in gray scale, as the human eye will not detect the difference between different gray values as easy as with different colours [11].

Masking and filtering techniques, usually restricted to 24 bits or gray scale images, take a different approach to embedding a message. These methods are effectively similar to paper watermarks, creating markings in an image. This can be achieved, for example, by modifying the luminance of parts of the image. While masking does change the visible properties of an image, it can be done in such a way that the human eye will not notice the difference. Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing. The information is not hidden at the noise level but is in the visible part of the image which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used [11]. In transform based data embedding, the cover image is transformed into another domain. Then the data is embedded in the transform coefficients. This method is highly robust and complex. The major transformations used are DCT and DWT. DCT is used in JPEG compression algorithm to transform successive 8_8 pixel blocks of the image, into 64 DCT coefficients each. After calculating the coefficients, the quantizing operation is performed. Although a modification of a single DCT will affect all 64 image pixels, the LSB of the quantized DCT coefficient can be used to embed information. When information is hidden in video, the program or person embedding the information will usually use the DCT method. DCT works by slightly changing the coefficients of each of the images in the video, only so much that it is not noticeable by the human eye. Data embedding in videos is similar to that of data embedding in images, apart from information is hidden in each frame of the video. When only a small

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

amount of information is hidden in a video, generally it is not noticeable. However, when more information is hidden, it will be more noticeable. DWT is based on sub-band coding and is found to yield a fast computation of Wavelet Transform. It is easy to implement and reduces the computation time and resources required.

A 2-D DWT transforms an image into four sub bands: LL, LH, HL and HH where L and H stand for Low and High. The LL sub band contains the average information and the other three sub-bands give the finer details of the image. Even if the three sub-bands LH, HL, HH are made zero, the LL alone can give the average image (an image of lower quality, with no finer details). We can embed the message image in two LSB planes of LH, HL and HH sub bands. Data is embedded in LL sub-band to avoid compression losses. Human Visual System (HVS) model points out different insensitivities among different level sub bands.

There are some other classification is also available, Digital steganography methods can be classified in three distinct modes: *injection*, *substitution* and for the third I coin the term *propagation* (otherwise known as "generating a new file"). The first two, and often the third type utilize specific *bit locations* as the covert channel for communications. And most utilize a *stego-key*, which provides control for the hiding and recovery processes, preventing or restricting detection by those who are not aware of the key, or do not have access to it.

a. Injection steganography works as might be expected, in that the *payload* or *embedded data* is placed inside the original (unaltered) host *cover-text*, *cover-image*, *cover-audio* or *cover-program* file. Doing so increases the host file size, and the process must be done in such a manner as to prevent the end-processing or presentation application (word processing program, picture viewer, music player, etc.), from revealing the presence of the embedded data within the cover. Most file types are susceptible to injection steganography. The file resulting from this process, or any other steganographic methodology is often referred to as the stego-text, stegoimage (audio, *etc.)* file, or more generically, a stego-object.

b. Substitution steganography *replaces* what is viewed as an insignificant part of the cover file, but also must survive when processed by any "native" application such as those listed above. The substituted portion of an executable cover file could be a program module or segment of executable code that is rarely or never used. This method (sometimes referred to as "bit-twiddling" or "bit-tweaking") can result in file degradation such as aberrations in video or still images, audible noise in sound files or in the case of executables, processing errors.

c. Propagation Steganography most often utilizes a generation engine which when fed the payload produces an output file. (It is possible to do it manually using a lookup table when the stego-object will be text). The content of this file, sometimes referred to as a "mimic", may appear as a freeform graphic, a music file, a verbose text document, a fractal image or some other form. When reprocessed by the generation engine, with few exceptions, a given payload will yield the same stego-object file. There is no host file or cover-object involved in this method.

The advantage of Steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages, no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, Steganography can be said to protect both messages and communicating parties. Techniques provide an interesting challenge for digital forensic investigations.

2. NEURAL NETWORK IN STEGANOGRAPHY

The term neural network was traditionally used to refer to a network or circuit of biological neurons. The modern usage of the term often refers to artificial neural networks, which are composed of artificial neurons or

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

nodes. Artificial Neural Networks may either be used to gain an understanding of biological neural networks, or for solving artificial intelligence problems without necessarily creating a model of a real biological system. Artificial Neural Networks have been applied successfully to speech recognition, image analysis and adaptive control, in order to construct software agents or autonomous robots.

There is (or should be!) interest from the counterterrorism and law-enforcement communities in measures that can be used to detect the existence of hidden data. This is steganalysis [3]. A single feature may provide only scant indication of the presence of Steganography, or, several features may on their face conflict in their diagnosis. What is needed is a method of combining multiple features into a single conclusion of "stego" or "innocent". For this we utilize a pattern recognition system called an artificial neural network (ANN). Developing an ANN is a two-stage process. First the network is trained by feeding it the features from a large pool of images, some of which are known to contain stego, and some that are known to not contain stego.

Based on the training, the neural net determines computational rules that can then be applied to the features of an image of unknown character. One particular merit of an artificial neural network is that it is adaptive—as additional data is provided to the system it refines its prediction function. In this way the pattern recognizer can respond to evolution in the data. For example, if small modifications are made to an existing steganographic algorithm, the software will be able to adapt. Liu Shaohui et al adopted neural network approach for finding the features which has significant effect on data hiding process [5].

3. RELATED WORK

a. Neural network has the super capability to approximation any nonlinear functions. We first extract features of image embedded information, then input them into neural network to get output. Manikopoulos et al. [2] discussed an algorithm that utilises the probability density function (PDF) to generate discriminator features fed into a neural network system which detects hidden data in this domain. A group of scientists at Iowa State University are focusing on the development of an innovative application which they call ''Artificial Neural Network Technology for Steganography (ANNTS)'' aimed at detecting all present Steganography techniques including DCT, DWT and DFT.

b. Adoption of Neural Network Approach in Maher EI Arbi et al. suggested video watermarking based on neural network [7]. They propose a novel digital video watermarking scheme based on multi resolution motion estimation and artificial neural network. A multi resolution motion estimation algorithm was adopted to preferentially allocate the watermark to coefficients containing motion. In addition, embedding and extraction of the watermark were based on the relationship between a wavelet coefficient and its neighbour's. A neural network was given to memorize the relationships between coefficients in a 3x3 block of the image. Experimental results showed that embedding watermark where picture content is moving is less perceptible. Further, it showed that the scheme was robust against common video processing attacks.

c. Guohua Wu el al. [5], suggested Counter propagation Neural Network (CNN) based method for fast audio digital watermark. By making use of the capabilities of memorization and fault tolerance in CPN, watermark is memorized in the nerve cells of CPN. In addition, they adopt a kind of architecture with an adaptive number of parallel CPN to treat with each audio frame and the corresponding watermark bit. Comparing with other traditional methods by using CPN, it was largely improve the efficiency for watermark embedding and correctness for extracting, namely the speed of whole algorithm. The extensive experimental results showed that, we can detect the watermark exactly under most of attacks. This method efficaciously trade off both the

E-ISSN: 2321–9637
Volume 2, Issue 1, January 2014
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

robustness and inaudibility of the audio digital watermark.

4. CONCLUSION

There are many techniques for Video Steganography. We only discussed here Neural Networks based Methods. Because today AI Based computer are used very rapidly in various fields, and NN techniques are used widely. The performance of various methods can be further improved with the use Neural Networks Methods.

Similarly, we can also use error back propagation algorithm to improve video Steganography performance of today new era of computer Techniques which is mostly based on Artificial Intelligence.

5. REFERENCES

[1]. "Video Steganography by LSB Substitution Using Different Polynomial Equations", *International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5*
[2]. C. Manikopoulos, S. Yun-Qing, S. Sui, Z. Zheng, N. Zhicheng, Z. Dekun, "Detection of Block DCT-based Steganography in Gray-scale Images", Proceedings of the IEEE Workshop on Multimedia Signal Processing, 9–11 December 2002, pp. 355–358.
[3]. Chuan-Yu Chang et al, "Using a Full Counterpropagation Neural Network for Image Watermarking", International Computer Symposium, Dec. 15-17, 2004, Taipei, Taiwan.
[4]. Clifford Bergman, Jennifer Davidson, "An Artificial Neural Network for Wavelet Steganalysis", Final Report to Midwest Forensics Resource Center.
[5]. Guohua Wu, Xiaodong Zhou, "A Fast Audio Digital Watermark Method Based on Counter-propagation Neural Networks", International Conference on Computer Science and Software Engineering, 2008, pp. 583-586
[6]. Liu Shaohui et al, "Neural Network Based Steganalysis in Still Images", ICME 2003, pp. 509-512.
[7]. Maher El' Arbi et al, "Video Watermarking Based On Neural Networks", ICME 2006, pp. 1577-1580.
[8]. M. Natarajan, Gayas Makhdumi., "Safeguarding the Digital Contents: Digital Watermarking", DESIDOC Journal of Library & Information Technology, 29, No. 3, May 2009, pp. 29-35.
[9]. Sanjeev kumar , Balasubramanian Raman And Manoj Thakur, "Real Coded Genetic algorithm Based Stereo Image Watermarking", International Journal of Secure Digital Information Age, 1, No.1, June 2009
[10]. Yu et al, "Digital Watermarking Based on Neural Networks for Color Images", Elsevier Signal Processing, 81 (2001).
[11]. "Advanced Video Steganography Algorithm" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 1, January -February 2013, pp.1641-1644.