A Secure Image Stegnography Process

Sakshi[1], Jaspreet Kaur[2]

[1, 2] Chadigarh Engineering College, Landran

Abstract: ***Steganography is available to gain its significance due to the exponential growth and covert communication of possible computer users over the internet. It can also be distinct as the study of imperceptible communication that typically deals with the ways of hiding the survival of the communicate message. A usually data embed is achieved in message, image, text, voice or multimedia content for rights, military message, verification and many other purpose. In image Steganography, secret message is achieved to establish significance into cover image and generate a stego image, generated image which is carrying a hidden message. This paper has analyzed various steganographic techniques like DWT, NN, DCT, GA, Embedding algorithm with their advantages as well as disadvantages.***

Keywords: Steganography, Data hiding, envelop symbols, Information Security, Least Significant Bit and techniques.

1. Introduction

Steganography word is originate from Greek words Stegano means Covered, and Grates means writing which correctly means "cover writing" [1]. In general steganography is known as "invisible" message. Steganography means to obscure messages subsistence in another medium like audio, video, image, communication. Now days, steganography systems use multimedia substance like image, audio, video etc as cover media since people often broadcast digital images over email or share them through other internet communication request. It is different from defensive the actual content of a message. In simple words it would be like that, hiding in order into other in order.

All digital file formats can be used for steganography, but the format that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that give correctness far greater than essential for the object's use and exhibit [2]. The redundant bits of an object are those bits that can be distorted without the change being detect easily [3]. Image and audio files especially comply with this obligation, while research has also uncovered other file formats that can be used for in order hiding. Figure 1 shows the four main categories of file formats that can be used for steganography.

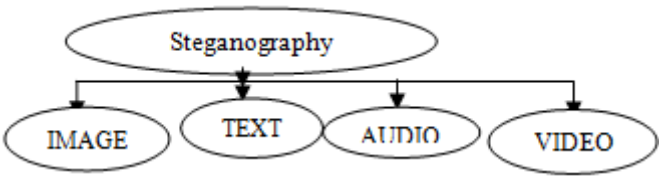


Figure 1: Categories of steganography

a) **Image Steganography:** An attractive the cover object as image in steganography is known as image steganography [4]. Normally, in this technique pixel intensities are used to hide the information.

b) **Video Steganography:** Video Steganography is a method to hide any kind of files or information into digital video format. Video is used as movers for hidden information. In general discrete cosine transform alter values which are used to hide the information in each of the images in the video, which is not clear by the human eye.

c) **Audio Steganography:** When taking audio as a carrier for in sequence hiding it is called audio steganography. It has turn into very significant medium due to voice over IP popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, and AVI MPEG for steganography.

d) **Text Steganography:** General method in text steganography, such as number of tabs, white spaces, principal writing, just like Morse code [5] and is used to achieve information hiding.

2. Classification of Image Steganography

The four main categories of steganography based on nature of file formats as well as the classification of image steganography are shown in Figure below.

A. Spatial and transform domain steganography

Based on the way of embedding data into an image, image steganography techniques can be divided into the following groups:

1. Spatial domain or Image domain.
2. Transform domain or Frequency domain.

1. Spatial Domain

This technique embeds messages in the intensity of the pixels directly. Some of the spatial domain methods are:

a) Least Significant Bit (LSB) [8]

It is one of the most common and easiest methods for message hiding. In this method, message is hidden in the least significant bits of image pixels. Changing the LSB of the pixels does not introduce much difference in the image and thus the stego image looks similar to the original image.

b) Matrix Embedding [7]

This research focuses on LSB Replacement method for data hiding. Among all message embedding techniques, the

Licensed Under Creative Commons Attribution CC BY

LSB insertion / modification is considered a difficult one to detect [6].

2. Transform Domain

In Transform domain, images are first transformed and then the message is embedded into it. These are robust methods for data hiding. It is more complex method to hide secret message into an image. It performs data hiding by manipulating mathematical functions and image transformations. Transformation of cover image is performed by tweaking the coefficients and inverts the transformation.

a) DWT [11]

A wavelet is a small wave which oscillates and decays in the time domain. The Discrete Wavelet Transform (DWT) is a relatively recent and computationally efficient technique in computer science. Wavelet analysis is advantageous as it performs local analysis and multi-resolution analysis.

b) DCT [10]

DCT is a general orthogonal transform for digital image processing and signal processing with advantages such as high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity. DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands thus making it easier to choose the band in which the watermark is to be inserted.

3. Hybrid Techniques

a) Genetic Algorithm [9]

Genetic algorithm (GA) is a stochastic seeks strategy that will mimic the actual healthy advancement offered by simply Charles Darwin throughout 1858.

STEP 1: At random, produce an initial population M (0).
STEP 2: Compute as well as help save the actual fitness f(m) for every specific individual m in the current population M(t);
STEP 3: Specify selection probabilities p (m) for every specific individual m
STEP 4: Throughout M (t) making sure that p (m) is actually proportional to f (m).
STEP 5: Crank out M (t+1) by simply probabilistically choosing individuals from M (t) to produce offspring via genetic operators.
STEP 6: Repeat step 2 until satisfying solution is actually attained.

b) Neural network [8]

Neural frameworks are made out of clear segments which work parallel. A neural framework can be arranged to perform a particular limit by changing the estimations of the weights between parts. Framework limit is controlled by the relationship between parts. There is order limits used to convey imperative yield. target

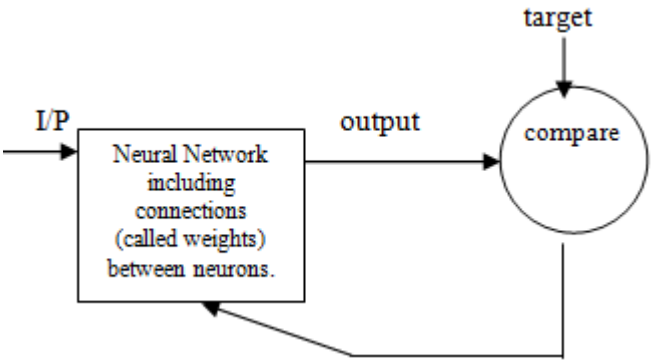


Figure 2: Neural Network

Planning can be either coordinated or unsupervised [8]. In coordinated planning structure adjusts by endeavoring to predict results for known delineations. Structure differences its expectations and the known results and increases from is misunderstandings. In unsupervised get ready structure no yield or result is exhibited as a part of planning technique.

4. Comparison Analysis

Table 1: Comparison Table

Method	Advantages	Disadvantages
LSB [8]	With the LSB replacement technique, the two parties in communication share a private secret key that key that creates a random sequence of samples of a digital signal. The encrypted secret message is embedded in the LSB's of those samples of the sequence. This digital steganography technique takes the advantage of random noise present in the acquired images	By performing the comparison of the cover image and the stego-image of above two methods datasets author come to conclude that the perceptibility ratio of the proposed method i.e. neural network is better than the LSB steganography technique.
Matrix Embedding [7]	This approach gives higher embedding capacity while giving higher embedding efficiency	Costly Method
DWT [11]	The image is transformed using DWT algorithm. The message is extracted and using DWT and decrypted to get original message as human eyes are very sensitive to colors.	Less compression Ratio
DCT [10]	Today in this insecure world transmitting of data from source to destination is very important, because the transmitting message can be easily hacked by attackers and hackers, hence the efficient way of transmitting the data over jpeg image can be done by steganography, here the stego image have been divided into blocks so this the advantage of the users, by the steganalysis	The dissimilarity in file size between stego image and cover image reduces or raises of unique colors in stego image can be used in visual detection steganalysis attack

Licensed Under Creative Commons Attribution CC BY

	cannot be able to find the secret mug in the image.	
NN [8]	Usage of NNs trained to classify pixels, and select pixels in less sensitive areas to embed more secret data. On the receiving side, the original image is not needed for extracting the embedded data.	Time consuming.
GA [9]	Genetic Algorithm is used to modify the pixel location of stego image which is another protection lock for the secret message and image. Using Genetic Algorithm's cross-over concept the column pixel shuffling happen first and the row pixel shuffling happens next and the detection of this message is complex that makes more secure. The Implementation of the algorithm yields better result as compared to other approaches as it is simple and ease of use	Applicable only against RS attack

5. Conclusion

In the few years, steganography has become a concerned field of data hiding method [12]. This paper provides an impression of different steganography method that satisfies the most important factors of steganography design. These are un-delectability, capacity and sturdiness. Steganography has its place in security. It is not proposed to replace cryptography but supplement it. Hiding a message with steganography method reduces the chance of a message being detected. However, if that message is also encrypted, if exposed, it must also be cracked .There is an infinite number of steganography applications but Genetic algorithm is more efficient This paper explores a tiny fraction of the art of steganography. It goes well beyond simply embed text in an image.

References

[1] Pfitzmann, B., Information hiding terminology - results of an informal plenary meeting and additional proposals. In: Proceedings of the First International Workshop on Information Hiding. Springer-Verlag, London, UK, pp. 347–350. **(1996)**.

[2] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.

[3] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996.

[4] N. Johnson and S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer, pp. 26-34, February **(1998)**.

[5] N. F. Johnson and S. Katzenbeisser, "A Survey of steganographic techniques. in Information Hiding Techniques for Steganography and Digital Watermarking,S.Katzenbeisser and F.Petitcolas, Ed. London: Artech House, **(2000)**, pp. 43-78.

[6] S. C. Katzenbeisser. Principles of Steganography. in Information Hiding Techniques for Steganography and Digital Watermarking", S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, **(2000)**, pp. 43-78

[7] Divya, "An approach to adaptive steganography based on matrix embedding" IEEE, 2007.

[8] Imran Khan , "An Efficient Neural Network based Algorithm of Steganography for image", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1 , Issue 2.

[9] Rehana, "Best Approach for LSB Based Steganography Using Genetic Algorithm and Visual Cryptography for Secured Data Hiding and Transmission over Networks", IJARCSSE, Volume 4, Issue 6, June 2014.

[10] Suchitra, "Image Steganography Based On DCT Algorithm for Data Hiding", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 11, November 2013.

[11] Archana, "Image Steganography using DWT and Blowfish Algorithms", IOSR Journal of Computer Engineering (IOSR-JCE), pp-15-19, 2013.

[12] Luo, Xiang-Yang, et al. "A review on blind detection for image steganography."Signal Processing 88.9 (2008): 2138-2157.

Licensed Under Creative Commons Attribution CC BY