A Comparative Study of Various Approaches of Image Stenography

Deepika Sharma[1], Jaskiran Kaur[2]
[1]*M.Tech (Scholar),* [2]*Assistant Professor*
Department of Information Security, Chandigarh Engineering College, Landran, Mohali

Abstract **-** Image steganography detection is not only distinguishing cover images (the normal images) and stego images, but also regulates the steganography procedures of the stego-pictures, and extracts the embedded information, of which the precondition is to determine the image steganography algorithm. Image Steganography is generally more preferred media because of his inoffensiveness and desirability. Moreover conversation of greetings through digital means is on the increase through the increased use of the internet and ease of comfort and flexibility is sending them. Technology advancement in design of cameras & arithmetical picture being stored in cameras and then transfer to PCs has also enhanced.

Keywords **-** Image Steganography, digital images, advantages and disadvantages and Steganography techniques.

I. INTRODUCTION

Steganography is the skill of embedding the actual presence of a confidential text in innocuous-looking cover medium, such as text, audio, image and video. The main purpose of steganography is for secret communication via public channel without drawing any doubt. As the conflicting of steganography, steg-analysis is advanced to detect the hidden messages transmitted through the shield media. Through the improvement of network & multimedia expertise, various videos can be acquired from the Internet easily.

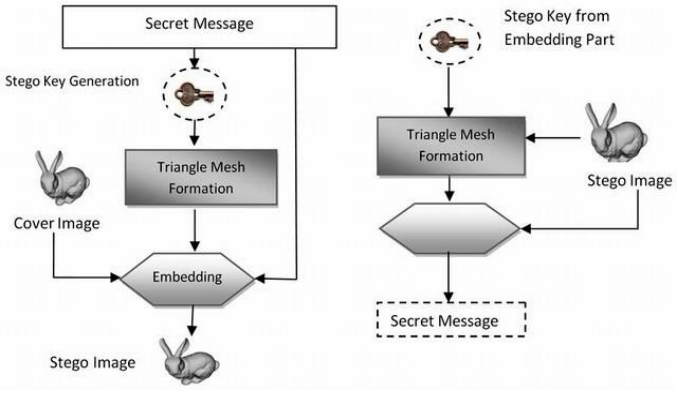

Fig.1 Process of Steganography

Thus, video becomes a very promising cover candidate that has a very high payload volume for information hiding. Currently, although several steganographic procedures for video have been proposed. Steganography, as definite above is a method to hide information in picture in such a way that it is unperceivable. To achieve such consequence one may reason of slicing the raw information that is the info to be hidden in equal number of block and hide it in specific areas within an image. Such a thought interprets that the concept is not vivid. That is, one is not able to extract the true beauty of Steganography.[1]

II. TYPES OF STEGANOGRAPHY

The steganography can be classified according to its position and objectives. So; several kinds of steganography are:

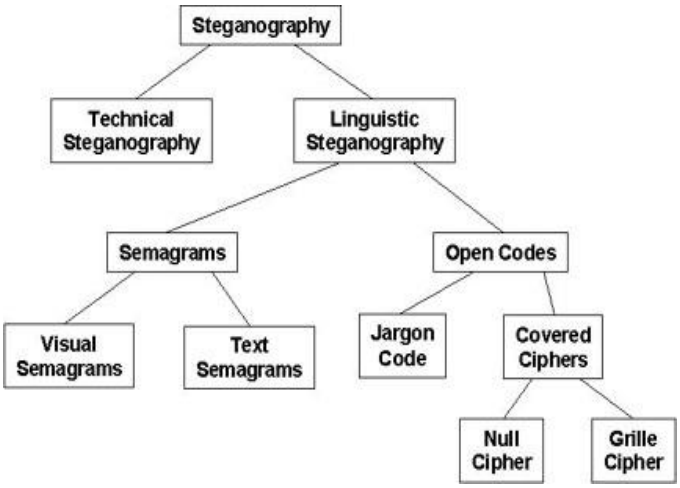

Fig.2: Types of Stenography

A. Linguistic Steganography

Linguistic method is used to embed the information within the hiding place text in non-obvious way such that the occurrence of text is unnoticeable to an outsider. It is divided into two types:

i) Seagram's: It uses only symbols and signs to embed the info. It is further characterized into dualistic ways:

- **Visual Seagram's:** A visual dekagrams usages physical substances used each day to convey a missive. For example: the putting of items on a particular website.
- **Text Seagram's:** This type is used to hides a message by modify the appearance of the carrier text, or by changing font scope and category, or by adding additional space among words and by using different flourished in letters or handwritten text.

B. Open Cipher

In this method the missive is entrenched in legitimate paraphrases of cover text in the method such that it seems not clear to an unsuspecting spectator. It can be achieved by two ways viz., Jargon which is unspoken individual by a collection of peoples and Code which uses certain concealed ciphers to hide a memo openly in the carrier medium. A subsection of jargon cyphers are cue codes, wherever certain planned phrases convey meaning.

C. Technical Steganography

Practical steganography usages special outfits, plans or scientific methods to hide a information. In this type one can use invisible ink, computer founded approaches, microdots or several embedding places to keep message secret.

i) Cover: The cover message is the transporter of the information such as picture, music, video, textual, or certain other digital media. The cover is alienated into chunks and information bits which are secret in every block. The information is encoded by changing various properties of hiding place image. The cover chunks remain unaffected if message block is zero [2**].**

a. Image Steganography: Taking the cover entity as picture in steganography is recognized as image steganography. Usually, in this method pixel intensities are used to embed the data.

b. Network Steganography: When attractive hiding place object as network protocol, such as TCP, UDP, IP, ICMP etc, anywhere procedure is used as transporter, is recognized as network protocol steganography. In the OSI network layer prototypical there exist secret channels where steganography can be attained in unused shot bits of TCP/IP fields

c. Video Steganography: This is a method to embed any type of files or message into digital video format. Video is recycled as transporter for hidden data. Generally discrete cosine transform (DCT) alter standards that used to embed the information in every of the images in the video, which is not noticeable by the humanoid sense. Video steganography treatments such as MPEG, H.264, Mp4, AVI or additional video formats.

d. Audio Steganography: When captivating music as a transporter for information embedding it is called audio steganography. It has become very significant average owing to voice ended IP (VOIP) approval. Audio steganography usages digital audio formats such as WAVE, MIDI, AVI MPEG or etc for steganography.

e. Text Steganography: Universal procedure in textual steganography, such as amount of tabs, fair similar Morse code, white places, capital letters, and etc. is used to achieve information hiding. [3]

III. ADVANTAGES AND DISADVANTAGES OF STENOGRAPHY

Advantages

1. It is used to way of hiding not the information but the password to reach the information.
2. Difficult to detect. Only receiver can detect.
3. Can be applied differentially in digital image, audio and video file.
4. It can do with large number of software.

Disadvantages

1. Huge number of data, huge files size, so someone can suspect about it.
2. If this technique gone wrong hands like hacker, terrorist, criminals then this can be very much dangerous to all.

III. STEGANOGRAPHY APPLICATIONS

There are several requests for digital steganography of pictures, containing copyright protection, feature tagging, & surreptitious communication. Patent sign or watermark can embedded inside an image to identify it as intellectual stuff. If somebody attempts to usage this image devoid of permission, we can prove by extracting the watermark. In piece classification, slogans, comments, time imprints, and other descriptive elements can be embedded inside an image. Repetition the stego–image likewise copies of the entrenched features and only gatherings who posses the decoding stego-key will be talented to excerpt and opinion the structures. On the other hand, secret communication does not advertise a covert communication through using steganography. So, it can escape inspection of the sender, message and recipient. This is effective only if the hidden communication is not detected by the others people. [4]

IV. RELATED WORK

A high PSNR value, and an nearly indistinguishable histogram when likened to the before stego image. We also discuss the robustness of this algorithm under attack methods such as steganalysis. **Jinsuk Baekl et al 2010[5]** A high capacity stenographic technique in which surreptitious data is entrenched in Intermediate Important Bit planes of the cover image. The data to be embedded is wrecked down in chunks

of relatively decreasing distances and each block is embedded in the cover media under control of a extremely secure key. This effort shows attractive outcomes with respect to imperceptibility and capacity when compared through a few stated techniques in fvadding to providing adequate data security **Shabir A. Parah et al 2012.[6]** Improved scheme of password verification and user secrecy using Elliptic Curve Cryptography (ECC) and stegnography. The future scheme also delivers privacy to the customer. Based on scheme performance criteria such as immunity to known occurrences and functional structures, we came to the deduction that the proposed scheme is much efficient and solves several hard security threats **Vineeta Singh et al 2014[7]** Detecting data hiding in motion vectors of compressed video and propose a new steganalytic procedure based on the shared constraints of gesture vectors. The constraints of motion vectors from manifold surrounds are analyzed and formulized through three functions, and then statistical features are extracted based on these functions. Furthermore, we also join calibration method to recover the detection accuracy. Experimental results demonstrate that the projected method can efficiently attack typical motion-vector based video steganography **Xikai Xu et al 2013.[8]** Applied into a example tool coded in VB.NET. The obtainable approach is effective in a way that multiple file arrangements such as jpeg, bmp, gif & tiff are likewise supported. A agreed of sample images were processed with the tool and the results of the original experiments designate the possible of the obtainable approach not only in terms of secure stenography but similarly in relations of fast data communication over internet **Imran Sarwar Bajwa et al 2011.[9]**

V. DIFFERENCE BETWEEN FREQUENCY DOMAIN AND SPATIAL DOMAIN

Spatial domain techniques directly deal with the image pixels. The pixel values are operated to achieve desired improvement. Spatial domain methods like the logarithmic alter, power law transforms, histogram equalization, and are based on the direct manipulation of the pixels in the image. Spatial techniques are particularly useful for directly altering the gray level values of individual pixels and hence the overall contrast of the entire image. But they usually enhance the whole image in a uniform manner which in many cases produces undesirable results. It is not possible to selectively enhance edges or other required information effectively. Now we see two techniques of spatial domain techniques.

Frequency domain: Transformation or frequency domain techniques are based on the manipulation of the orthogonal transform of the image rather than the image itself. Transformation domain techniques are suited for processing the image according to the frequency content. The principle behind the frequency domain methods of image enhancement consists of computing a 2-D discrete unitary transform of the image, for instance the 2-D DFT, manipulating the transform coefficients by an operator M, and then performing the inverse transform. The orthogonal transform of the image has two components magnitude and phase. The magnitude consists of the frequency content of the image. The phase is used to restore the image back to the spatial domain. The usual orthogonal transforms are discrete cosine transform, discrete Fourier transform, Hartley Transform etc. The transform domain enables operation on the frequency content of the image, and therefore high frequency content such as edges and other subtle information can easily be enhanced**.[10]**

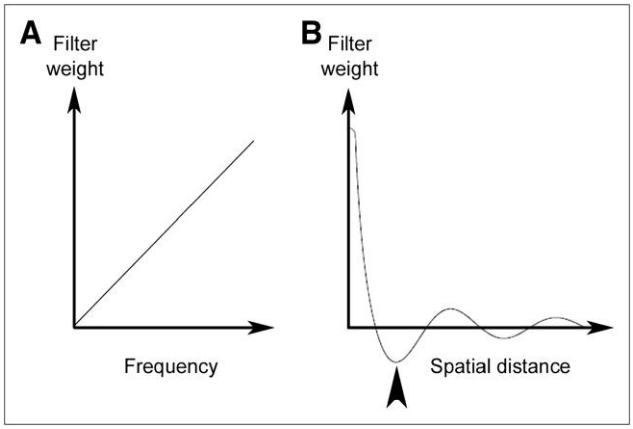

Fig.3: Frequency domain & Spatial domain

VI. DIFFERENCE BETWEEN LSB AND DWT

LSB (LEAST SIGNIFICANT BIT SUBSTITUTION): LSB substitution is the most adapted method to increase capacity by reducing the quality of image.A digital image is represented by two digits that is 1 or 0. The concept of LSB is associated with the bit position in an image. The lower (rightmost) bits in an 8 bit grey level plane of host image carries very less significant information. While the most significant bits (leftmost) carries the most of the information. LSB substitution makes use of this bit position and smartly replaces the least significant bits of host image with most significant bits of secret image.

DWT (DISCRETE WAVELET TRASFORM): Transformation is generally used to uncorrelate the wavelet coefficient. It converts an image from spatial domain to frequency domain. The mathematical representation of wavelet transform is given by formula : F(a,b) = $f\ x\ \Psi\ a,b \infty * -\infty\ (x)\ dx$ (3) Wavelet transform is a convenient means to split an image into 4 frequency bands.

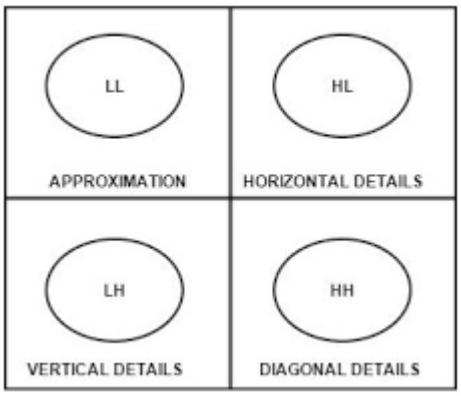

Fig.4: Frequency band

As seen from the Fig , LL band is low frequency band containing most of the information of the secret image. Steganography makes use of this band for altering or modifying data to make it undetectable with human eye.Thus more decomposition levels are applied to an image to make it look like an unaltered image**.[11]**

VII. DIFFERENCE BETWEEN STEGNOGRAPHY AND TEXT WATER MARKING

The main goal of steganography is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot detect the presence of m in d'. The main goal of watermarking is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot remove or replace m in d'. It is also often said that the goal of steganography is to hide a message in one-to-one communications and the goal of watermarking is to hide message in one-to-many communications. Shortly, one can say that cryptography is about protecting the content of messages, steganography is about concealing its very existence. Steganography methods usually do not need to provide strong security against removing or modification of the hidden message. Watermarking methods need to to be very robust to attempts to remove or modify a hidden message.

VIII. CONCLUSION

As steganography becomes more widely used in computing there are issues that need to be resolved. There are a wide variety of different techniques with their own advantages and disadvantages. Image enhancement techniques such as spatial and transform domain technique are important techniques. Most of the techniques are useful for altering the gray level values of individual pixels and hence the overall contrast of the entire image. Some commonly known steganography techniques were implemented. LSB substitution and DWT are widely used for the same. Each of the method has its own advantage. LSB method embedded about 60% of data bits and retained the same size of the image because only the pixels values were shuffled. In DWT method, the given data is decomposed to get uncorrelated data which changes the image composition.

IX. REFERENCES

[1]. Narayana, Sujay, and Gaurav Prasad. "Two new approaches for secured image steganography using cryptographic techniques and type conversions."Signal & Image Processing: An International Journal (SIPIJ) Vol 1.2 (2010): 60-73.

[2]. Kaur, Navneet, and Sunny Behal. "A Survey on various types of Steganography and Analysis of Hiding Techniques."

[3]. Singh, Kamred Udham. "A Survey on Image Steganography Techniques."International Journal of Computer Applications 97.18 (2014).

[4]. Amin, Muhalim Mohamed, et al. "Information hiding using steganography."Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on. IEEE, 2003

[5]. Lin, Chang-Chou, and Wen-Hsiang Tsai. "Secret image sharing with steganography and authentication." Journal of Systems and software 73.3 (2004): 405-414.

[6]. Parah, Shabir A., Javaid A. Sheikh, and G. M. Bhat. "Data hiding in intermediate significant bit planes, a high capacity blind steganographic technique." Emerging Trends in Science, Engineering and Technology (INCOSET), 2012 International Conference on. IEEE, 2012.

[7]. Singh, Vineeta, Priyanka Dahiya, and Sushil Singh. "Smart card based password authentication and user anonymity scheme using ECC and steganography." Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE, 2014.

[8]. Xu, Xikai, et al. "Video steganalysis based on the constraints of motion vectors." Image Processing (ICIP), 2013 20th IEEE International Conference on. IEEE, 2013.

[9]. Bajwa, Imran Sarwar, and Rubata Riasat. "A new perfect hashing based approach for secure stegnograph." Digital Information Management (ICDIM), 2011 Sixth International Conference on. IEEE, 2011.

[10]. Mundhada, Snehal O., and V. K. Shandilya. "Spatial and Transformation Domain Techniques for Image Enhancement." International Journal of Engineering Science and Innovative Technology (IJESIT) 1.2 (2012): 213-216.

[11]. Kumar, Vipin, and Dinesh Kumar. "Performance evaluation of dwt based image steganography." Advance Computing Conference (IACC), 2010 IEEE 2nd International. IEEE, 2010.