[Soni, 3(6): June 2016]
DOI - 10.5281/zenodo.57125

ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

STUDY OF DATA HIDING TECHNIQUES FOR IMAGES

Ashish Soni[*1], Chirag Jain[2] and Anshul Maloo[3]
[*1,2,3]Assistant Professor, ECE Department, Acropolis Technical Campus, Indore

ABSTRACT

As the amplification of internet is one of the main feature of information technology, data hiding techniques has taken a important role for the transfer of multimedia content. One of the essential properties of digital information is that it is in principle very easy to create and distribute unlimited number of its duplicates. The fact that an unlimited number of perfect copies of text, image, audio and video data can be illegally created and distributed requires studying ways of embedding copyright information and serial numbers in image, audio and video data. Steganography and watermarking bring a variety of very significant techniques how to hide important information in an imperceptible and/or irremovable way in image, audio and video data. Steganography and watermarking are main part of the fast emerging area of information hiding. In this research paper, we survey on existing work which used different techniques for image steganography and image watermarking.

Keywords: *Data Hiding; Steganography; Watermarking; LSB Substitution; Spread Spectrum; PSNR.*

I. INTRODUCTION

In the current developments of the world, the technologies have highly developed so much that most of the persons prefer using the internet as the primary medium to transfer information from one end to another across the world. There are many possible ways to transmit data using the internet. The information transition is made very simple, fast and exact using the internet. However, one of the main problems with transferring information over the internet is the 'security threat'. In order to increase the security features in information transfers over the internet and for information hiding into digital media, many techniques have been developed like: Cryptography, Steganography and Digital watermarking.

The most common way to do this is to transform the data into a changed form. The resulting data can be understood only by those who know how to return it to its original form. This technique of protecting information is known as encryption. A major problem to encryption is that the existence of data is not hidden. Data that has been encrypted, however unreadable, still exists as data. If given adequate time, someone could eventually decrypt the data. A resolution to this problem is steganography [1].

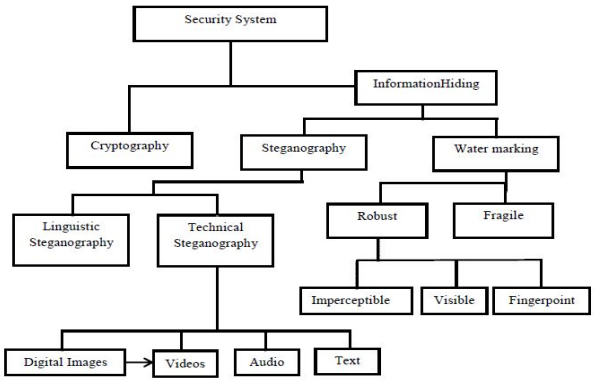

Fig.1: The different disciplines of data hiding techniques

Steganography is the art and science of writing hidden messages in such a manner that no one, apart from the sender and intended receiver, suspects the existence of the message, a form of security through obscurity. Steganography basically consists of three things: cover object (used to hide secret message), secret message to be embed, and stego object (cover object after hiding the secret data).

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the subsistence of a message secret [2]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised.

Many different steganography methods have been proposed during the last few years; most of them can be seen as substitution systems. Such methods try to substitute redundant parts of an image with a secret message; their main disadvantages being the relative weakness against cover modifications.

Watermarking is used to verify the identity and authenticity of the owner of a digital image. A watermark can be considered to be some kind of information that is embedded into underlying data for tamper detection, localization, ownership proof, and/or traitor tracing purposes (Agrawal et al., 2003). Watermarking techniques apply to various types of host content [3]. The main objective of watermarking is to hide a message *m* in some image 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'.

Watermarking techniques are particular embodiments of steganography. However, their usage aim is different. A watermark contains copyright information of the cover object. The robustness is a major anxiety for watermarking because the valuable data is protected (or the ownership is proved) as long as the watermark is present in it. On the other hand, hidden message may have no value and no relationship with the cover in steganography.

Earlier used spatial domain methods of steganography are based on Least Significant Bit (LSB) substitution which giver better PSNR result. Alternatively other methods involve steganography in frequency domain. Various transforms have been used for various data hiding techniques. Discrete Fourier transform (DFT), Discrete Cosine transform (DCT) or discrete fractional Fourier transform (DFrFT) found numerous applications in image processing. The area of image processing applications includes steganography, watermarking, compression, encryption [4].

In this manuscript, we are focusing on a watermarking method for digital images that uses either DFT, DCT OR DFrFT because in many literatures, it is pointed that the frequency domain techniques are more robust then spatial domain techniques. So spread spectrum techniques are used which embed secret messages adopting ideas from spread spectrum communications.

Steganography can be used for many applications such as intelligence agencies, defense organizations, in identity cards, for copyright control, in medical imaging etc. While watermarking is used for data protection, data authentication, copyright protection, source tracking and annotation of photographs.

This paper is organized as follows. Section II discusses the basics of steganography and its types i.e. the spatial domain method which involves encoding at the LSBs level, frequency domain techniques and comparison of different data hiding technique. Section III describes the details of watermarking. In section IV, image quality measures are discussed. And last, section IV gives the conclusion.

II. STEGANOGRAPHY

The word steganography is originally derived from Greek words which mean “Covered Writing” (Greek words “stegos” meaning “cover” and “grafia” meaning “writing”). It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave’s head, tattooed a message on his skull and the slave was dispatched with the message after his hair grew back. With the boost in computer power, the internet and with the development of digital signal processing (DSP), information theory and coding theory, steganography has gone “digital” [5].

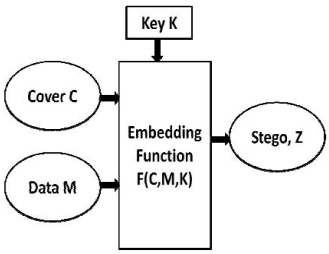

Fig.2: Basic Steganography Model

The main objective of steganography is to communicate securely such a way that the true message is not visible to the observer. That is unwanted parties should not be able to distinguish any sense between cover-image and stego-image. Thus the

ISSN 2348 – 8034
Impact Factor- 4.022

stego-image should not deviate much from original cover-image. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. The schematic representation of the steganography is given in Fig. 3:

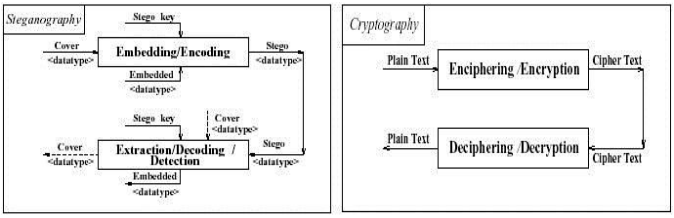

Fig. 3: Steganography versus Cryptography

The techniques of data hiding i.e. steganography, watermarking and cryptography are interlinked. The first two are quite difficult to tease apart especially for those coming from different disciplines. Table 1 summarizes the differences and similarities between steganography, watermarking and cryptography [5].

Table 1: Comparison of steganography, watermarking and crytography [4]

Creterion / Method	**Stegano graphy**	**Water marking**	**Crypto graphy**
Carrier	Any digital media	Mostly image/audio files	Usually text based
Secret Data	Payload	Watermark	Plain text
Key	Optional		Necessar y
Inputt files	Atleast two unless in self-embedding		One
Output files	Stego-file	Watermarked-file	Cipher-text
Objective	Secrete communicatio n	Copyright preserving	Data protectio n
Visibility	Never	Sometimes	Always
Flexibilty	Free to choose any cover	Cover choice is restricted	N/A
Fails When	It is detected	It is removed/replace d	De-ciphered

On the basis of the image formats i.e. Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and to a lesser extent- Portable Network Graphics (PNG), image steganography are of two types:

ISSN 2348 – 8034
Impact Factor- 4.022

(i) Steganography in the image spatial domain

(ii) Steganography in the image frequency domain

Steganography in the image spatial domain: Here spatial features of image are used. This is a simplest steganographic technique that embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. In a gray-level image, every pixel consists of 8 bits. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly [4]. The mathematical representation for LSB is as equation 1:

$$x_i' \equiv x_i - x_i \bmod 2^k + m_i \qquad (1)$$

In Equation (1), x_i' represents the i^{th} pixel value of the stego-image and xi represents that of the original cover-image. m_i represents the decimal value of the i^{th} block in the confidential data. The number of LSBs to be substituted is k. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as in equation 2:

$$x_i = x_i \bmod 2^k \qquad (2)$$

Hence, a simple permutation of the extracted m_i gives us the original confidential data [6]. This method is easy and straightforward but this has low ability to bear some signal processing or noises. And secret data can be easily stolen by extracting whole LSB plane. A general framework showing the underlying concept is highlighted in Fig. 4.

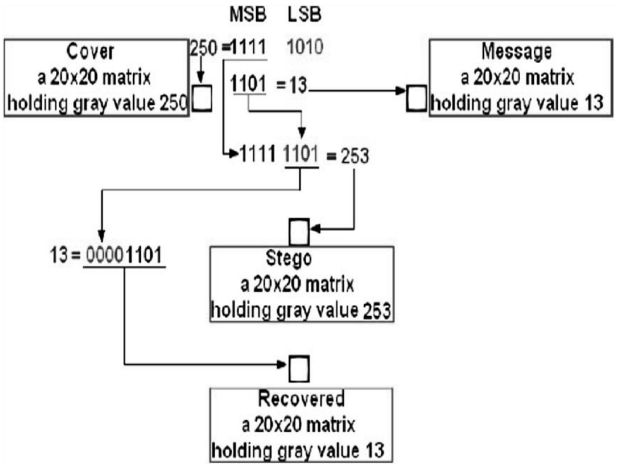

Fig. 4: Steganography in spatial domain. The effect of altering the LSBs up to the 4th bit plane

In the case of steganography, the reconstructed image is only an approximation to the original. Although many performance parameters exist for quantifying image quality, it is most commonly expressed in terms of mean squared error (MSE) and peak signal to noise ratio (PSNR). For a good steganography, MSE should be less. PSNR is provided only to give us a rough approximation of the quality of steganography. PSNR should be more for good perception of received image.

Steganography in the image frequency domain: Robustness of steganography can be improved if properties of the cover image could be exploited. Taking these aspects into consideration working in frequency domain becomes more attractive. Here, sender transforms the cover image into frequency domain coefficients before embedding secret messages in it [7]. Using transform-domain techniques it is possible to embed a secret message in different frequency bands of the cover. These methods are more

[Soni, 3(6): June 2016] ISSN 2348 – 8034
DOI - 10.5281/zenodo.57125 Impact Factor- 4.022

complex and slower than spatial domain methods; however they are more secure and tolerant to noises. Frequency domain transformation can be applied either in Fast Fourier transform i.e. FFT, Discrete Cosine Transform i.e. DCT or Discrete Fractional Fourier transform i.e. DFRFT.

III. WATERMARKING

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time. In general, any watermarking scheme consists of the following three parts:

(i) The watermark signal,

(ii) Watermark embedder that embeds the watermark into the media

(iii) Watermark detector that verifies the presence of watermark

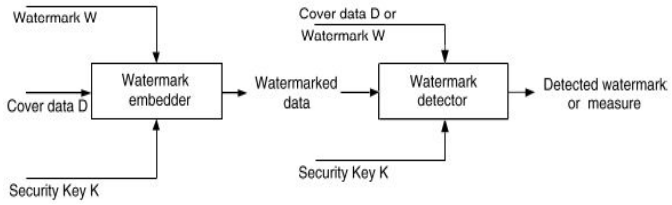

Fig. 5: A typical watermarking system

Above Fig. 5 is a conventional watermarking system [8] consists of watermark embedder and watermark detector. The inputs to the watermark embedder are the watermark, the cover media data and the embedding security key. The watermark can be a number sequence, a binary bit sequence or may be an image. The key is used to enhance the security of the whole system. The output of the watermark embedder is the watermarked data. The inputs to the watermark detector are the watermarked data, the security key and, depending on the method, the original data and/or the original watermark. Basically there two type of watermarking scheme [9]:

I. **Visible Watermarking:** As the name suggests, visible watermarking refers to the information visible on the image or video or picture. Visible watermarks are typically logos or text. For example, in a TV broadcast, the logo of the broadcaster is visible at the right side of the screen.

II. **Invisible Watermarking:** refers to adding information in a video or picture or audio as digital data. It is not visible or perceivable, but it can be detected by different means. It may also be a form or type of steganography and is used for widespread use. It can be retrieved easily.

Major properties of the watermarks are robustness and fidelity [10]. However, a watermark may not satisfy all of these properties. In addition, that may be not required for all types of watermarks. For a visible watermark, fidelity is not an issue, however, for an invisible watermark it is one of the most important issues.

A robust watermark must resist to possible attacks and remains detectable after applied attacks. However, it is probably impossible for a watermark to resist all kind of attacks, in addition, it is unnecessary and excessive. The robustness criterion is specific for the type of application.

High fidelity means that, the amount of degradation caused by the watermark in the cover is imperceptible for the viewer. It is a primary concern for invisible types of watermarks. However, in most applications increasing the robustness by embedding a more powerful watermark signal may result in loss of fidelity. In this case a trade-off must be made and fidelity or robustness may be decreased to a required level [10].

[Soni, 3(6): June 2016] ISSN 2348 – 8034
DOI - 10.5281/zenodo.57125 Impact Factor- 4.022

IV. IMAGE QUALITY MEASURES

Image quality measures are of great importance in various image processing applications. Because, the reconstructed image is only an approximation to the original. Although many performance parameters exist for quantifying image quality, it is most commonly expressed in terms of mean squared error (MSE) and peak signal to noise ratio (PSNR) [11]. MSE is defined as the mean square of difference of corresponding pixel values in the original image and stego-image or watermarked image. Mathematically it is defined for an image $f(i, j)$ of size M × N as:

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[f'(i,j) - f(i,j)]^2$$

The PSNR is the only rigorously defined metric. The main reason for this is that no good rigorously defined metrics have been proposed that take effect of the Human Visual System (HVS) into account. PSNR is provided only to give us a rough approximation of the quality of steganography. The PSNR in mathematical form for an image of size M × N as can be given as:

$$PSNR = 10log_{10}\left[\frac{M \times N}{MSE}\right]$$

V. CONCLUSION

To transmit confidential data, protection is necessary to protect them from malicious users to illegally copy, destroy or change them on internet. Digital Watermarking is more secure and easy method of data hiding for copyright control and data authentication. While steganography plays an vital role in secret communication. An overview of steganography and watermarking was presented along with applications that can benefit from the technology. Immense research in steganography and watermarking continues to expand the perceptual transparency, robustness and capacity of information hiding systems.

REFERENCES

1. *T. Morkel, J. H. P. Eloff, M. S. Olivier, "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, South Africa, 2005.*
2. *Wang, H and Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004*
3. *Sukriti Bhattacharya, AgastinoCortesi, "Data Authentication by Distortion Free Watermarking", ICSOFT 2010.*
4. *Ashish Soni, Rakesh Roshan, Jitendra Jain, "Image Steganography in Discrete Fractional Fourier Transform Domain", International Conference on Intelligent System and Signal Processing 2013, ISBN no: 978-1-4799-0316-0©IEEE.*
5. *G.J. Simmons, "The prisoners' problem and the subliminal channel", in: Proceedings of International Conference on Advances in Cryptology, CRYPTO83, August 22–24, 1984, pp. 51–67.*
6. *Johnson, N. F. and Jajodia, S, "Exploring Steganography: Seeing the Unseen." IEEE Computer, 31 (2): 26-34, Feb 1998.*
7. *Anjali A. Shejul and Umesh L. Kulkarni, "A Secure Skin Tone based Steganography Using Wavelet Transform", International Journal of Computer Theory and Engineering, Vol.3, No.1, February, 2011, 1793-8201*
8. *Zheng, D., Liu, Y., Zhao, J., and El Saddik, A. "A survey of RST invariant image watermarking algorithms", ACM Computing Surveys, Volume 39, No. 2, Article 5, June 2007.*
9. *K.Sridhar et al, "Comparison of Digital Watermarking with Other Techniques of Data Hiding", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 350-353*
10. *R. van Schyndel, A. Tirkel, and C. Osborne, "A digital watermark," in Proceedings of ICASSP. Piscataway, NJ: IEEE Press, vol. II, pp. 86–90, 1994*

Abbas Cheddad, JoanCondell, Kevin Curran, PaulMcKevitt, "Digital image steganography: Survey and analysis of current methods", Elsevier, Signal Processing 90 (2010) 727–75