www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 9 Sep 2015, Page No. 14396-14400

A Comparative Study: Image Steganography and Watermarking

Kamred Udham Singh[1], Achintya Singhal[2]

[1]DST-CIMS, Banaras Hindu University, Varanasi U.P., India
kamredudhamsingh@mail.com

[2] Department of Computer Science, Banaras Hindu University,
Varanasi U.P., India
Achintya.singhal@gmail.com

Abstract: ***Steganography technique plays an important role in information hiding in any digital cover object. Security of information on internet against unauthorized access has become a prime problem. Due to this, steganography technique becomes more popular. Steganography is the science which includes secret communication in an appropriate digital cover objects viz. audio, image, text and video files. The main objective of steganography technique is to hide the presence of the embedded information in carrier file and other objectives are robustness, Un-detectability and capacity of the concealed data. Steganography is separate from other related techniques viz. watermarking and cryptography in term of robustness and Un-detectability of information. Watermarking is a technique that hides information in digital image to protect intellectual properties and copyright, such as logo for proving ownership. Steganography and watermarking are important techniques to conceal important data in cover object an undetectable and irremovable way. Both techniques are the fast developing area of information hiding. This paper delivers a comparative study on digital images steganography and watermarking techniques and significant research growths are also discussed.***

Keywords: Steganography, watermarking, carrier, robustness and information.

1. Introduction

1.1 Steganography

Steganography technique is the art of concealing information imperceptibly in a digital cover medium such as image, audio, and video. The word Steganography derived from the Greek words which mean covered writing in any object [1]. The main objective of steganography is to conceal the existence of the information in the cover medium. Steganography, Cryptography and Watermarking are mostly used to hide the message in image and these techniques are closely related to each other [2]. The strong point of steganography over cryptography is that the hidden messages do not attract attention of third party when it transmitted to the desired recipients because of robustness and undetectably. As observed, during the last several decades, an exponential growth of use of multimedia data over the Internet in the form of Digital Images, Video and Audio files. The rise of digital data on the internet has further enhanced the research work devoted to steganography. The several applications of steganography like secure multimedia watermarking, military communications and fingerprinting applications for the authentication determination to control the problem of digital piracy. Many steganographic algorithms can be used for these tasks but these are not perfect applications of steganography.

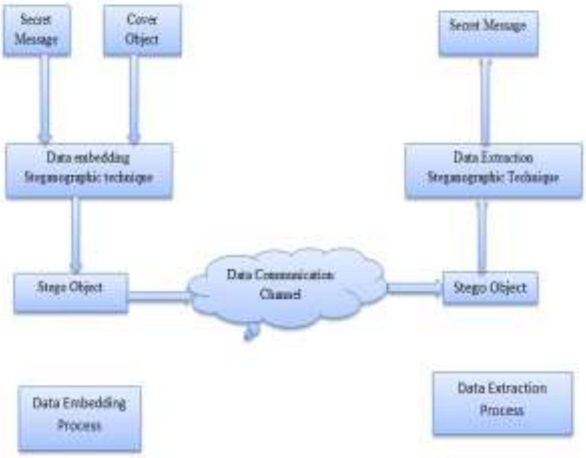

Fig1 Steganography system

In Steganography, generally some secret data embed into an innocuous looking simple image as a cover image and create a Stego image file. The Stego image visually seems to be same as cover image but hides the secret data inside it and transmitted to the recipients over the communication channels. When the desired recipient receives the Stego image, then follow the data extraction process to recover the secret data. To improve the security of the hidden data there may some keys included in this process of data embedding and extraction. The given figure depict that secret message is hide in the cover object using data embedding steganography technique and generate a stego file. Stego file send to the receiver use using data communication channel. Receiver extracts the stego file via data steganographic technique and get the secrete message.

1.2. Watermarking

Watermarking is a technique of hiding information in digital image to protect intellectual properties and copyright in the logo for proving ownership. Due to development of information communication technology distribution of multimedia data is become very easy. Now it is an important issue to protect digital data from many attacks viz. piracy, counterfeiting and malicious maniple. Number of mechanism developed to provide the solution of this problem, digital watermarking is one of them. Watermark can be visible or invisible. Digital watermarks are embedded to digital images which can be catch by a computer but it is imperceptible to the Human Visual System (HVS). Watermark containing information about the owner of the image or a logo or even about the image itself. It is used to prove copyright authentication about an image in order to decrease copyright infringement. To help embedded the digital watermark, varies the watermark energy within the digital image so that it is imperceptible in both detailed and flat areas. There are two important characteristics for image watermarking are, first is embedding watermark should not reduce the quality and visually of image. The second characteristics are robustness which means that the attacker can't discard Watermark form image [3]. Generally, any watermarking technique consists of three parts [3] [4]:

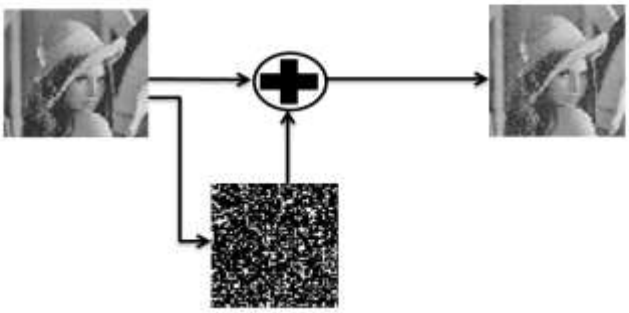

Fig2 Watermarking System

- **Watermark**: It is pattern of bits which are embedded into image.
- **Watermarking Embedding Algorithm:** Watermark is embedded into image using any watermarking algorithms like LSB. Watermark is a uniquely identified the image object.
- **Extraction or Detection Algorithm:** It authenticates the image and determining both the owner of image and the integrity of the image. It extracts the digital watermark from the image using extraction algorithms.

2. Factors which Affecting Digital Watermark and Steganography Strength

Steganography and watermarking both are data hiding techniques. When watermark embedding or data embedding process chosen the strength of a digital watermark or steganography are also affected by the following factors:

• **Image variations/randomness**:

Successful embedding of a watermark in digital image is dependent on the randomness and variation existing in the pixels of the image. As an example, if an image which contains maximum flat color regions in comparison to detailed areas, select higher watermark strength so that the digital watermark will overcome the boundaries of the specific image and this may result in a visible watermark.

• **Image size**: Steganography and watermarking both conceal data in image but the size of image should not increase after the data embedding as far as possible. Due to size attackers attacks on the suspected large size image. The large number of pixels in the digital image is appropriate for digital watermarking and steganography because data is embedded in these pixels.

• **Compression**: After data embedding process if saving the watermarked image or stego image in a compressed format, it may affect the durability of hidden message in stego image or digital watermark. So the recommended least size for an image which will be compressed is 256 *256 pixels.

3. Discipline of Information Security

Three common discipline of information security are cryptography steganography and watermarking. All these techniques are used for embedding data in cover image. The following figure depicts the application and fundamental characteristic of these techniques. Steganography and watermarking are used for information hiding whereas cryptography is an information encryption technique. Steganography hide the secret information in image and focus on information security but watermarking embedded logo in image visible or invisible form for content authentication.

4. Digital Image Steganography Techniques

Image Steganography technique concentrate mainly for images [6] [7] for data hiding viz. gray-scale and color images. Gray scale image are commonly used for data hiding in comparison to colour image [8]. Here we give an overview on image steganography techniques. Some popular image formats are JPEG, GIF, PING and GIF.

4.1 Spatial domain steganography

In spatial domain steganography technique the data is embedded into intensity of cover image pixels. Data embedding rate is measured in bits per pixel. Spatial domain techniques are very easy to apply due to its simplicity. Steganographer modifies the secret data and cover image in the spatial domain. Least significant bit (LSB) technique is commonly used in spatial domain it hides data in least significant bit of the pixels value and BMP image are usually considers for data hiding because they use lossless data compression. According to the embedding way major kinds of steganography are the following [9] [10] [11] [12].

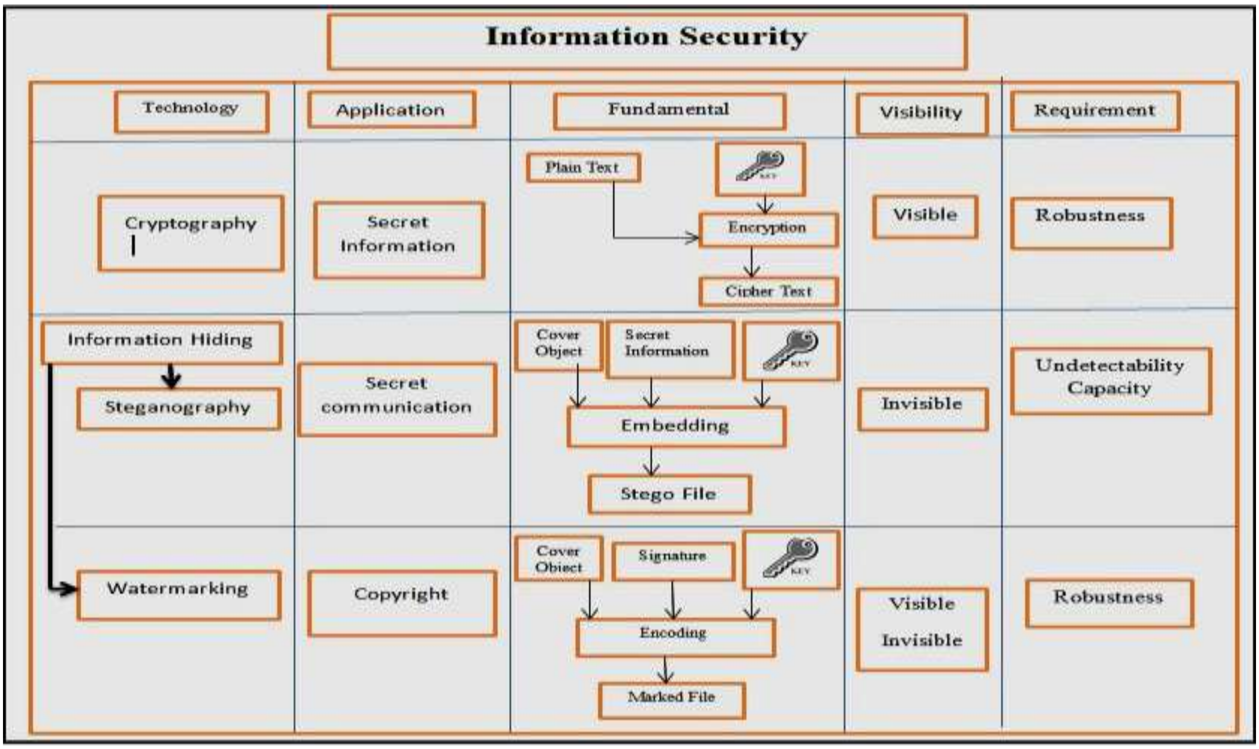

Fig3 Discipline of Information Security [5]

1. Least Significant Bit Based Steganography
2. Multiple Bit-planes Based Steganography
3. Noise-adding Based Steganography
4. Prediction Error Based Steganography
5. Quantization Based Steganography

4.2. Steganography in Frequency Domain

Frequency domain algorithms are developed to increase the performance over spatial domain techniques. It is necessary to improve the security system due to growth of the information technology. LSB data imbedding technique is great achievement of information security but this technique is not more secure than frequency domain techniques. In frequency domain first transform the mage and then hide the secret data in significant areas of the transformed image. Some popular transformations are Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT). Many techniques are developed in frequency domain some of them are given following [13] [14] [15] [16] [17].

1. JSteg
2. F5
3. OutGuess
4. YASS
5. Model-Based Steganography
6. Adaptive image steganography

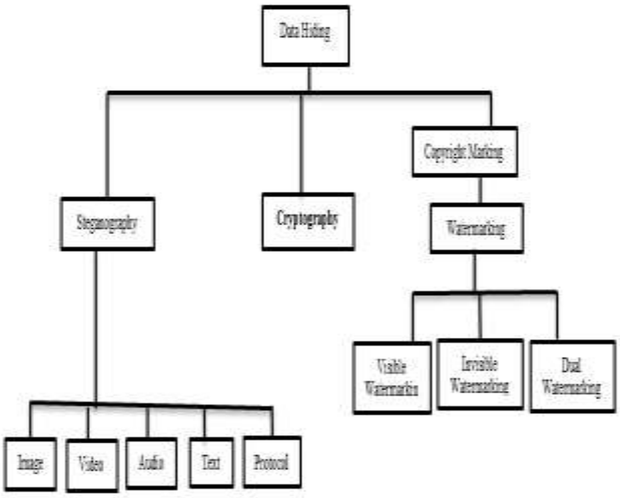

Fig4 Types of Steganography and watermarking

5. Digital Image Watermarking Techniques

5.1 Spatial Domain Watermarking

The spatial domain watermarking represents the digital image in the form of pixels. Spatial domain watermarking embeds the watermark in the colour value of particular selected pixels by modifying its pixel value [18]. The advantage of the spatial domain watermarking is

- Less time consuming
- Simplicity

- Low computational complexity

Spatial domain watermarking technique is simple to implement and its computational speed is higher than transform domain but this technique is low robust against attacks. The most popular method of spatial domain watermarking is LSB. In LSB technique brake the image in pixels and change the least significant bit of the pixel value with the secrete data which want to hide in image. Advantage of this technique is that it is easily applied on images and it also provides high perceptual transparency but poor robustness is main disadvantage of LSB technique.

5.2 Transform Domain Watermarking

The transform domain watermarking attains more success than the spatial domain watermarking. The image is transform in the form of frequency in the transform domain watermarking. Transform domain watermarking techniques first convert the original image in the transformed image by a predefined transformation and then embedded the watermark in transformed image. After embedding process, inverse transform is performed to get the watermarked image [19] [20]. Commonly used image transform domain techniques are Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT).

6. STEGANOGRAPHY vs. WATERMARKING

Attributes	**Steganography**	**Watermarking**
Objective	The objective of steganography is to hide the existence of message in cover object viz. image, audio, video and text. Popular for secret data communication. Steganography is called as cover writing.	The main objective of watermarking is to hide a message or a logo in cover object viz. image video and text. Popular for content authentication and copy right protection
Visibility	Visible	Visible / invisible
Carrier	Image, text, audio and video etc.	Mostly image , text & video
Domain	Transform domain, Spatial domain	Transform domain, Spatial domain
Techniques	LSB, Multiple Bit-planes Based Steganography, Steganography, Quantization Based Steganography, JSteg, F5 OutGuess, YASS etc.	Fragile watermarking, Least Significant Bit, DCT, DWT etc.
Attack method	Steganalysis , Attacking Stochastic Modulation Steganography, Attacking YASS, Stego-only attack	Data Processing , Synchronization Attacks, Watermark Drowning, Stochastic Attacks, Scrambling Attack, Copy Attack, Collusion Attack
Robust	Yes	Yes
Detection	Not easy to detect	Not easy to detect
Imperceptibility	High	High
Durability	Steganography basically Conceal message without modifying it	Watermarking embedded the message covertly in to the noise signals. Extend information and it became an attribute of the object.
Applications	For confidential data transmission like Defense Data, Medical history of patients	For Copyright authentication

7. Conclusions

We have presented a comparative study of steganography and watermarking which are widely used for the confidential data transmission. Generally watermarking used for copyright the image. Combination of two technique steganography and cryptography produce most secure data hiding technique and also enhance the security, security is the main challenge of data over internet.

8. References

[1] Liu Quan, Jiang Xuemei “Researches on uniform meaningful watermark”, proceedings of the 2002 6t international conference on signal processing, 2002.

[2] Silman, J., “Steganography and Steganalysis: An Overview”,SANS Institute, 2001

[3] Aggarwal, M. Singla, “Image Watermarking Techniques in Spatial Domain: A Review International Journal of Computer Technology and Applications, vol.2 (5), pp. 1357–1363, ISSN: 2229-6093, Sept-Oct, 2011.

[4] S. P. Mohanty, "Digital Watermarking: A Tutorial Review", URL: http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999Mohanty.pdf

[5] K.U. Singh, “A Survey on Audio Steganography Approaches”, International Journal of Computer Applications (0975 – 8887), pp.7-14, 2014.

[6] M. Wu, E. Tang, and B. Lin, Data hiding in digital binary image, Proc. of 2000 IEEE International Conference on Multimedia and Expo,vol. 1, pp. 393-396, 2000.

[7] G. Liang, S. Wang, and X. Zhang, Steganography in binary image by checking data-carrying eligibility of Boundary pixels, Journal of Shanghai University, vol. 11, no. 3, pp. 272-277, 2007.

[8] Jessica Fridrich, Miroslav Goljan, and Rui Du, Reliable detection of lsb steganography in color and Gray scale images. Proc. of 2001 ACM workshop on Multimedia and security: new challenges, pp.27-30, ACM Press, 2001.

[9] Wang, H., Wang, S.: Cyber Warfare: Steganography vs. Steganalysis. Communications of the ACM 47(10) (2004)

[10] Eiji Kawaguchi and Richard O. Eason, Principle and applications of bpcs steganography, In Multimedia Systems and Applications, vol. 3528, pp. 464-473, SPIE, 1998.

[11] Fridrich and M. Goljan, Digital image steganography using stochastic modulation, Proc. Of IST/SPIE Electronic Imaging: Security and Watermarking of Multimedia Contents V, vol. 5020, pp. 191-202, 2003

[12] B. Chen and G. W. Wornell, Quantization index modulation: A class of provably good methods for digital watermarking and information embedding, IEEE Trans. Information Theory, vol. 47, no. 4, pp. 1423-1443, 2001.

[13] N. Provos, P. Honeyman, Hide and seek: an introduction to steganography, IEEE Security and Privacy 1 (3) (2003) 32–44.

[14] A. Westfeld, F5-A steganographic algorithm: high capacity despite better steganalysis, in: Proceedings of Fourth International Work-shop on Information Hiding, Lecture Notes in Computer Science, vol. 2137, Pittsburgh, USA, April 2001, pp. 289–302.

[15] N. Provos, P. Honeyman, Detecting steganographic content on the Internet, Centre for Information Technology Integration, University of Michigan, Technical report, August 31, 2001

[16] K. Solanki, A. Sarkar, and B. S. Manjunath, Yass: Yet another steganographic scheme that resists blind steganalysis, Proc. of the 9th Information Hiding Workshop, Springer, vol. 4567, pp. 16-31, 2007.

[17] R. Tzschoppe, R. Baum, J. Huber, A. Kaup,Steganographic system based on higher-order statistics,in: Proceedings of SPIE, Security and Watermarking ofMultimedia Contents V. Santa Clara, California, USA 2003, vol. 5020, pp. 156–166.

[18] N. Chandrakar and J. Baggaa,"Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of computer Application Technology and Research, vol. 2, no. 2, (2013), pp. 126-130

[19] Guan-Ming Su, "An Overview of Transparent and Robust Digital Image Watermarking" Available online atwww.watermarkingworld.orgLWMMLArchive/0504/pdf00000.pdf

[20] Pe. Lee, C., Lee, H., "Geometric attack resistant watermarking in wavelet transform domain," in Optics Express vol. 13, no. 4, pp. 1307-13212005