Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cosrev

Current status and key issues in image steganography: A survey

Mansi S. Subhedar[a,*], Vijay H. Mankar[b]

[a] Research Scholar, Department of Electronics & Telecommunication, Bapurao Deshmukh College of Engineering, Sevagram, Wardha, 442102, Maharashtra, India

[b] Department of Electronics & Telecommunication, Government Polytechnic, Nagpur, 440001, Maharashtra, India

ARTICLE INFO

Article history:
Received 5 October 2013
Accepted 11 September 2014
Published online 5 October 2014

Keywords:
Information hiding
Image steganography
Steganalysis
Image quality measures

ABSTRACT

Steganography and steganalysis are the prominent research fields in information hiding paradigm. Steganography is the science of invisible communication while steganalysis is the detection of steganography. Steganography means "covered writing" that hides the existence of the message itself. Digital steganography provides potential for private and secure communication that has become the necessity of most of the applications in today's world. Various multimedia carriers such as audio, text, video, image can act as cover media to carry secret information. In this paper, we have focused only on image steganography. This article provides a review of fundamental concepts, evaluation measures and security aspects of steganography system, various spatial and transform domain embedding schemes. In addition, image quality metrics that can be used for evaluation of stego images and cover selection measures that provide additional security to embedding scheme are also highlighted. Current research trends and directions to improve on existing methods are suggested.

1. Introduction

The word steganography is obtained from the Greek words "stegos" means "cover" and "grafia" means "writing", defining it as "covered writing". Usually secure communication is achieved by the method of encryption. But nowadays, demand for security is increasing day by day that leads to the use of steganography for information security. The idea of data hiding or steganography was first introduced with the example of prisoner's secret message by Simmons in 1983 [1–3]. Fig. 1 shows various disciplines of information hiding.

Steganography and cryptography are closely related concepts. Though both the terms share a common goal, the way and the usage of both differ significantly. Steganography is hidden writing where as cryptography is secret writing i.e. cryptography provides security with respect to content of the message whereas steganography will hide the existence of the message itself. Digital watermarking is another branch of information hiding. Both steganography and watermarking are the methods of data embedding, but there are several differences among them. A detailed comparison can be found in [4–7]. A variety of multimedia carriers that includes

* *Corresponding author.* Tel.: +91 9867967304.
E-mail addresses: mansi_subhedar@rediffmail.com, msubhedar@mes.ac.in (M.S. Subhedar), vhmankar@gmail.com (V.H. Mankar).

http://dx.doi.org/10.1016/j.cosrev.2014.09.001
1574-0137/

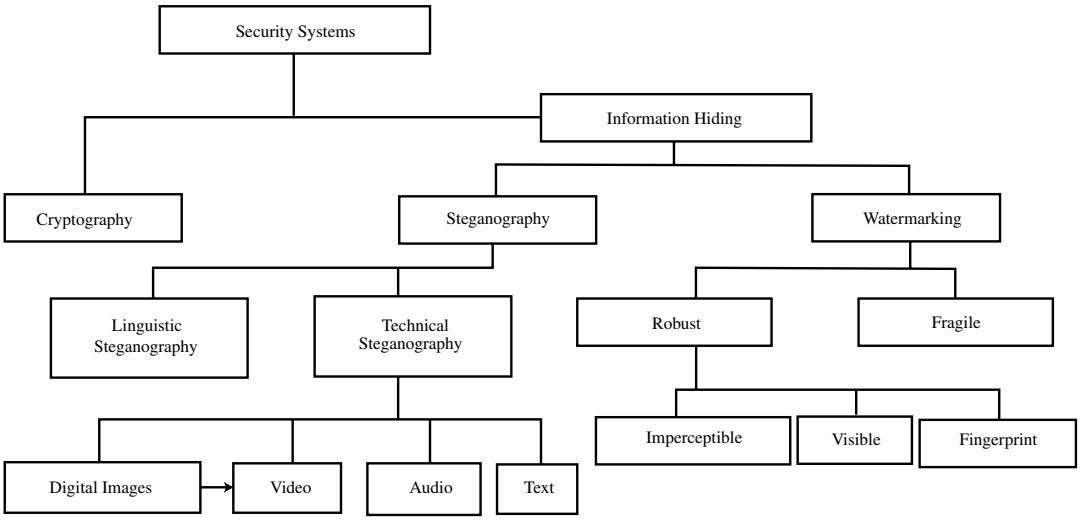

Fig. 1 – Disciplines of information hiding [4].

text, audio, video, image can be used for steganography. Some of the ways to achieve text steganography involve modification of text layout, use of *n*th character from text or alteration of some of the rules such as spaces etc. Another approach includes usage of a code consisting of combination of character, line and page numbers. However, this technique lacks in security. Hiding information in audio files can be done by using frequencies that are inaudible to human ear. Similarly, video files can also be thought of to embed secret information. Since it is a moving stream of images and sounds, any minor distortions may be unseen because of continuous flow of information. The advantage in this case will be high payload capacity. Image is the most popular file format used for steganography as they possesses high degree of redundancy. With image steganography, better imperceptibility and payload capacity can be achieved. Steganalysis is an art of detecting covert communication [8]. In this paper, we focus only on image steganography with little more emphasis on transform domain steganography.

1.1. *Fundamental concepts*

Cover image refers to the image used for carrying the embedded bits, embedded data is known as *payload* and the image with embedded data is called as *stego image*. *Steganalysis* refers to the attack on steganography. The distortion induced on the host signal by the data embedding process is called the *embedding distortion*.

Imperceptibility is innocuousness of the stego image. Stego image should not have severe visual artifacts. Some of the major requirements of steganography include capacity, robustness and security. *Robustness* indicates the amount of modification that the stego medium can withstand before an adversary can destroy hidden information. *Capacity* refers to the amount of information that can be hidden in cover medium without deteriorating the integrity of the cover image. It is represented in terms of bits per pixel (bpp). Embedding operation needs to preserve the statistical properties of the cover image in addition to the perceptual quality.

Security means eavesdropper's inability to detect hidden information. *Perceptual transparency* ensures the retention of the visual quality of the cover after data embedding. *Tamper resistance* means to remain intact in the face of malicious attacks. The *embedding rate* is measured as the number of embedded bits per carrier bit. The *embedding efficiency* is given by the expected number of embedded message bits per modified carrier bit. The *change rate* gives the average percentage of modified carrier bits.

1.2. *General model of steganography*

The concept of steganography is usually modeled by prisoner's problem. Fig. 2 exhibits the overall structure for the steganography system. Let 'C' denotes the cover medium i.e. image *A* and *C′* be the stego image obtained by data embedding. Let 'K' represents an optional key and 'M' is the message we want to communicate. E_m suggests the embedding process and E_x is for the process of extraction. Compression and encryption eliminate the redundancy in secret message and result in enhanced security. Thus, data embedding process can be represented as follows:

$$E_m : C \oplus K \oplus M \rightarrow C'$$
$$E_x\left(E_m\left(c, k, m\right)\right) \approx m, \quad \forall c \in C, k \in K, m \in M. \tag{1}$$

Image is the most often used file format for steganography and is only discussed here where the secret message is embedded in cover image. Applications of steganography include copyright control of materials, enhancing robustness of image search engines and smart id's, feature tagging, secret communication, video-audio synchronization, TV broadcasting, TCP/IP packets etc. [10,11]. Image quality measures are used for the evaluation of stego image quality obtained after embedding. Different methods exist for attacking the steganographic algorithm. The number of steganography tools are available that includes Ezstego, F5, Hide and Seek, Hide4PGP, Mp3Stego, OutGuess, StegHide, Stegnos, S-tools etc. Various forms of steganalysis include identifying the existence of secret message and finding its