International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Steganography and Watermarking: Review

Mohammed Salem Atoum

Department of Computer Science, IRBID National University, Jordan

Abstract: ***Steganography and watermarking techniques are two methods used to hides information within the cover file. Several different file formats are used in both techniques, such as text, image, audio and video. This paper concluded the latest issues and challenges faced in two methods which that using to hide information. As well as to find a possibility other ways to hide information that is mentioned earlier with the increase in research on information hiding.***

Keywords: Information Hiding, Steganography, Watermarking

1. Introduction

The rising potential of modern communications needs the exceptional means of security in the computer network. The network security is becoming more important and challenges of data exchanged on the Internet increases. Therefore, the confidentiality and data integrity are requiring protecting against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding [1].

Information hiding is an addition of application oriented information to a multimedia signal, without causing any perceptible distortion. The energy of the embedded signal should be low enough when projected onto the human perception domain, but it should be strong enough for robust machine detection [2].

Information hiding techniques have recently emerged in many different application areas. Digital audio, videos, and images are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or a serial number, which can even help to prevent unauthorized copying directly [3].

Steganography and watermarking are two methods used in information hiding, which focuses on secret communication. The use of watermarking and steganography, as a viable form of communication, has been largely propelled by the growth of the Internet. The Internet offers an opportunity to exchange large amounts of digital information over great distances. The prevalence of media, such as audio, videos, and images, on the Internet, provides an ideal channel for watermarking and steganographic communication. Figure 1 shows the details of information hiding

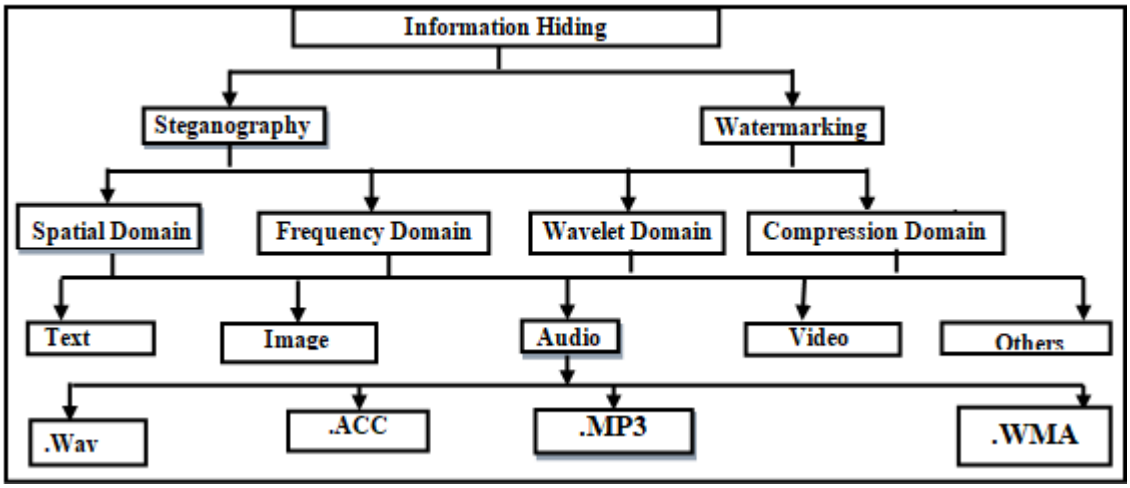

Figure 1: Information hiding overview

Much of the research that has been done on information hiding adopts steganography and watermarking methods. Steganography refers to methods that are used to transmit the embedded message without the observer being able to notice the embedded message in the cover message. In steganography method, transparency is a critical issue but not robustness. Watermarking ensures the security of data by embedding a "watermark" for authentication purpose, which is an important step for copyright protection and tamper proofing [4]. The embedded watermark is usually perceivable and cannot easily be removed from the stego message. Watermarks are extended information and are considered as attributes of the cover image but more so they are usually required to be semi-fragile or robust [5-7].

2. Steganography

Steganography or (Covert Communication) is an ancient art that has been reborn in recent years; it plays a very important role in protecting information in the current age of virtually connected system, organisation's secret information needs to be shared to its branches worldwide and copyright issues need to protect as well. Therefore, the increasing demand for protecting information will continue [2].

Steganography basically aims at hiding communication between two parties from the attackers [8].

Steganography system involves inserting an identifier be it a message, the secret message or a marker into a medium that will not be affected. The most important object inserted into a cover medium is the secret message or serial numbers or secret code. When this information is embedded, the steganographic technique ensures that it will not be detected and assess by any unauthorized person. The cover message that hosts the embedded is called a Stego Object [6]. The cover message is required to be disposed of after the receivers got it in order to prevent an accidental reuse. Figure 2 shows the basic model of steganography.

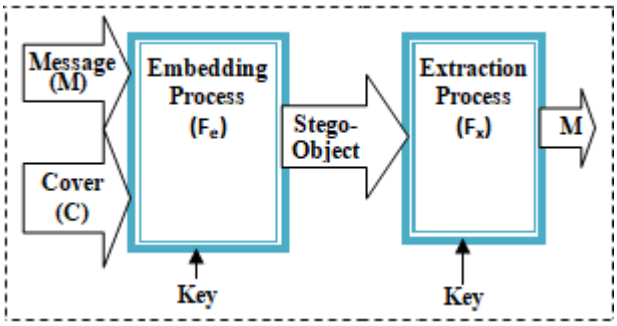

Figure 2: Basic model of steganography

The basic model of steganography contains two processes namely embedding process (F_e) and extracting process (F_x). Message, M is embedded into host cover, C to create a stego-object, SO by using F_e function and key, K. The F_x process using SO and K to obtain M [9]. The two processes can be written as follows:

$$F_e: C \times M \times K \rightarrow SO \quad (1)$$

$$SO \times K \rightarrow M \quad (2)$$

Steganography technique used in the data hiding process must have important properties in order to secure data successfully. Some of these properties include robustness, imperceptibility, invisibility, security, complexity, and capacity [7]. The capacity property is the most challenge in steganography.

Capacity or (Data rate) refers to the amount of ratio of the data able to be embedded into a cover file and the amount of the cover file that will host the embedded file without degrading the cover file condition to the message [10].The ratio between the quantity of the host file and the embedded file has to be made as a steganographic rule of thumb. Steganography techniques are liable to work under large embedded data rate or a huge resistance to any alteration both not under all conditions. The relation is made in such a way the higher the increase in one the lower the other one becomes [8]. A bit plane tool encompasses methods that apply LSB insertion and noise handling. LSB steganographic technique achieves a huge success as the basis steganography technique used for both audio and image. It allows huge amount of information to be hidden in the cover message with little compression through the use of LSB technique [10]. These requirements were explained before being mutually competitive and cannot be clearly optimized at the same time. This observation is schematically depicted in Figure 3. Absolute imperceptibility and high robustness cannot be used simultaneously. On the other hand, if robustness is an issue the message that can be reliably hidden cannot be too long [11].

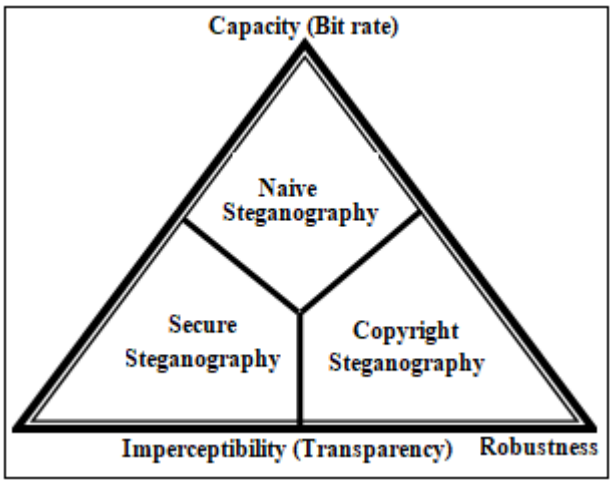

Figure 3: Trade-off between properties

3. Watermarking

Watermarking Also referred to as simply watermarking, a pattern of bits inserted into the cover file that identifies the file's copyright information (author, rights, etc.). The name comes from the faintly visible watermarks imprinted on stationery that identify the manufacturer of the stationery. The purpose of digital watermarks is to provide copyright protection for intellectual property that's in digital format [2].

In both watermarking techniques (fragile watermarks and semi-fragile watermarks), message integrity can be applied by checksum for the most significant bit and embedding it into selected pixels randomly by using LSB technique. Alternatively, Image can be partition into blocks of variable sizes and each block is a uniquely identify by size, so that when a block size is a change this will clearly then the watermark also changes [10]. Since watermarking does not provide an avenue for an image processing scheme any changes to image might not be important to detect, on like when message integrity need to be monitored. Therefore watermarking will not reliable for ensuring the secrecy or in the integrity of secret message [7].

Watermarking is a technique through which the secure information is carried without degrading the quality of the original signal. The technique consists of two blocks: Embedding and Extraction block. The system has an embedded key as in a case of steganography. The key is used to increase security, which does not allow any unauthorized users to manipulate or extract data. The embedded object is known as watermark, the watermark embedding medium is termed as the original signal or cover object and the modified object is termed as embedded signal or watermarked data [10].

The embedding block, shown in Figure 4 consists of watermark, original signal (or cover object), and the watermarking key as the inputs (creates the embedded signal or watermarked data) [11]. Whereas, the inputs for the extraction block is embedded object, key and sometimes the watermark as illustrated in Figure 5 [11].

The watermarking technique that does not use the watermark during extraction process is termed as „blind watermarking.“ Blind watermarking is superior over other watermarking involving watermark for extraction as watermarked signal and key are sufficient to find the embedded secret information [12].

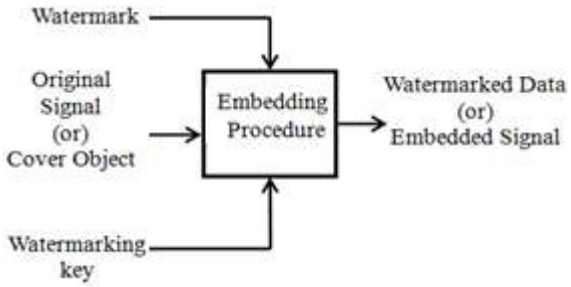

Figure 4: Digital watermarking embedding

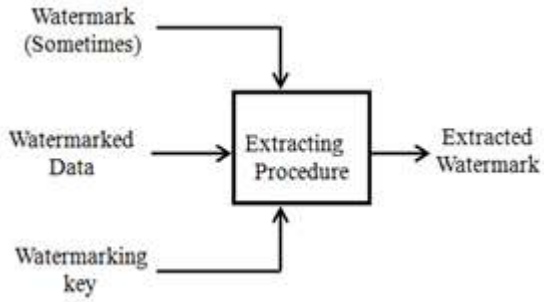

Figure 5: Digital watermarking extraction

The watermarking technique has evolved considerably from its origin [12]. Due to the evolution of technology, the medium of transmission has been changed. Watermarking is employed in digital media such as image and audio. Audio watermarking is quite challenging than image watermarking due to the dynamic supremacy of the human auditory system (HAS) over human visual system (HVS) [12]. Applications of Watermarking are used in Ownership protection and proof of ownership, Authentication and tampering detection, Finger printing, Broadcast monitoring, Copy control and access control, Information carrier, Medical applications and Airline traffic monitoring [12].

4. Conclusions

This paper presents two methods of information hiding: Steganography and watermarking. The process of embedding information in host media in steganography technique and watermarking are usually done transparently. The difference between steganography and watermarking is that while steganography is a technique which hides the information, visible watermarking actually allows the third person to see the message. Thus, in terms of watermarking visible and invisible, the process needs to ensure robustness so that any intentional attacks would not compromise, remove, or cause destruction of the information in any way in the marked media while at the same time preserving the quality of the signal. The invisible watermarking technique is the most suitable technique in cases where knowledge of the hidden information could cause possible manipulations.

References

[1] A.Z. Al-Othmani, A. A. Manaf and A. M. Zeki, “A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation”, IJCSI International Journal of Computer Science Issues, Vol. 9, no. 1, 2012
[2] S. B. Kumar, D. Bhattacharyya, P. Das, D. Ganguly and S. Mukherjee, “A tutorial review on Steganography”, International Conference on Contemporary Computing (IC3-2008), Noida, India, 2008, pp. 105-114.
[3] P. Dutta, D. Bhattacharyya, and T. Kim, “Data Hiding in Audio Signal: A Review”, International Journal of Database Theory and Application, Vol. 2, No. 2, June 2009
[4] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, and S. Pogreb, “Techniques for data hiding”, IBM Systems Journal, Vol. 39, No. 3-4, pp. 547 – 568, 2000.
[5] Atoum, M. S. (2015). A Comparative Study of Combination with Different LSB Techniques in MP3 Steganography. In Information Science and Applications(pp. 551-560). Springer Berlin Heidelberg.
[6] Atoum, M. S., Ibrahim, S., Sulong, G., and Zamani, M. (2013). A New Method for Audio Steganography Using Message Integrity, Journal of Convergence Information Technology,8(September), 35–44.
[7] Atoum, M. S., Ibrahim, S., Sulong, G., and Ahmed, A. (2013).New Secure Scheme in Audio Steganography (SSAS). Australian Journal of Basic and Applied Sciences, 7(6), 250–256.
[8] Atoum, M. S., Ibrahim, S., Sulong,G. and Ahmed, A. (2012). MP3 Steganography: Review. Journal of Computer Science issues, 9(6).
[9] Atoum, M. S., Suleiman, M., Rababaa, A., Ibrahim, S., and Ahmed, A. (2011). A steganography Method Based on Hiding secretes data in MPEG / Audio Layer III. International Journal of Computer Science and Network Security, 11(5), 184-188.
[10] Atoum, M. S., Rababah, A. and Al-attili, A. I. (2011).New Technique for Hiding Data in Audio Files. International Journal of Computer Science and Network Security, 11(4), 173-177.
[11] Atoum, M. S., Ibrahim, S., Sulong, G., Zeki, A and Abubakar, A. (2013). Exploring the Challenges of MP3 Audio Steganography. Proceding IEEE from 2nd International Conference on Advanced Computer Science Applications and Technologies (ACSAT) ,Sarawak, Malaysia.
[12] Atoum, M. S. (2015, August). New MP3 Steganography Data Set. In IT Convergence and Security (ICITCS), 2015 5th International Conference on (pp. 1-7). IEEE.

Author Profile

Mohammed Salem Atoum is assistant professor in Irbid National University. His research interests, Steganography, Watermarking, data hiding, cryptography and Information Security.