Digital Watermarking and Other Data Hiding Techniques

Gurpreet Kaur, Kamaljeet Kaur

Abstract- Digital watermarking is not a new name in the technology world but there are different techniques in data hiding which are similar to watermarking. In this paper we compare digital watermarking with other techniques of data hiding. Steganography, Fingerprinting, cryptography and Digital signature techniques are compared with watermarking. We need watermarking for digital data security .It provides ownership assertion, authentication and integrity verification, usage control and content labelling.

Keywords: - Cryptography, Digital signature, Fingerprinting, Steganography, Watermarking

I. INTRODUCTION

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[1]. Digital watermarking is changing an image in a way so that you can see some text or background image without actually corrupting the image. Watermarking is used to verify the identity and authenticity of the owner of a digital image. It is a process in which the information which verifies the owner is embedded into the digital image or signal. These signals could be either videos or pictures or audios. For example, famous artists watermark their pictures and images. If Somebody tries to copy the image, the watermark is copied along with the image.[3]

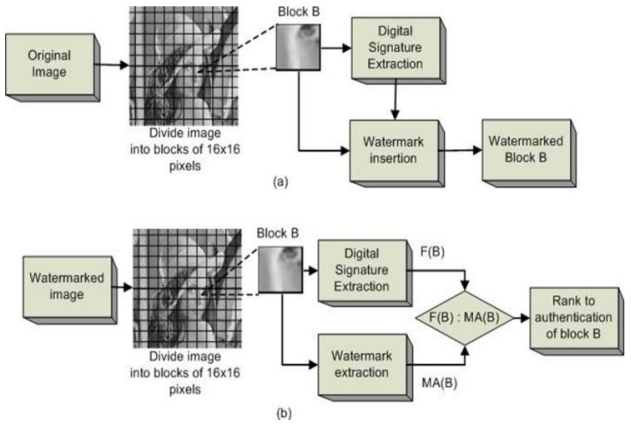

Fig 1: Watermarking insertion and extraction system.[3]

1.1 TYPES OF WATERMARKING

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.

Manuscript received on April, 2013.

Gurpreet Kaur, Gurpreetkaur, Student, Shiri Guru Granth Sahib World Uni (Fatehgarh sahib)

Kamaljeet Kaur, KamaljeetKaur, Assit Prof, Shiri Guru Granth Sahib World Uni (Fatehgarh sahib)

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.

1.2 Applications:

- It is used for copyright protection.
- It is used for source tracing.
- Annotation of photographs.

II. COMPARISION OF WATER- MARKING WITH DIFFERENT DATA HIDING TECHNIQUES

2.1 STEGANOGRAPHY:-

Steganography is derived from the Greek for covered writing and essentially means “to hide in plain sight”. Steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in an electronic format new techniques for information hiding have become possible. This document will examine some early examples of steganography and the general principles behind its usage. We will then look at why it has become such an important issue in recent years. There will then be a discussion of some specific techniques for hiding information in a variety of files and the attacks that may be used to bypass steganography. [2]Figure 2 shows a common taxonomy of steganography techniques (Arnold et al. 2003; Bauer 2002).

- Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size-reduction methods.
- Linguistic steganography hides the message in the carrier in some nonobvious ways and is further categorized as semagrams or open codes.
- Semagrams hide information by the use of symbols or signs. A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or Website. A text semagram hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra spaces, or different flourishes in letters or handwritten text.
- Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer. The carrier message is sometimes called the overt communication whereas the hidden message is the covert communication. This category is subdivided into jargon codes and covered ciphers.

- Jargon code, as the name suggests, uses language that is understood by a group of people but is meaningless to others. Jargon codes include warchalking (symbols used to indicate the presence and type of wireless network signal [Warchalking 2003]), underground terminology, or an innocent conversation that conveys special meaning because of facts known only to the speakers. A subset of jargon codes is cue codes, where certain prearranged phrases convey meaning.
- Covered or concealment ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed. A grille cipher employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the hidden message. A null cipher hides the message according to some prearranged set of rules, such as "read every fifth word" or "look at the third character in every word."[2]

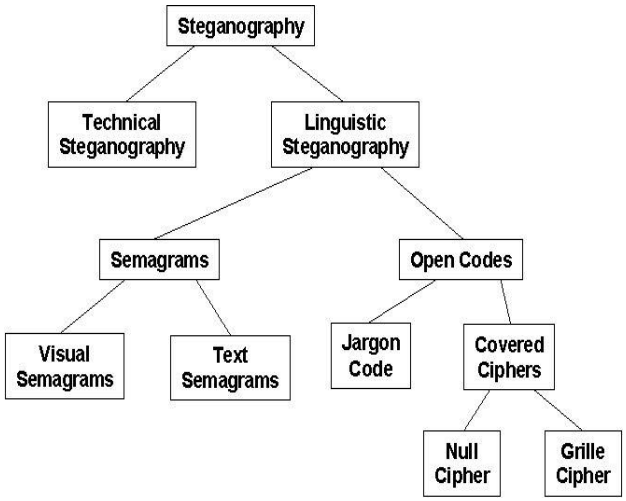

Figure 2 Steganography and its techniques[2].

WATERMARKING AND STEGANO- GRAPHY

- The information hidden by a watermarking system is always associated to the digital object to be protected or to its owner while steganographic systems just hide any information
- "Robustness" criteria are also different, since steganography is mainly concerned with detection of the hidden message while watermarking concerns potential removal by a pirate
- Steganographic communications are usually point-to-point (between sender and receiver) while watermarking techniques are usually one-to-many[9]

2.2 FINGERPRINTING

Fingerprinting has at least two definitions when it comes to protecting content. The first deals with taking each copy of your content and making it unique to the person who receives it. This way, if the work is shared, you know exactly which person spread the work initially. A variation of this technique is used by the CopyFeed plugin, which embeds the IP address of the feed reader into every entry. Thus, if the feed is scraped and reposted, the person doing the scraping can be identified and blocked. In short, what fingerprinting usually does is take the content, use some kind of software to convert it into a unique number or string of characters and then use that string to match it against other content out there. It basically does to the content what a fingerprint scanner does to your fingerprint. The principles are very much the same.[7]

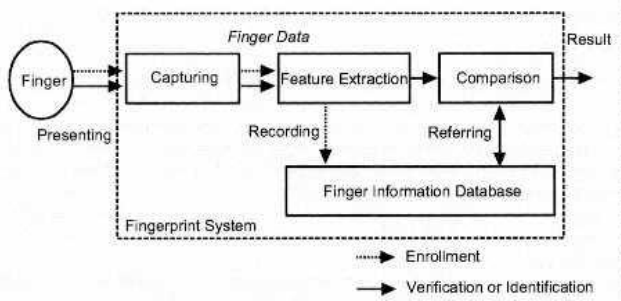

Fig 3 Fingerprinting Process [5]

III. WATERMARKING AND FINGER- PRINTING

- In watermarking modifications of contents by adding identification data while in fingerprinting contents are not affected.
- Watermarking allow the precise identification of each piece of content and in fingerprinting work for legacy content.
- Watermarking stand alone and fringerprinting connection to database required.

2.3 CRYPTOGRAPHY

Cryptography is the science of enabling secure communications between a sender and one or more recipients. This is achieved by the sender scrambling a message (with a computer program and a secret key) and leaving the recipient to unscramble the message (with the same computer program and a key, which may or may not be the same as the sender's key). The emphasis of cryptography is on data confidentiality, data integrity, sender authentication, and non-repudiation of origin/data accountability .In cryptography, the message is usually scrambled and unreadable. However, when the communication happens, it is known or noticed. Although the information is hidden in the cipher, an interception of the message can be damaging, as it still shows that there is communication between the sender and receiver. In contrast, steganography takes a different approach in hiding the evidence that even a communication is taking place.[8]

There are two main types of cryptography:

Secret key cryptography is also known as *symmetric key* cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

Public key cryptography, also called *asymmetric encryption*, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys.[8]

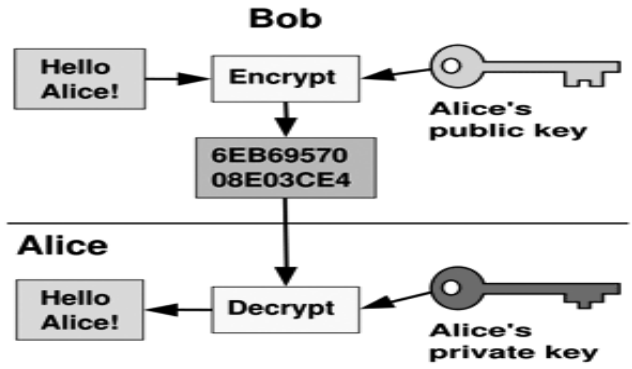

Fig 4 Encryption and Decryption[5]

WATERMARKING AND CRYPTO- GRAPHY

- In cryptography two keys are used for encryption and detection while in watermarking information is added in data for security.
- In cryptography keys are needed for detection but watermarking does not needed any key.

2.4 DIGITAL SIGNATURES:

A mechanism employed in public-key cryptosystems (PKCS) that enables the originator of an information object to generate a signature, by encipherment (using a private key) of a compressed string derived from the object. The digital signature can provide a recipient with proof of the authenticity of the object's originator. A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

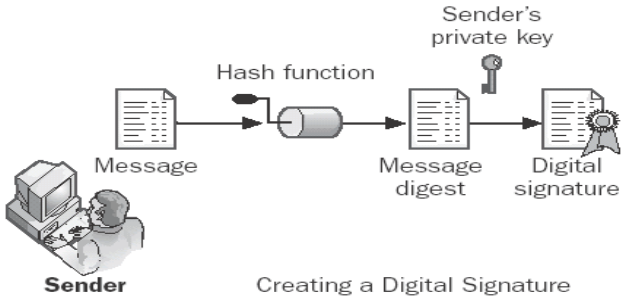

Fig 5 Digital signature process [10]

WATERMARKING AND DIGITAL SIGNATURE

- Watermarking mark a secreat message while digital signature used secreat message.
- Watermarking is a concept of data hiding. Digital signature support origin authentication and content integrity service and belong to the field of cryptography.

WHY WE NEED WATER- MARKING??

A Watermark is a form, image or text that is impressed onto paper, which provide evidence of its authenticity. Digital Watermarking is an extension of this concept in the digital world. In recent years the phenomenal growth of the internet has highlighted the need for mechanism to protect ownership of digital media. Digital Watermarking is a technique that provides a solution to the longstanding problems faced with copyrighting digital data. For following applications we used digital watermarking:-

- Ownership assertion:- Watermarking is used to establish ownership over the content.
- Authentication and integrity verification:- content which is protected by key verification should not be accessible without authentication.
- Usage control:- To limit copies creation of copyrighted data,by blocking using watermark.
- Content labelling:- Bits embedded in data giving extra information.

IV. CONCLUSIONS

There are many techniques in data hiding. Digital Watermarking is more secure and easy method of data hiding .All techniques of data hiding secure data with their methods, but watermarking is more capable because of its efficiency. In Watermarking we mark the information which is to be hiding. Security of data is essential today because of cyber-crime, which is highly increased day by day. Watermarking provide us easy and efficient security solutions of digital data. Watermarking provide security of not only images, but also audio video and text

REFERENCES

1. Sukriti Bhattacharya, AgastinoCortesi, "Data Authentication by Distortion Free Watermarking", ICSOFT 2010
2. Jonathan Cummins, Patrick Diskin, Samuel and Robert Parlett,"Steganography and Digital Watermarking", 2004.
3. Clara Cruz Ramos, Rogelio Reyes Reyes, Mariko Nakano Miyatakeand Héctor Manuel Pérez Meana, "Watermarking-Based Image Authentication System in the Discrete Wavelet Transform Domain".intechopen.
4. Gary C Kessler, "An Overview of Steganography for the Computer Forensics Examiner". February 2004 (updated June 2011).
5. Tsutomu Matsumoto ,Hiroyuki Matsumoto ,Koji Yamada ,Satoshi Hoshino, "Impact of Artificial "Gummy" Fingers on Fingerprint Systems" Optical Security and Counterfeit Deterrence Techniques IV, January 2002
6. http://blog.securemymind.com/wp-content/uploads/2012/11/ encryption-awareness.png
7. http://www.plagiarismtoday.com
8. http://www.querycat.com
9. http://jayitsecurity.blogspot.in
10.]http://www.microsoft.com/mspress/ books/sampchap/6429/0-7356-1877-3.gif