ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.5 , No.1, Pages : 74 -80 (2016)
Special Issue of ICACEC 2016 - Held during 23-24 January, 2016 in Institute of Aeronautical Engineering, Quthbullapur, Telangana-43, India

COMPARISON OF DIGITAL WATERMARKING WITH OTHER TECHNIQUES OF DATA HIDING

D.Sai Chaitra Student, IARE

P.Veenasri Student, IARE

A.Vinuthna Reddy Student, IARE

V.Srinidhi Student,IARE

ABSTRACT

As the requirements of information security within an organisation have undergone major changes, methods which are required to secure the information about the organisation has also undergone several changes. As the network need to ensure confidentiality, integrity, availability, it is necessary to ensure the information is secured. This paper tells the importance of digital watermarking, how it helps to secure, and even how stenography, finger printing, digital signature, cryptography helps to secure the data. Water marking is the thing which helps to provide data security. It provides ownership assertion authentication and integrity verification, usage control and content labelling.

KEYWORDS: Cryptography, Steganography, Digital signature, Finger printing, Digital watermarking.

1. INTRODUCTION

Water marking is a technique accustomed to hide information or distinct data at intervals digital multimedia system. A watermark can be considered to be some kind of message or information that is embedded into underlying data for localization, ownership proof, and/or traitor tracing purposes. Watermarking techniques apply to various types of host or user content. Digital watermarking is changing an image in a way so that one 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 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 [4].

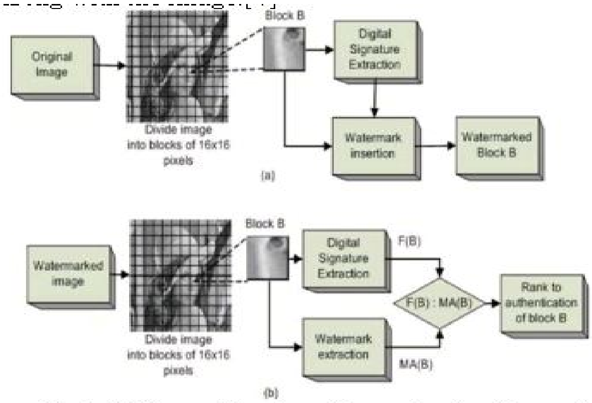
Original Image
Divide image into blocks of 16x16 pixels
Block B
Digital Signature Extraction
Watermark insertion
Watermarked Block B
(a)
Watermarked image
Divide image into blocks of 16x16 pixels
Block B
Digital Signature Extraction
F(B)
F(B) : MA(B)
Rank to authentication of block B
Watermark extraction
MA(B)
(b)

Fig 1: Watermarking insertion and extraction system.[4]

NEED OF WATERMARKING

In recent years the phenomenal growth of the internet has highlighted the need for mechanism to protect ownership of digital media. Digital Watermarking is an extension of this concept in the digital world. Digital Watermarking is a technique that provides a solution to the longstanding problems faced with copyrighting digital data.

A Watermark is a form, image or text that is impressed on to paper, which provide evidence of its authenticity[2].

For following applications we used digital watermarking**: -**

*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.

Ownership assertion: Watermarking is used to establish ownership over the content.

2. LITERATURE SURVEY

The different watermarking techniques are used for data security while transferring the complex data [1]. There are two types of water marking techniques, they are visible and invisible which are explained in the following section.

Visible Water Marking: It refers to the information visible on the picture, or image, or video. Those are typically texts or logos.

For Example, logos of the channel in TV live broadcasting.

Invisible Water Marking: It refers to adding digital data in a video, or audio or picture. It is not visible or perceivable, but by different means it can be detected. It may also be a form of steganography and is used for widespread and retrieved easily. [3]

Applications:_ It is used for copyright protection, source tracing and photograph annotations.

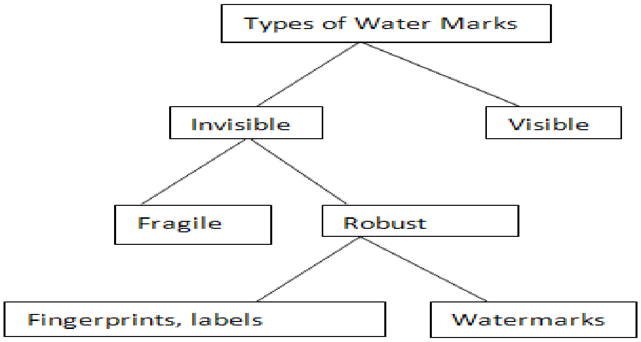

Fig.1: Types of Watermarking

DIFFERENT DATA HIDING TECHNIQUES

1.Steganography:

The word Steganography is derived from Greek covered writing, which means “to hide in plain sight”. By this, the presence of a message cannot be detected. This technique has been used for many years, but with increasing use of files in electronic media new techniques are introduced. This document will examine some early examples and general principles. Then we will look at why it has become such an important issue in recent years and some specific techniques for information hiding and attacks that may be used to bypass Steganography [5].

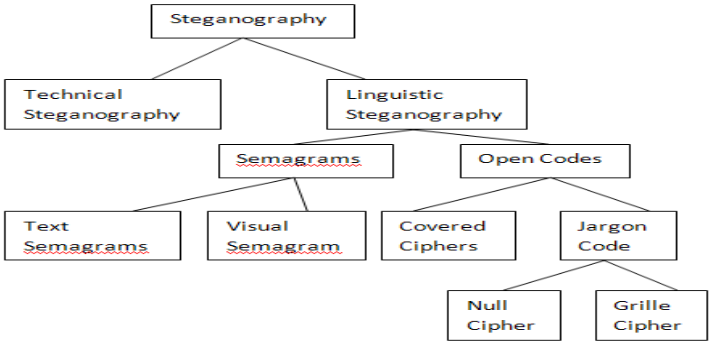

Fig.2 Common Taxonomy of Steganography Techniques

Technical steganography: It uses scientific methods to hide a message, such as the use of invisible ink or microdots and some size-reduction methods.

Linguistic Steganography: In some non obvious ways it hides the message in the carrier. It is further categorized as Semagrams and Open Codes [3].

Semagram: It hide information by the use of symbols or signs. It is further categorized as Visual and Text Semagrams.

Visual Semagrams: It uses innocent-looking of everyday physical objects to convey a message, such as positioning of items on a desk or Website [8].

Text Semagrams: It hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or style, adding extra spaces, or flourishes in letters or handwritten text.

Open codes: It hides 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. It is sub divided into jargon codes and covered ciphers.

Jargon code – It uses language that is understood by a group of people but is meaningless to others. It includes war chalking (symbols used to indicate the presence and type of wireless network signal 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.[9]

Covered Cipher /Concealment Cipher – It 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.

Grille Cipher – It employs a template which is used to cover the carrier message. The words that appear in the openings of the template are hidden message.

Null Cipher – It hides the message according to some pre-arranged set of rules, such as "read every third word" or "look at the fourth character in every word."

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[6]. A variation of this technique is used by the Copy Feed plug-in, 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]

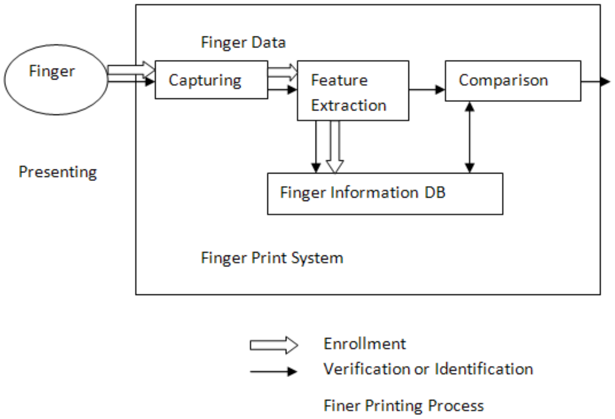

Fig. 3 Finger Printing Process

3.Cryptography:

Cryptography is the science of enabling secure communications between a sender and one or more recipients. This is achieved by the sender encrypting a message (with a computer program and a secret key) and leaving the recipient to decrypting 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 encrypted 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[10].

There are two main types of cryptography*:*

Secret Key Cryptography: It 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 and decrypted by the receiver using the same key [8].

Public Key Cryptography: It also called Asymmetric Key Cryptography. It is same as Secret Key Cryptography, but uses pair of same keys at sender encryption and receiver decryption. With this, keys work in pairs of matched public and private keys.

ISSN 2278-3091

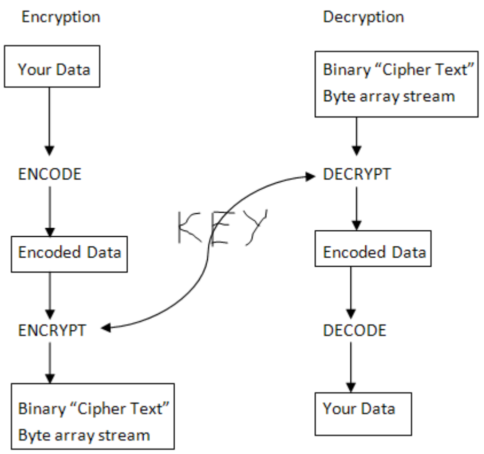

Fig.4 Encryption – Decryption

4. Digital Signature*:*

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.

It can provide a recipient with proof of the authenticity of the object's originator. It 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. Those are easily transportable, cannot be imitated by someone else, and can be automatically time stamped [11].

The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

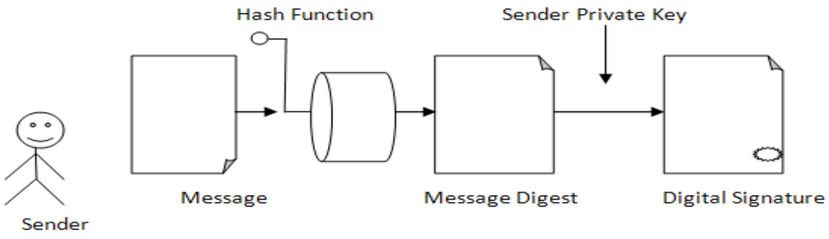

Fig.5 Digital Signature Process

3. PROPOSED TECHNIQUE FOR DATA SECURUTY

3.1 DIFFERNTIATING WATERMARKING TECHNIQUE WITH DATA HIDING TECHNIQUES

This section lists the merits of watermarking technique over other data hiding techniques.
Watermarking and Stenography: The information hidden by a watermarking system is always associated to the digital object to be protected or to its owner and it concerns potential

removal by a pirate. These communications are usually one-to-many. While Stenography just hide any information, “Robustness” criteria are also different and it mainly concerned with detection of the hidden message. These communications are usually point-to- point.

Watermarking and Finger Printing: In watermarking, modifications of contents by adding identification data. It allows the precise identification of each piece of content and it is stand alone. While in fingerprinting contents are not affected. It work for legacy content and connection to database required.

Watermarking and Cryptography: In watermarking information is added in data for security and doesn’t use any keys. In cryptography two keys are used for encryption and decryption and detection.

Watermarking and Digital Signature: Watermarking mark a secret message. It is a concept of data hiding. While Digital Signature used secret message. It support origin authentication and content integrity service and belong to the field of Cryptography.

3.2 IRIS TECHNOLOGY WITH WATER MARKING

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the **irises** of an individual's eyes, whose complex random patterns are unique, stable, and can be seen from some distance.

Iris recognition is the only biometric authentication technology designed to work in the 1-n or exhaustive search mode. This makes it ideal for handling applications requiring management of large user groups, such as a National Documentation application might require.. Large databases are accommodated without degradation in authentication accuracy. Iris Access platforms integrate well with large database back ends like Microsoft SQL and Oracle 9i.

Iris technology is a best way to provide safety to the data bases. In this process the iris image of an individual is captured in order to retrieve the corresponding information of that particular person. The image captured must be protected in order to avoid felonious access to the data bases by using Digital Water Marking for the iris image.

4. CONCLUSIONS

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

5. REFERENCES

[1]“Digital Watermarking and Other Data Hiding Techniques”IJITEE, Gurpreet Kaur, Kamaljeet Kaur,2013
[2]Sukriti Bhattacharya, AgastinoCortesi, “Data Authentication by Dis- tortion Free Watermarking”, ICSOFT 2010
[3] Jonathan Cummins, Patrick Diskin, Samuel and Robert Par- lett,“Steganography and Digital Watermarking”, 2004.
[4] Clara Cruz Ramos, Rogelio Reyes Reyes, Mariko Nakano Miyata- keand Héctor Manuel Pérez Meana, “Watermarking-Based Image Authentication System in the Discrete Wavelet Transform Do- main”.intechopen.
[5] Gary C Kessler, “An Overviewof Steganography for the Computer Forensics Examiner”. February 2004 (updated June 2011).
[6] Tsutomu Matsumoto ,Hiroyuki Matsumoto ,Koji Yamada ,Satoshi Hoshino, “Impact of Artificial "Gummy" Fingers on Fingerprint Sys- tems” Optical Security and Counterfeit Deterrence Techniques IV, January 2002
[7] http://blog.securemymind.com/wpcontent/uploads/2012/1 encryp- tion-awareness.png
[8] http://www.plagiarismtoday.com
[9] http://www.querycat.com
[10] http://jayitsecurity.blogspot.in
[11] http://www.microsoft.com/mspress/ books/sampchap/6429/0-7356-1877-3.gif

Authors:

	Student of Institute of aeronautical engineering Pursuing B.Tech degree in computer science engineering
	Student of Institute of aeronautical engineering Pursuing B.Tech degree in computer science engineering
	Student of Institute of aeronautical engineering Pursuing B.Tech degree in computer science engineering
	Student of Institute of aeronautical engineering Pursuing B.Tech degree in computer science engineering