Advances in Computational Research

Advances in Computational Research
ISSN: 0975–3273 & E-ISSN: 0975–9085, Volume 3, Issue 1, 2011, PP-37-41
Available online at http://www.bioinfo.in/contents.php?id=33

INFORMATION HIDING TECHNOLOGY- A WATERMARKING

MEENA V. KAMBLE
Vidyabharati Mahavidyalaya, Amravati, Department of computer Science, Amravati University, Amravati MS, India
*Corresponding Author Email:- Kamblemeena365@gmail.com

Received: December 03; Accepted: December 12, 2011

Abstract- In this Paper, we are discussing about a security which is essential for today world .we briefly discuss the Digital watermarking and historical development of watermarking which is use as a one of the tool for hiding data/ information . We also introduce various data hiding terminologies used in current literature and attempt has clear distinction of them. Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The signal may be audio, pictures or video. In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media. The image on the right has a visible watermark. In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden) The watermark may be intended for widespread use and is thus made easy to retrieve or it may be a form of Steganography where a party communicates a secret message embedded in the digital signal.
Keywords- sequrity, Digital watermarking, information Hiding, watermarking

INTRODUCTION

The idea of communicating secretly is as old as communication itself. The earliest allusion to secret writing in the West appears in Homer's Iliad Stenographic methods made their record debut a few centuries later in several tales by Herodotus, the father of history. An important technique was the use of sympathetic inks.. Later, chemically affected sympathetic inks were developed. This was used in World Wars 1 and 2. The origin of stenography is biological and physiological. The term steganography came into use in 1500's after the appearance of Triteness' book on the subject Steganographia. A whole other branch of steganography, linguistic steganography, consists of linguistic or language forms of hidden writing. These are the semagrams and the open code. A semagram is a secret message that is not in a written form.

Watermarking technique has evolved from steganography. The use of watermarks is almost as old as paper manufacturing. Paper Watermarks have been in wide use since the late middle Ages. Their earliest use seems to have been to record the manufacturer's trademark on the product so that the authenticity could be clearly established without degrading the aesthetics and utility of the stock.. Today most developed countries also watermark their paper, currencies and postage stamps to make forgery more difficult. The digitisation of our world has expanded our concept of watermarking to include immaterial digital impressions for use in authenticating ownership claims and protecting proprietary interests. However, in principle digital watermarks are like their paper ancestors. They signify something about the token of a document or file in which they inherit. Whether the product of paper press or discrete cosine transformations, watermarks of varying degree of visibility are added to presentation media as a guarantee of authenticity, quality ownership and source.

II -INFORMATION HIDING TERMINOLOGY:

n this section we will discuss different information hiding terminology. The various information hiding techniques can be classified as given in Fig. 1

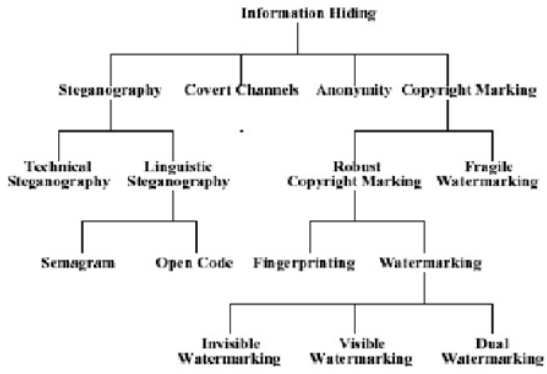

Fig. 1-Information Hiding Techniques

Steganography

The art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics,

sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.
Steganography is the art / science /study of communicating in a way which hides a secret message in the main information. The term steganography means cover writing. In steganography an issue of concern is bandwidth for the hidden message whereas robustness is of more concern with watermarking. . Steganography hides messages in plain sight rather than encrypting the message, it is embedded in the data and doesn't require secret transmission. The message is carried inside data. Steganography is therefore broader than cryptography.

Cryptography

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet.
Cryptography is the study of methods of sending messages in distinct form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called plain text and disguised message is called cipher text. The process of converting a plain text to a cipher text is called enciphering or encryption, and the reverse process is called deciphering or decryption. Encryption protects contents during the transmission of the data from the sender to receiver. However, after receipt and subsequent decryption, the data is no longer protected and is the clear.

Watermarking

Watermarking is the process that embeds data called a watermark, tag or label into a multimedia object such that watermark can be detected or extracted to make an assertion about the object may an image or video or audio may also be text only. A watermark can be perceived as an attribute of the carrier (cover). It may contain information such as copyright, license, tracking and authorship etc. Whereas in case of steganography, the embedded message may have nothing to do with the cover. Digital watermarking differs from digital fingerprinting.

III-WATERMARKING

***A:* life-cycle:**

Digital Watermarking, an extension of Steganography, is a promising solution of content copyright protection in the global network. It imposes extra robustness on embedded information. To put into words, digital watermarking is the art and science of embedding copyright information in the original files, the information embedded is called watermarks. Digital watermarks don't leave a noticeable mark on the content and not affect its appearance. These are imperceptible and can be detected only by proper authorities. Digital watermarks are difficult to remove without noticeably degrading the content and are a covert means in situations where cryptography fails to provide robustness.

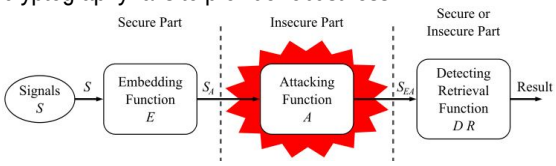

Fig. 2- General watermark life-cycle phases with embedding-, attacking- and detection/retrieval function

The information to be embedded is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal.
The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where pirates attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data, cropping an image or video, or intentionally adding noise.
Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark is still present and it can be extracted. In robust watermarking applications, the extraction algorithm should be able to correctly produce the watermark, even if the modifications were strong. In fragile watermarking, the extraction algorithm should fail if any change is made to the signal

B: Type of digital Watermark:

Watermarks and watermarking techniques can be divided into various categories in various ways. The watermarks can be applied in spatial domain. An alternative to spatial domain watermarking is frequency domain watermarking. It has been pointed out that the frequency domain methods are more robust than the spatial domain techniques. Different types of watermarks are shown in the figure below
Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows.

- Image Watermarking
- Video Watermarking
- Audio Watermarking
- Text Watermarking

According to the human perception, the digital watermarks can be divide into three different types as follows.

- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark
- Dual watermark

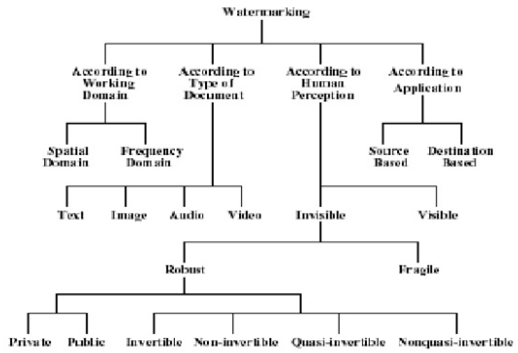

Fig. 3-Type of digital Watermark:

Visible watermark is a secondary translucent overlaid into the primary image. The watermark appears visible to a casual viewer on a careful inspection. The invisible-robust watermark is embed in such a way that an alternation made to the pixel value is perceptually not noticed and it can be recovered only with appropriate decoding mechanism. The invisible-fragile watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark. Dual watermark is a combination of a visible and an invisible watermark .In this type of watermark an invisible watermark is used as a back up for the visible watermark as clear from the following diagram

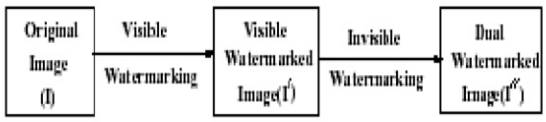

Fig. 4-Dual watermark

An invisible robust private watermarking scheme requires the original or reference image for watermark detection; whereas the public watermarks do not. The class of invisible robust watermarking schemes that can be attacked by creating a counterfeit original is called invertible watermarking scheme From application point of view digital watermark could be as below.

- Source based or • Destination based.

Source-based watermark are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. A source-based watermark could be used for authentication and to determine whether a received image or other electronic data has been tampered with. The watermark could also be destination based where each distributed copy gets a unique watermark identifying the particular buyer. The destination -based watermark could be used to trace the buyer in the case of illegal reselling.

C: Application of Digital Watermarks

1. Visible watermarks can be used in following cases:

• Visible watermarking for enhanced copyright protection. In such situations, where images are made available through Internet and the content owner is concerned that the images will be used commercially (e.g. imprinting coffee mugs) without payment of royalties. Here the content owner desires an ownership mark, that is visually apparent, but which does not prevent image being used for other purposes.

• Visible watermarking used to indicate ownership originals. In this case images are made available through the Internet and the content owner desires to indicate the ownership of the underlying materials (library manuscript), so an observer might be encouraged to patronize the institutions that own the materia

2. Invisibal Robust Watermark

Invisible robust watermarks find application in following cases.

• Invisible watermarking to detect misappropriated images. In this scenario, the seller of digital images is concerned, that his, fee-generating images may be purchased by an individual who will make them available for free, this would deprive the owner of licensing revenue.

• Invisible watermarking as evidence of ownership. In this scenario, the seller that of the digital images suspects one of his images has been edited and published without payment of royalties. Here, the detection of the seller's watermark in the image is intended to serve as evidence that the published image is property of seller

3. Invisible marking on blank paper

Digital watermarks can also be adapted to mark white paper with the goal of authenticating the originator, verify the authenticity of the document content, or to date the document. Such applications are especially of interest for official documents, such as contracts. For example, the digital watermark can be used to embed the name of the lawyer or important information such as key monetary amounts. In the event of a dispute, the digital watermark is then read allowing authentication of key information in the contract. AlpVision developed genuine process to invisibly mark white blank paper with normal and visible ink. This patented technology is now known as Cryptoglyph.

The image on the left shows blank paper marked by the invisible digital watermark using standard visible ink, with the Cryptoglyph technology.

Invisible Fragile Watermarks

Following are the applications of invisible fragile watermarks.

• Invisible watermarking for a trustworthy camera. In this scenario, images are captured with a digital camera for later inclusion in news articles. Here, it is the desire of a news agency to verify that an image is true to the original capture and has not been edited to falsify a scene. In this case, an invisible watermark is embedded at capture time; its presence at the time of publication is intended to indicate that the image has not been attended since it was captured.

• Invisible watermarking to detect alternation of images stored in a digital library. In this case, images (e.g. human fingerprints) have been scanned and stored in a digital library; the content owner desires the ability to detect any alternation of the images, without the need to compare the images to the scanned materials

A watermark is very useful in the examination of paper because it can be used for dating, identifying sizes, mill trademarks and locations, and the quality of a paper.

One application of watermarking is in copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. In this use a copy device retrieves the watermark from the signal before making a copy; the device makes a decision to copy or not depending on the contents of the watermark.

Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark can be retrieved from the copy and the source of the distribution is known. This technique has been reportedly used to detect the source of illegally copied movies.

Annotation of digital photographs with descriptive information is another application of invisible watermarking.

While some file formats for digital media can contain additional information called metadata, digital watermarking is distinct in that the data is carried in the signal itself.

The use of the word of watermarking is derived from the much older notion of placing a visible watermark on paper.

D: Classification

A digital watermark is called robust with respect to transformations if the embedded information can reliably be detected from the marked signal even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise and quantization. For video content temporal modifications and MPEG compression are often added to this list. A watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, unwatermarked content.[1] In general it is easy to create robust watermarks or imperceptible watermarks, but the creation of robust and imperceptible watermarks has proven to be quite challenging.[2] Robust imperceptible watermarks have been proposed as tool for the protection of digital content, for example as an embedded 'no-copy-allowed' flag in professional video content [3]. Digital watermarking techniques can be classified in several ways

Robustness

A watermark is called fragile if it fails to be detected after the slightest modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that are clearly noticeable are commonly not referred to as watermarks, but as generalized barcodes.

A watermark is called semi-fragile if it resists benign transformations but fails detection after malignant transformations. Semi-fragile watermarks are commonly used to detect malignant transformations.

A watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copy protection applications to carry copy and access control information.

Perceptibility

A watermark is called imperceptible if the original cover signal and the marked signal are (close to) perceptually indistinguishable.

A watermark is called perceptible if its presence in the marked signal is noticeable, but non-intrusive.

Capacity

The length of the embedded message determines two different main classes of watermarking schemes:

A. The message is conceptually zero-bit long and the system is designed in order to detect the presence or the absence of the watermark in the marked object. This kind of watermarking schemes is usually referred to as Italic zero-bit or Italic presence watermarking schemes. Sometimes, this type of watermarking scheme is called 1-bit watermark, because a 1 denotes the presence (and a 0 the absence) of a watermark.

B. The message is a n-bit-long stream

($m = m_1 \ldots m_n,\ n \in \mathbb{N}$,)

X. with n = | m |) or M = {0,1}n and is modulated in the watermark. This kinds of schemes are usually referred to as multiple bit watermarking or non zero-bit watermarking schemes.

EMBEDDING METHOD

A watermarking method is referred to as spread-spectrum if the marked signal is obtained by an additive modification. Spread-spectrum watermarks are known to be modestly robust, but also to have a low information capacity due to host interference. A watermarking method is said to be of quantization type if the marked signal is obtained by quantization. Quantization watermarks suffer from low robustness, but have a high information capacity due to rejection of host interference. A watermarking method is referred to as amplitude

modulation if the marked signal is embedded by additive modification which is similar to spread spectrum method but is particularly embedded in the spatial domain.

Reversible data hiding
Reversible data hiding is a technique which enables images to be authenticated and then restored to their original form by removing the watermark and replacing the image data which had been overwritten. This would make the images acceptable for legal purposes.

IV -CHARACTERISTICS OF WATERMARKS

A: Characteristics of Visible Watermarks
A visible watermark should be obvious in both color and monochrome images. The watermark should spread in a large or important area of the image in order to prevent its deletion by clipping. The watermark should be visible yet must not signifi- cantly obscure the image details beneath it. The watermark must be difficult to remove. Rather, removing a watermark should be more costly and labor intensive than purchasing the image from the owner. The watermark should be applied automatically with little human intervention and labor.

B: Characteristics of Invisible Robust Watermarks
The invisible watermark should neither be noticeable to the viewer nor should degrade the quality of the content. An invisible robust watermark must be robust to common signal distortions and must be resistant to various intentional tamperings solely intended to remove the watermark Retrieval of watermark should unambiguously identify the owner .It is desirable to design a watermark whose decoder is scalable with each generation of computer While watermarking high quality images and art works the amount of pixel modification should be minimum. Insertion of watermark should require little human intervention or labor

C: Characteristics of Invisible fragile Watermarks
The invisible watermark should neither be noticeable to the viewer nor should degrade the quality of the content. An invisible fragile watermark should be readily modified when the image pixel values have been altered. The watermark should be secure. This means that it is impossible to recover the changes, or regenerate the watermark after image alternations, even when the watermarking procedure, and/or the watermark itself is known. For high quality images, the amount of individual pixel modification should be as small as possible

D: Characteristics of Video Watermarks
The presence of watermark should not cause any visible or audible effects on the playback of the video. The watermark should not affect the compressibility of the digital content.• The watermark should be detected with high degree of reliability. The probability of false detection should be extremely small. The watermark should be robust to various intentional and unintentional attacks.

IV- Conclusion
The watermarking research is progressing very fast and numerous researchers from various fields are focusing to develop some workable scheme. The dual watermarking is combination of a visible watermark and an invisible watermark. The invisible watermark is used as protection or back up for the visible watermark.The watermark is robust to common signal and geometric distortion such as A/D and D/A conversion, resampling, quantization, compression, rotation, translation, cropping and scaling. The watermark is universal in the sense that it can be applied to all three media. Retrieval of the watermark unambiguously identifies the owner and the watermark can be constructed to make counterfeiting almost impossible Different companies also working to get commercial products. We hope some commercial and effective schemes will be available in future.

REFERENCES

[1] Biermann, Christopher J. (1996) *Handbook of Pulping and Papermaking* (2 ed.). San Diego, California, USA: Academic Press. p. 171. ISBN 0-12-097362-6.
[2] Bender W., et. Al (1996) *IBM Systems Journal,*Vol 35, 313(23).
[3] Yeung Minerva (1998) *Communications of the ACM*, 31(3).
[4] Meggs Philip B. (1998) *A History of Graphic Design (Third ed.). John Wiley & Sons, Inc..* pp. 58. ISBN 978-0471291985.
[5] Craver Scott, et. Al (1998) Communications of the ACM, 45(9).
[6] Fraser Bruce (1998) Macweek, 22(1).
[7] http://www.ee.princeton.edu/~minwu/rsch_data hiding.html
[8] Zhao Jian, et. Al (1998) *Communications of the ACM*, 67(5).
[9] Metev S. M. and Veiko V. P. (1998) *2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag.*
[10] Memon Nasir, and Ping WaWong (1998) *ProtectingDigitalCommunications of the ACM,* 35(8).
[11] Yeung M., Yeo B. & Holliman M. (1998) *IEEE Micro*, 18(6), 32-41.
[12] Hwang Min-Shiang, et. Al (1999) *IEEE Transactions on Computer Electronics*, Vol 45, 286(8).
[13] Zhao J., Koch E., & Luo C. (1998) *Communications of the ACM*,41(7), 67-71.
[14] Voyatzis G., and Pitas I. (1999) *IEEE Computer Graphics & Applications, 19*(1),18-24.