ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

Digital Watermarking

Sahil Anand, Swati Mehla, Samiksha Arya, Piyush Kapoor

Abstract-Digital watermarking is basically a technique that embeds a watermark into two integrated images such that the watermark can be extracted by overlaying these into half toned images. These water markings techniques are used to Coded anti-piracy, attack, constellation, Pattern,Steganography. Basically very helpful in medical sciences and authenticating various products. The watermark images in these strategies are binary images and the pixels in the two halftone images are interrelated or not depending on whether the corresponding pixel in the watermark. In these strategies, the watermark is binary and does not contain detailed features. Digital Watermarking is based on the fact of "perceptual invisibility," this paper makes a study of the maximum watermarking of spatial domain image, which is related to not only embedding intensity, but also to factors such as the size of image, image roughness and visual sensitivity, and so forth. The interrelation among the maximum payload and the embedding intensity and size of an image is theoretically deduced through the objective estimation indicator of the peak signal to the noise rate (PSNR) while the relationship model among Digital watermarking and image roughness and visual sensitivity is deduced through effective experiments designed on the basis of subjective estimation indicators. Finally, taking all these relationship models into account, this paper proposes a Digital watermarking estimation method and verifies its effectiveness through experiments.

Keywords: **PSNR, *FMCG*, SSW, PN, JPEG.**

I. INTRODUCTION

Digital Watermarking is an account of the commonly used and well known paper watermarks to the digital world. The research on technologies of information hiding and digital watermarking has developed for nearly twenty years. Information hiding is applied to covert communication, and digital watermarking is applied to copyright protection. They share one common feature: When some data are organised into the carrier data, no obvious damage is caused. Therefore, the key point of information thrashing and digital watermarking is the same and that's what is called information hiding in a broad sense. However, differences in their application environments result in different study emphasis and needs. Information hiding emphasizes on the confrontation to steganalysis attacks while digital watermarking stresses the perceptual invisibility.

A. Digital Watermarking basics:

Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. The embed of information should be such that it should not create any visible effect in the image by changing the value of the pixels. The example below shows that digital watermarking allows hiding information in a totally invisible manner. The real image is on the left; the watermarked image is on the right and contains the name of the writer.

Fig 1. General Image[8]

B. Digital Watermarking Description

A watermark is a clear image in paper that can be seen in many shades of lightness/darkness when viewed by transmitted light affected by thickness variations in the paper. A watermark well-established in a data file ensures a method of authentification of data which combines aspects of data hashing and digital watermarking. Both are useful for fiddle detection, though each has its own advantages and disadvantages. Digital watermarking is the process of possibly irreversibly embedding information. A subscriber, with knowledge of the watermark and how it is recovered, can determine changes in a file, lossy compression. A disadvantage of digital watermarking is that a subscriber cannot significantly alter some files without sacrificing the quality or utility of the data

Fig 2. Example[8]

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

An image with visible digital watermarking - the text "Brian Kell 2006" is visible across the centre of the image in visible digital 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. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark.

In invisible digital 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 in the signal). a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals. 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 whether to copy or not, depending on the contents of the watermark. Another application is in source tracing. Annotation of digital photographs with descriptive information is another application of invisible watermarking. While some file formats for digital media may contain additional information called metadata, digital watermarking is distinctive in that the data is carried right in the signal.

II. APPLICATIONS

Digital watermarking may be used for a wide range of applications, such as:

- Copyright protection
- Source tracking (different recipients get differently watermarked content)
- Broadcast monitoring (television news often contains watermarked video from international agencies)
- Covert communication

Digital watermarking life-cycle phases

General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions the information to be embedded in a signal 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.

Then the watermarked digital signal is 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 (in which resolution is diminished), cropping an image or video or intentionally adding noise.

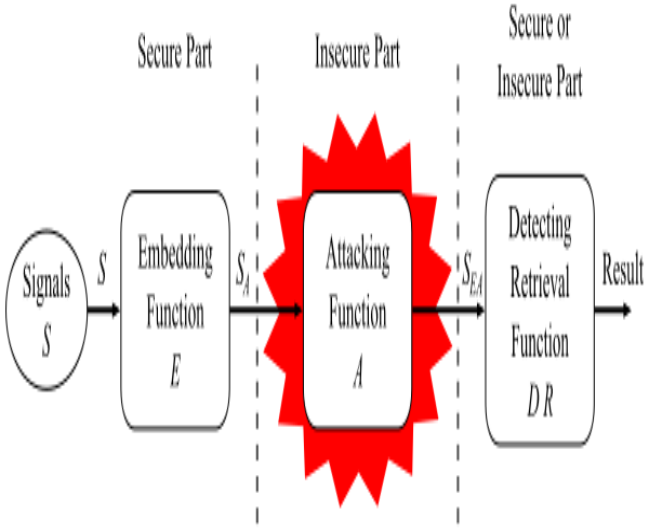

Fig 3. Block Diagram[8]

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 still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

III. CLASSIFICATION

A digital watermark is called robust with respect to transformations if the embedded information may be detected reliably 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 often are added to this list. A digital watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, unwatermarked content. 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. 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. Digital watermarking techniques may be classified in several ways.

Robustness

A digital watermark is called fragile if it fails to be detectable after the slightest modification. Fragile

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that clearly are noticeable commonly are not referred to as watermarks, but as generalized barcodes. A digital 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 no access control information.

Perceptibility

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

- 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 scheme is usually referred to as zero-bit or 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.
- The message is a n-bit-long stream ($m = m_1 \ldots m_n,\ n \in \mathbb{N}$, with n = | m |) or M = $\{0,1\}^n$ and is modulated in the watermark are referred to as multiple-bit watermarking .

IV. EMBEDDING METHOD

A digital 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

Evaluation and Benchmarking

The evaluation of digital watermarking schemes may provide detailed information for a watermark designer or for end-users, therefore, different evaluation strategies exist. Often used by a watermark designer is the evaluation of single properties to show, for example, an improvement. Mostly, end-users are not interested in detailed information. They want to know if a given digital watermarking algorithm may be used for their application scenario, and if so, which parameter sets seems to be the best.

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 digital watermark and replacing the image data that had been overwritten. This would make the images acceptable for legal purposes. The U.S. Army also is interested in this technique for authentication of reconnaissance images. http://en.wikipedia.org/wiki/Digital_watermarking - cite_note-Uhh-6

Watermarking For Relational Databases

- Coded Anti-Piracy
- Copy attack
- EURion constellation
- Pattern Recognition (novel)
- Steganography
- Watermark (data file)
- Watermark detection

Digital Video and Audio watermark detection

Digital video watermarking can be achieved by either applying still image technologies to each frame of the movie or using dedicated methods that exploit inherent features of the video sequence. Watermarking is the process of embedding information into a signal (e.g. audio, video or pictures) in a way that is difficult to remove. If the signal is copied, then the information is also carried in the copy. A signal may carry several different watermarks at the same time. Watermarking become more and more important to enable copyright protection and ownership verification. One of the most secure techniques of audio watermarking is spread spectrum audio watermarking (SSW). Spreading spectrum is done by a pseudo noise (PN) sequence.

Copy attack

- In some scenarios, a digital watermark is added to a piece of media such as an image, film, or audio clip, to prove its authenticity. The copy attack attempts to thwart the effectiveness of such systems by estimating the watermark given in an originally watermarked piece of media, and then adding that watermark to an un-watermarked piece. The following diagram shows the evaluation procedure we employ to test the robustness of video watermarking solutions against compression. Each frame of the video is first watermarked using a 64 bit signature. The resulting signed frames are then compressed using an MPEG-2 encoder at different bit rates.

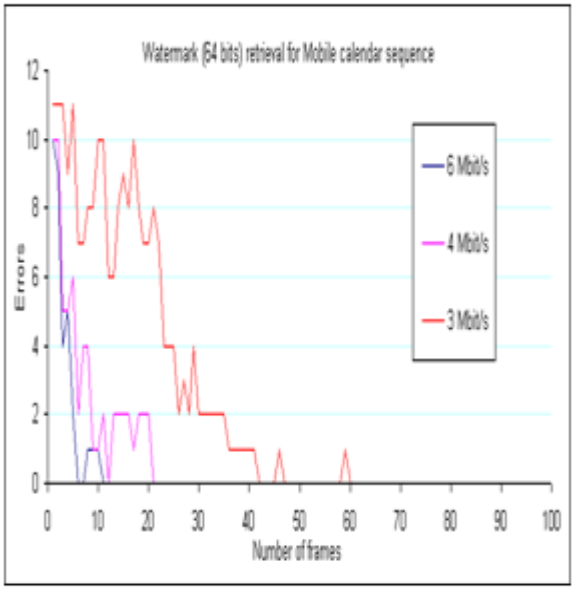

Fig 4. Result Graph[8]

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

In other words, the signature is retrievable from less than 500 ms of video compressed at 6 Mbit/s and about 2.5 seconds of video compressed at 3 Mbit/s. It should be noted that 3 Mbit/s is a fairly low bit rate for a CCIR-601 sequence and that it creates compression artefacts that are substantially more visible than the watermark itself.

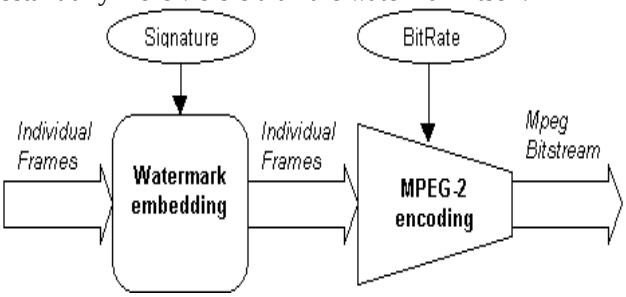

Fig 5. Watermark Embedding Method[8]

Fig 6. signed.avi & signer.m2v[8]

To recover the embedded signature, the video bit stream is first decompressed and then each individual frame is passed through the watermark detection system. If the detection is perfect all the bits of the retrieved signature are correct and the same signature is found in each frame. This also means that only one single frame is required to recover the embedded information. However, practice has shown that in order to keep the watermark invisible, only very slight modifications of the frames are acceptable. As a consequence, and depending on the compression bit rate, some of the signature bits may therefore be wrongly detected on individual frames. An additional step based on statistical analysis over several frames is therefore required in order to correct possible errors.

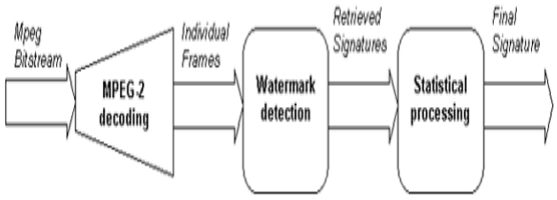

Fig7 .Flow Diagram[8]

Is your brand adequately protected?

The protection of consumer and industrial products against counterfeiting and fraudulent imports is a major concern of every brand owner. It remains a constant battle as market diversion and counterfeiting increase, as shown by statistics on custom seizures. Protect billions of FMCG against counterfeiting and market diversion: cryptoglyph is the security solution that invisibly marks labels, primary and secondary packaging for food, beverage, tobacco, cosmetics and pharmaceutical products or any other Fast Moving Consumer Goods (FMCG), using standard visible ink or varnish.

Protect Solid Parts and Components[8]:

For metallic or plastic parts such as wristwatches ,jewellery automotive and aerospace components, ICs, and medicine tablets, technology based on the object "as is", namely the identification of the intrinsic characteristics of a solid object. This unique pattern depends on the raw material and the industrial manufacturing process used. No additional markings are necessary. High tech digital imaging software is used to identify the genuine object from fake ones.

Go Global Using Online Authentication[8]:

Global markets need global mobile solutions working worldwide. Developed an open platform that integrates various levels of product security detection as well as delivering information about products. An online brand authentication system, which includes the Cryptoglyph convert security solution as well as Fingerprint

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

Authenticate Products In The Field[8]:

Simple off-the-shelf flatbed scanner, digital camera or camera phone are used when inspecting products in the field with detection software. Information is sent to the secured online authentication system which returns a "genuine" or "fake" verdict after a few seconds.

V. CONCLUSION

In the recent twenty years, the technology of information hiding has been widely applied to fields of copyright protection (digital watermarking), communication, and so forth. At present, most researches focus on how to embed information without visual distortion and there have been few researches on the maximum payload, that is, the maximum payload under the constraint of perceptual invisibility.

This paper proposes the estimation method for the maximum payload. The maximum payload is influenced not only by internal but also external factors. The external factors are mainly the image size, embedding intensity, and so forth while the internal factors are mainly the image roughness, visual sensitivity, and so forth. The size of image is in direct proportion to the payload while the embedding intensity is in inversely proportional to the payload because higher bits embedding generates more noise than lower bits embedding does and the noise is the normalized indicator of image distortion. Different degrees in roughness result in different perceptibility because while it is difficult for the human eyes to identify the subtle changes in a highly rough image, it is easy to identify such changes in a smooth image. The sensitivity of human eyes to changes in different images is varied, which is affected by image contrast and brightness. The correlation between the maximum payload and the embedding intensity and size of image is theoretically deduced through the objective estimation indicator of the peak signal to noise rate (PSNR) while the relationship model between watermarking payload and image roughness and visual sensitivity is deduced through effective experiments designed on the basis of subjective estimating indicators. Finally, taking into account of all these relationship models, this paper proposes the watermarking payload estimation method and verifies its effectiveness through experiments. There are still shortcomings in our method and further research is still needed to improve the estimating accuracy. (1)The method is rough. This paper makes a study of the maximum watermarking payload of spatial domain image under the conditions of invisibility, in another word, the maximum embedding payload. Different area has the different payload capacity. For example, the payload of high roughness and perceptual invisibility areas is higher than the area of low roughness and visual sensitive areas. This article does not do further research of this aspect; it is the deficiency of this article and also further research directions of ours, which is closer to the practical applications.(2)The experimental plan lacks novelty. Since evaluation of visual perceptibility in images is needed in the experiments, it costs much time of the experts. In the future work, better plans will be designed to save the expert's time and to improve accuracy in estimating.

REFERENCES

[1] www.itstudyguide.com/**paper**s/cwdiss780annotatedbib.

[2] domino.watson.ibm.

[3] www.scielo.cl/pdf/jtaer/v3n3/art08.

[4] www.waset.org/journals/waset/v45/v45-8.

[5] Www.Com/watermarking.html.

[6] ec.europa.eu/justice/policies/privacy/docs/...rights/dwwg_en.

[7] ieeexplore.ieee.org › ... › Conferences › Image and Signal Processing.

[8] http://www.alpvision.com.