Volume 2, Issue 8, August 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Digital Watermark: A Study

Er. Jaspreet Kaur *
Assistant Professor, IT dept.
GNDEC, Ludhiana
Ludhiana, Punjab, India

Er. Karmjeet Kaur
Assistant Professor, CSE dept.
BCET, Ludhiana
Ludhiana, Punjab, India

Abstract— The digital data can be very easily duplicated and edited which generate the need for effective copyright protection tools. The Digital watermarking is the process of embedding additional data along with the digital audio, images and video. There are number of watermarking techniques used today. This paper covers the general watermarking principles and focuses on describing various watermarking applications.

Keyword-- Digital watermarking; copyright protection; spatial domain; frequency domain; Fragile Watermarks

I. INTRODUCTION

Due to the developments in computer and internet technology, multimedia data i.e. audio, images and video are transmitted through over the world. In the recent time, as the technologies are developed side by side we need methods to prevent illegal copying of multimedia that is transmitted over the internet. One of the best methods is Digital watermarking. Encryption method is also used for security of data but it requires the decryption key on another side to get original contents. But once the data is decrypted, it can be duplicated and distributed illegally. To enforce IP rights and to prevent illegal duplication, interpolation and distribution of multimedia data, Digital

Watermarking is an effective solution. Digital watermarking can be used to achieve Copyright protection, data authentication, covert communication and content identification [1,2]. A digital watermark is used for identification of the original digital documents. It is permanently embedded into digital data, carrying information on copyright protection and data authentication. A digital watermark is like a digital signal or information inserted into a digital image. Since this signal or information is present in each unaltered copy of the original image, the digital watermark may also serve as a digital signature for the copies.

During watermarking technique, it is required that quality of host signal should not be degraded. In order to achieve the copyright protection, the algorithm should meet few basic requirements [2]:

- *Imperceptibility*: To preserve the quality of original signal, digital watermark should be invisible/inaudible to human eyes/ ears.
- *Robustness*: Unauthorized distributors can't remove or eliminate watermarked data, thus it should be robust to resist common signal processing manipulations such as filtering, compression, filtering with compression.
- *Capacity*: the number of bits that can be embedded in one second of the host signal.
- Security: The watermark should only be detected by authorized person.
- Watermark detection should be done without referencing the original signals.
- The watermark should be undetectable without prior knowledge of the embedded watermark sequence.
- The watermark is directly embedded in the signals, not in a header of the signal.

All these requirements are often contradictory with each other and we need to make a trade-off among them. For example increasing data rate in watermarking system results in quality degradation of the watermarked signal and decreases the robustness against attacks. Imperceptibility and robustness are the most important properties for many applications [3,4]. These conflicting requirements pose many challenges to design of robust watermarking.

A. *Types of digital watermarks*

According to *casual viewer*, digital watermarking is of three types:

1) *Visible watermarks*: are visible to casual viewer. These are used in much the same way as their bond paper ancestors, whereby the opacity of paper is altered by physically stamping it with an identifying pattern [13]. This is done to mark the paper manufacturer or paper type. One might view digitally watermarked documents and images as digitally "stamped".

Any text or logo to verify or hide content

$F_w = (1-\alpha)\ F + \alpha * W$ [10]

F_w = Watermarked Image
α = constant; 0<=α<=1, IF α=0 No watermark, if α=1 then watermark present
F = original image
W =watermark

2) *Invisible watermarks*: In the event of illicit usage, the watermark would facilitate the claim of ownership, the receipt of copyright revenues, or the success of prosecution. Invisible watermarking, aim is to permanently and unalterably mark the image so that the credit or assignment is beyond dispute [13]. On the other hand, are potentially useful as a means of identifying the source, author, creator, owner, and distributor or authorized consumer of a document or image. Invisible watermarked are embedded in the original image in such a way that it can not be perceived by human eye. It is used to provide image authentications and to prevent it to be copied. It is of three types[31,36].
   - *Robust Watermarks*: This type of invisible watermark, do not destroy the original image. Different types of attack done in intentional (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. The main goal is to provide security
   - *Fragile Watermarks*: used to just check the integrity of object, having very low robustness.
   - *Public and Private Watermark*: They are differentiated in accordance with the secrecy requirements for the key used to embed and retrieve watermarks [13]. If the original image is not known during the detection process then it is called a public or a blind watermark and if the original image is known it is called a non blind watermark or a private watermark.
3) *Dual watermark* : is the combination of visible and invisible watermarks. An original digital item that contain both visible and invisible information for authentication. An invisible watermark is used as a backup for the visible watermark.

According to *Working Domain*, the watermarking techniques can be divided into two types

a) *Spatial Domain Watermarking Techniques*: In spatial domain techniques, the watermark embedding is done on image pixels [11].
b) *Frequency Domain Watermarking Techniques*: In frequency domain watermarking techniques the embedding is done after taking image transforms. Generally frequency domain methods are more robust than spatial domain techniques.

According to the watermarking extraction process, techniques can be divided into three types

a) *Non-blind*: Non-blind watermarking schemes require original image and secret key for watermark detection.
b) *Semi-blind* : In this schemes require secret key and watermark bit sequence for extraction.
c) *Blind*: In this schemes need only secret keys for extraction.

B. Visible versus invisible watermarks

Visible and invisible watermarks both work in different ways but main purpose is to provide copyright protection. Both serve to deter. Visible watermarks are especially useful where an immediate claim of ownership is required. The main advantage of visible watermarks is that they virtually eliminate the commercial value of the document to a would-be thief without lessening the document's utility for legitimate, authorized purposes. A familiar example of a visible watermark is in the video domain where CNN and other television networks place their logo at the bottom right of the screen image.

Invisible watermarks, on the other hand, are more of an aid in catching the thief than discouraging the theft in the first place.

II. WORKFLOW

The digital watermarking workflow consists of three activities that all build on each other and the contextual information provided at each stage to enable increasingly rich and interactive applications. A watermarking system is usually divided into three distinct steps, embedding, attack and detection as shown in Figure.1.

a) *Embed*: In the embedding stage original watermark signal is embedded in the original image to create a watermarked image. That watermarked image can be transmitted to other user.
b) ***Attack***: When the watermarked image is transmitted to other user, if modifications are done by that user then its called attack. The detection algorithms are applied on attacked signal to extract original watermark from it.
c) *Detect*: Once detected, a wide variety of responses are enabled based on the data carried in the watermark, or referenced in response to the presence of the watermark.

The P2P client (application) can incorporate other applications or plug-ins in addition to watermark detection and response application, such as data hash evaluators, acoustic fingerprint analyzers, and metadata readers.

When used in conjunction with watermark detection and response, they empower a more robust detection and response environment.

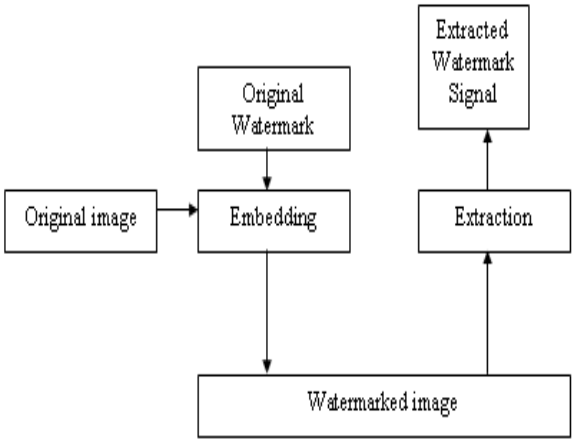

Figure.1 Watermarking block diagram

III. TECHNIQUES FOR WATERMARKING

Watermarking techniques tend to divide into two categories, text and image, according to the type of document to be watermarked.

A. Several different methods enable watermarking in the spatial domain. The simplest is to just flip the lowest-order bit of chosen pixels in a grey scale or colour image. This will work well only if the image is subjected to any human or noisy modification. A more robust watermark can be embedded in an image in the same way that a watermark is added to paper. Such techniques may superimpose a watermark symbol over an area of the picture and then add some fixed intensity value for the watermark to the varied pixel values of the image. The resulting watermark may be visible or invisible depending upon the value of the watermark intensity. One disadvantage of spatial domain watermarks is that picture cropping can be used to eliminate the watermark.

B. Spatial watermarking can also be applied using colour separation. In this way, the watermark appears in only one of the colour bands. This renders the watermark visibly subtle so that it is difficult to detect under regular viewing. However, the watermark appears immediately when the colours are separated for printing or xerography. This renders the document useless to the printer unless the watermark can be removed from the colour band. This approach is used commercially for journalists to inspect digital pictures from a photo-stockhouse before buying non-watermarked versions.

C. Watermarking can be applied in the frequency domain (and other transform domains) by first applying a transform like the Fast Fourier Transform. In a similar manner to spatial domain watermarking, the values of chosen frequencies can be altered from the original. Since high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies that contain important information of the original picture (feature-based schemes). Since watermarks applied to the frequency domain will be dispersed over the entirety of the spatial image upon inverse transformation, this method is not as susceptible to defeat by cropping as the spatial technique. However, there is more of a tradeoff here between invisibility and decodability, since the watermark is, in effect, applied indiscriminately across the spatial image.

D. Watermarking can be applied to text images as well. Three proposed methods are: text line coding, word space coding and character encoding.
   - For text line coding, the text lines of a document page are shifted imperceptibly up or down. For a 40-line text page, for instance, this yields 2**40 possible codewords.
   - For word-shift coding, the spacing between words in a line of justified text is altered.
   - For character coding, a feature such as the endline at the top of a letter "t" is imperceptibly extended.

   An advantage of these methods over those of picture images is that, by combining two or three of these to one document, two documents with different watermarks cannot be spatially registered to extract the watermark. Of course, the watermark can be defeated by retyping the text.

IV. DIGITAL WATERMARKING APPLICATIONS

A. *Copyright protection*: The most important application of watermarking is to provide copyright protection. Visible watermarking is used for copyright protection [5, 6]. The owner can protect the data audio, image or video from being used commercially if it is available on internet. The ownership mark should be clearly visible in such cases. Copyright protection requires high level of robustness so that the embedded watermark can not be removed without data distortion [12]. This watermark is extracted to show as proof if someone claims the ownership of the data.

B. *Finger Printing*: A robust watermarking algorithm is required for this application [9]. Watermark is embedded in digital data to trace the source of illegal copies. Information related to customer like serial number or customer identity information is used as watermark. Finger printing is similar to giving serial number to any product. The objective is to convey the information about the legal recipients. If any illegal copy is found, can be found by extracting the watermark.

C. *Content Authentication (integrity protection*): To check the integrity of data different algorithm are available with the help of those we can find how much and how the data is altered. Invisible watermark is an evidence of ownership [7, 8]. The objective of this application is to detect modification in data. To verify the authenticity of the received data watermark is embedded in host data. A fragile watermarking algorithm is required in this case.

D. *Broadcast Monitoring*: The main use of broadcast monitoring is to protect TV products like news items from illegal transmission [12]. Watermark is embedded in commercial advertisements. Automated monitoring system can verify whether the advertisements are broadcasted as contracted or not.

E. *Indexing*: Search engine use this technique to retrieve the required data in a short period of time and without any ambiguity. In indexing, Comments and markers or key information related to the data is inserted as watermark.

F. *Medical Applications*: To avoid ambiguities in searching the medical report of the patient use watermarking technique. In which patient's information is inserted as watermark in medical images.

This research suggests that not all watermarking techniques will be useful in resolving ownership disputes in courts of law. There are likely to be non-commercial applications, or those with limited vulnerability to theft, where "good enough watermarking" will suffice. More sensitive applications may require non-invertable or non-extracting watermarking techniques. These issues are under consideration at the time of writing.

V. CONCLUSIONS

In some watermarking techniques the detection process requires the original signal. These systems are not suitable for the applications where the original signal is not accessible at the detection or it is unacceptable to disclose it. According to the paper, we can conclude that watermarking is a potential approach for protection of ownership rights on digital properties. According to different applications, there are different requirements of the watermarking system. However, it is hard to satisfy all the requirements at the same time. A variety of techniques in different domains have been suggested by different authors to achieve above mentioned conflicting requirements. All watermarking techniques are different from each other and are used for differing applications.

REFERENCES

[1] Jian Liu, Xiangjian He; "A Review Study on Digital Watermarking", Information and Communication Technologies, 2005. ICICT 2005. First International Conference, Page(s):337 – 341, 27-28 Aug. 2005.

[2] Cox, I.J., M.L. Miller, and J.A. Bloom, "Digital Watermarking.", 1st edition 2001, San Francisco: Morgan Kaufmann Publisher.

[3] I.J.Cox, et al., "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. on Image Processing, Vol.6, No.12, Dec 1997, pp.1673-1687.

[4]) O'Ruanaidh J J K, Dowling W J, Boland F M., "Watermarking digital images for copyright protection" IEE Proceedings-Vision, Image and Signal Processing. 143 (4): 250-256, 1996.

[5] M.A.Dorairangaswamy, B.Padhmavathi, "An Effective Blind Watermarking Scheme for Protecting Rightful Ownership of Digital Images", IEEE international conference TENCON 2009.

[6] Ming-Chiang Hu, Der-Chyuan Lou and Ming-Chang Chang, "Dualwrapped digital termarking scheme for image copyright protection," Computers & Security, Vol. 26, No. 4, pp. 319-330,2007

[7] Jun Tian, "Reversible Data Embedding Using a Difference Expansion," IEEE Trans. Circuts and Systems for Video Technology, vol. 13, no. 8, pp. 890-896, Aug. 2003

[8] W. Zeng and B. Liu, "A statistical watermark detection technique without using original mages for resolving rightful ownerships of digital images", IEEE Transactions on Image Processing, Vol. 8, No. 11, pp. 1534-1548, 1999.

[9] Michael Arnold, Martin Schmucker, Stephen D.Wolthusen, "Techniques and Applications of Digital Watermarking and Content Protection", 1st edition July 2003, Artech House.

[10] K. R. Rao and P. Yip, "Discrete Cosine Transform: Properties, Algorithms, Advantages, Applications", Academic Press, Massachusetts, 1990.
[11] Mistry D., "Comparison of water marking methods", *IJCSEt.*, vol. 2, ISSN : 0975-3397, pp. 2905-2909, Sept. 2010.
[12] S. Vipula, "Digital Watermarking : A Tutorial", *JSET*, pp. 10-21, Jan 2011.

[13] Syed A. A., "Digital Watermarking" The University of Texas at Arlington.

