www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 12, Dec.2013 Page No. 3405-3410

Data Protection Using Digital Watermarking

Kapil Kumar Kaswan[1]**, *Dr. Roshan Lal***[2]
[1]Research Scholar,Mewar university,Chittorgarh,Rajasthan,india.
[2]Assistant Prof., Govt College,Karnal,Haryana,India.
[1]E-mail: kapilkaswan@gmail.com
[2]E-mail: Roshanhiranwal@gmail.com

Abstract: Digital watermarks allow information about the owner, usage rights and more to be permanently attached to the content. Watermarking is the art and science of communicating in such a way that the presence of a message cannot be detected. Simply steganographic techniques have been in use for hundreds of years, The other major area of copyright marking, where the message to be inserted is used to assert copyright over a document can be further divided into watermarking and fingerprinting. Digital watermarking has been proposed as a solution to the problem of copyright protection of multimedia data in a networked environment. It makes possible to tightly associate to a digital document a code allowing the identification of the data creator, owner, authorized consumer, and so on

keywords: DWT, DCT, Stegnography,Spatial Domain, Watermarking

I. INTRODUCTION

The digital communication is the backbone the society now. The digital data such as text, images and audio are stored and transmitted at high speed. It is easy copy the digital data. There is therefore a need to evolve a mechanism to check the illegal operation on the digital data. One of the ways is to hide secret information/identification inside digital data. This information can be used to prove copyright ownership, to identify attempt to temper with sensitive data and to embed annotation. There are mainly three ways of hiding data,Steganography ,Digital watermarking ,Fingerprinting.Steganography relates to convert point-to-point communication. Thus steganography is not robust against modification of data, or have limited robustness. Watermarking has additional notion of resilience against attempts to remove the hidden data. All watermarking methods shares same generic blocks,A watermark, embedding system and a watermark recovery system. Watermark can be any text, image and audio, visible or invisible.Fingerprinting is a special case of watermarking. A fingerprinting means watermarking where embedded information is either a unique code specifying the author or a unique code of the recipient of the data. So fingerprints are characteristics, which is capable of distinguishing objects of similar type. While the stenography deals with techniques of hiding information, the branch of steganalysis deals with detection and / or estimation of potentially hidden information from observed data with little or no knowledge about the steganography algorithm and/ or its parameters.

2. DIGITAL WATERMARKING

Paper watermarks appeared in the art of handmade papermarking 700 hundred years ago. Watermarks were mainly used to identify the mill producing the paper and paper format, quality and strength. Paper watermarks were a perfect technique to eliminate confusion from which mill paper is and what are its parameters. Paper watermarks in bank notes or stamps inspired the first use of the term *water mark* in the context of digital data. The first publications that really focused on watermarking of digital images were from 1990 and then in 1993.

2.1 WATERMARKING CONCEPT

A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted later by means of computing operations in order to make assertions about the data. The watermark is hidden in the host data in such a way that it is inseparable from the data and so that it is resistant to many operations not degrading the host document. Thus by means of watermarking, the work is still accessible but permanently marked.Digital watermarking is divided into two main categories: visible and invisible. The idea behind the visible watermark is very simple. It is equivalent to stamping a watermark on paper, and for this reason is sometimes said to be digitally stamped. An example of visible watermarking is provided by television channels, like BBC, whose logo is visibly superimposed on the corner of the TV picture. Invisible watermarking, on the other hand, is a far more complex concept. It is most often used to identify copyright data, like author, distributor, and so forth. Though a lot of research has been done in the area of invisible watermarks, much less has been done for visible watermarks. Visible and invisible watermarks both serve to deter theft but they do so in very different ways. Visible watermarks are especially useful for conveying an immediate claim of ownership. Their main advantage, in principle at least, is the virtual elimination of the commercial value of a document to a would-be thief, without lessening the document's utility for legitimate, authorized purposes. Invisible watermarks, on the other hand, are more of an aid in catching a thief than for discouraging theft in the first place. It seems that digital watermarking is a good way to protect intellectual property from illegal copying. It provides a means of embedding a message in a piece of digital data without destroying its value. Digital watermarking embeds a known message in a piece of digital data as a means of identifying the rightful owner of the data. These techniques can be used on many types of digital data including still imagery, movies, and music.

2.2 WATERMARKING CLASSIFICATION

There are different classifications of invisible watermarking algorithms. The reason behind this is the enormous diversity of watermarking schemes. Watermarking approaches can be distinguished in terms of watermarking host signal (still images, video signal, audio signal, integrated circuit design), and the availability of original signal during extraction (non-blind, semi-blind, blind). Also, they can be categorized based on the domain used for watermarking embedding process, as shown in Figure 2.1. The watermarking application is considered one of the criteria for watermarking classification. Figure 2.2 shows the subcategories based on watermarking applications.

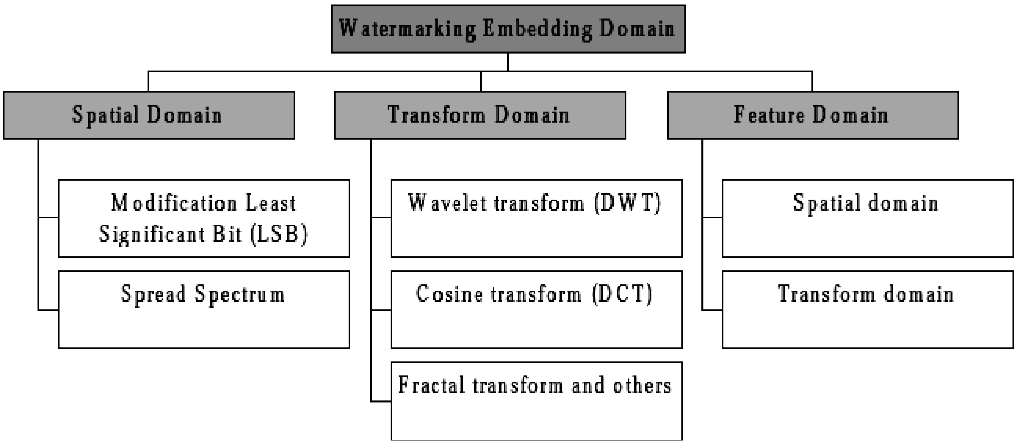


Figure 2.1 Classification of Watermarking Based on Domain

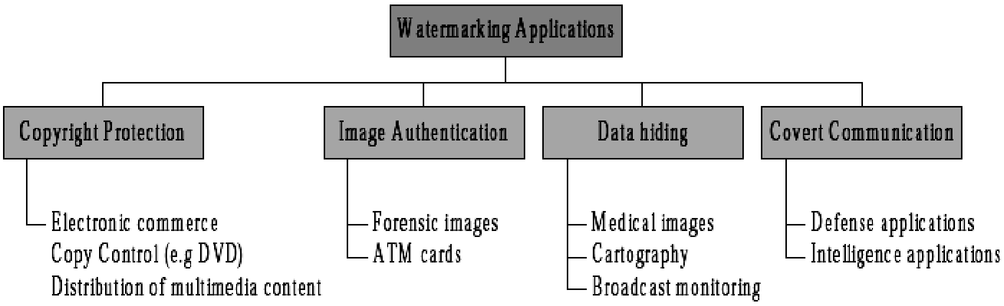


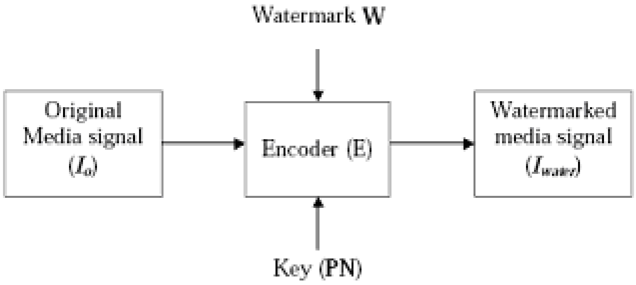
Figure 2.2 Classification of Watermarking Based on Applications

2.3 WATERMARK EMBEDDING

Generally, watermarking systems for digital media involve two distinct stages: (1) watermark embedding to indicate copyright and (2) watermark detection to identify the owner Embedding a watermark requires three functional components: a watermark carrier, a watermark generator, and a carrier modifier. A watermark carrier is a list of data elements, selected from the un-watermarked signal, which are modified during the encoding of a sequence of noise-like signals that form the watermark. The noise signals are generated pseudo-randomly, based on secret keys, independently of the carrier. Ideally, the signal should have the maximum amplitude, which is still below the level of perceptibility

The watermark *W* is encoded into *Iorig* using an embedding function *E*

$$E(Iorig\ ,\ W\ ) = Iwater$$



Watermark W
Original Media signal (I_o)
Encoder (E)
Watermarked media signal (I_{water})
Key (PN)

Figure 2.3 (a) Watermark Embedding System

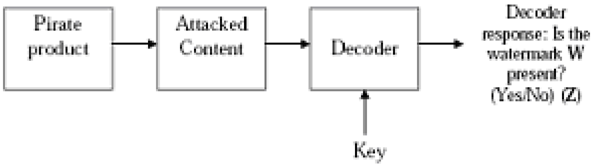


Figure 2.3 (b) Watermark Detecting System

The carrier modifier adds the generated noise signals to the selected carrier. To balance the competing requirements for low perceptibility and robustness of the added watermark, the noise must be scaled and modulated according to the strength of the carrier. Embedding and detecting operations proceeds as follows. Let *Iorig* denote the original multimedia signal (an image, an audio clip, or a video sequence) before watermarking, let *W* denote the watermark that the copyright owner wishes to embed, and let *Iwater* denote the signal with the embedded watermark. A block diagram representing a general watermarking scheme is shown in Figure 2.3.

The embedding function makes small modifications to *Iorig* related to *W*. For example, if *W* = (*w1*, *w2*, ...), the embedding operation may involve adding or subtracting a small quantity *a* from each pixel or sample of *Iorig*. During the second stage of the watermarking system, the detecting unction *D* uses knowledge of *W*, and possibly *Iorig*, to extract a sequence *W'* from the signal *R* undergoing testing:

$$D(R, Iorig) = W'$$

The signal *R* may be the watermarked signal *Iwater*, it may be a distorted version of *Iwater* resulting from attempts to remove the watermark, or it may be an unrelated signal. The extracted sequence *W'* is compared with the watermark *W* to determine whether *R* is watermarked. The comparison is usually based on a correlation measure ρ, and a threshold λ_o used to make the binary decision (*Z*) on whether the signal is watermarked or not. To check the similarity between *W*, the embedded watermark and *W'*, the extracted one, the correlation measure between them can be found using:

$$\rho(W, W') = \frac{W \cdot W'}{\sqrt{W' \cdot W'}}$$

Where *W, W'* is the scalar product between these two vectors. However, the decision function is:

$$Z(W', W) = \begin{cases} 1, & \rho \geq \lambda_0 \\ 0 & otherwise \end{cases}$$

where ρ is the value of the correlation and λ_o is a threshold. A *1* indicates a watermark was detected, while a *0* indicates that a watermark was not detected. other words, if *W* and *W'* are sufficiently correlated (greater than some threshold λ_o), the signal *R* has been verified to contain the watermark that confirms the author's ownership rights to the signal. Otherwise, the owner of the Figure 1.8 shows the detection threshold experimentally (of 600 random watermark sequences studied, only one watermark — which was origanally inserted — a higher correlation output above others) (Threshold is set to be 0.1 in this graph.)

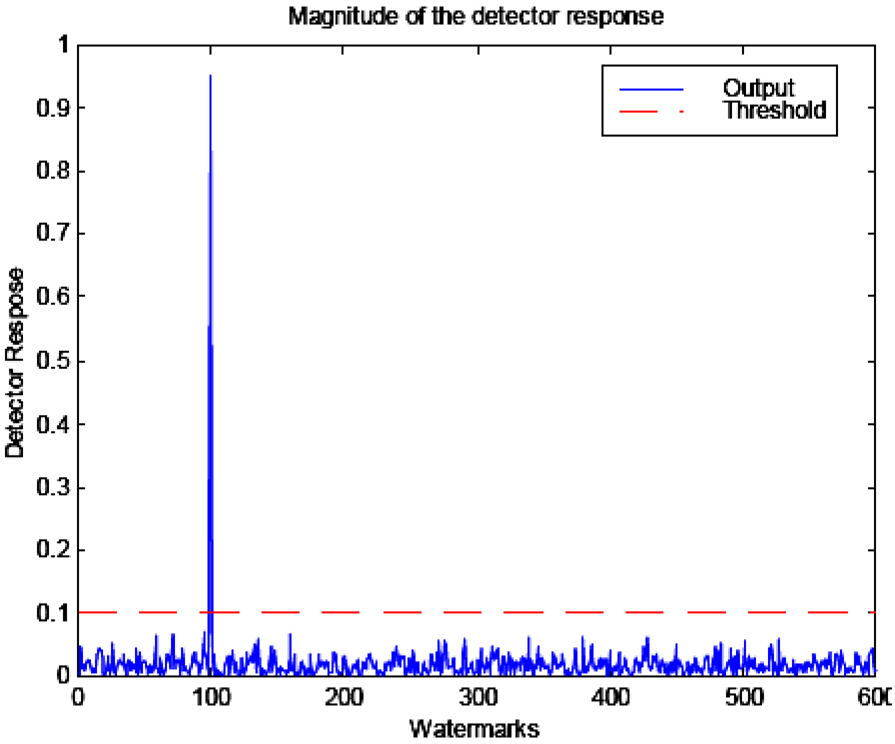


Figure 2.4 Detection threshold experimentally

Watermark *W* has no rights over the signal *R*. It is possible to derive the detection threshold λ_o analytically or empirically by examining the correlation of random sequences. Figure 1.8 shows the detection threshold of 600 random watermark sequences studied, and only one watermark, which was originally inserted, has a significantly higher correlation output than the others. As an example of an analytically defined threshold, τ can be defined as:

$$\tau = \frac{\alpha}{3N_c}\sum^{N_c} \; | I_{water}(m,n) |$$

Where α is a weighting factor and *Nc* is the number of coefficients that have been marked. The formula is applicable to square and non-square images.One can even just select certain coefficients (based on a pseudo-random sequence or a human visual system (HVS) model). The choice of the threshold influences the false-positive and false- negative probability. Hernandez and Gonzalez (1999) propose some methods to compute predictable correlation thresholds and efficient watermark detection systems. Figure 2.5 shows the basic scheme for watermark recovery schemes.

.

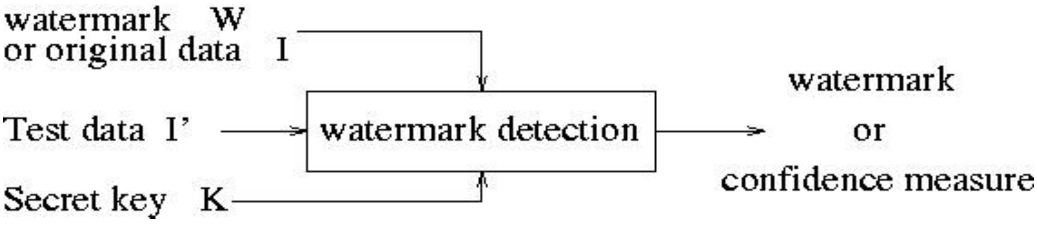


Figure 2.5 Watermark recovery scheme

3. APPLICATION OF WATERMARKING

A popular application of watermarking techniques is to provide a proof of ownership of digital data by embedding copyright statements into video or image digital products.Automatic monitoring and tracking of copy-write material on WEB. (For example, a robot searches the Web for marked material and thereby identifies potential illegal issues.). Automatic audit of radio transmissions: (A robot can “listen” to a radio station and look for marks, which indicate that a particular piece of music, or advertisement, has been broadcast.). Data augmentation to add information for the benefit of the public. Fingerprinting applications (in order to distinguish distributed data). Actually, watermarking has recently emerged as the leading technology to solve the above very important problems.All kind of data can be watermarked: audio, images, video, formatted text, 3D models, model animation parameters.

4. CONCLUSION

Watermarking technology plays an important role in securing the document owner. Some of most salient of watermarking features are perceptually invisiblundeletable by hackers robust to lossy data compression and robust to image manipulation and processing operations. To hide private, sensitive data in a cover, the data is embedded either in its original raw format or is encrypted first. Since the amount of data to be hidden may be large, the data is compressed before encryption or embedding. This enables several parties to exchange without communicating directly. The watermark is normally a small amount of data that indicates ownership, authorship, or another kind of relationship between the cover and a person or an organization. Fingerprinting is a variant of watermarking, where many copies of the same product have to be tagged. When a fingerprint is hidden in a music CD, any illegal copies discovered and seized can be traced back to original from which they were made.

REFERENCE:

[[1] Krzysztof Szczypiorski (4 November 2003). "Steganography in TCP/IP Networks. State of the Art and a Proposal of a New System - HICCUPS". Institute of TelecommunicationsSeminar http://www.tele.pw.edu.pl/~krzysiek/pdf/steg-seminar-2003.pdf. Retrieved 17 June 2010.

[2] Craig Rowland (May 1997). "Covert Channels in the TCP/IP Suite".FirstMondayJournal.http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/issue/view/80. Retrieved 16 June 2010

[3] Wojciech Mazurczyk and Krzyszt of Szczypiorski (November 2008). "Steganography of VoIP Streams". Lecture Notes in Computer Science (LNCS) 5332, Springer-Verlag Berlin Heidelberg, Proc. of The 3rd International Symposium on Information Security (IS'08), Monterrey,

[4] Bartosz Jankowski, Wojciech Mazurczyk and Krzysztof Szczypiorski (11 May 2010). "Information Hiding Using Improper Frame Padding". arXiv:1005.1925.

[5] Krzysztof Szczypiorski (October 2003). "HICCUPS: Hidden Communication System for Corrupted Networks". In Proc. of: The Tenth International Multi-Conference on Advanced Computer SystemsACS'2003,pp.31-40. http://krzysiek.tele.pw.edu.pl/pdf/acs2003-hiccups.pdf. Retrieved 11 February 2010.

[6] Asad,M., "Text Steganography Using Huffman Coding", ICIIT 2010, Page(s): 445-447.

[7] B.r., Roshan Shetty; J., Rohith; V., Mukund; Honwade, Rohan; Rangaswamy, Shanta (2009). Steganography Using Sudoku Puzzle. pp.623–626,doi:10.1109/ARTCom.2009.116.

[8] http://en.wikipedia.org/wiki/Printer_steganography

[9]Petitcolas, FAP; Anderson RJ; Kuhn MG (1999)."Information Hiding: A survey". Proceedings of the IEEE (special issue)87 (7):1062–78.doi:10.1109/5.771065. http://www.cl.cam.ac.uk/~fapp2/publications/ieee99-infohiding.pdf. Retrieved 2008-09-02.

[10]"British Muslim 'had Al Qaeda contacts book with terrorists' numbers written in invisible ink'". Daily Mail (London). 24 September,2008.http://www.dailymail.co.uk/news/article-1061190/British-Muslim-Al-Qaeda-contacts-book-terrorists-numbers-written-invisible-ink.html.

[11]Herodotus, The Hisories, chap. 5 - The fifth book entitled Terpsichore, 7 - The seventh book entitled Polymnia, J. M. Dent & Sons, Ltd, 1992.`

[12]Second Lieutenant J. Caldwell, Steganography, United States AirForce, ttp://www.stsc.hill.af.mil/crosstalk/2003/06/caldwell.pdf, June 2003.

[13]F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, “Information Hiding - A Survey”, Proceedings of the IEEE, vol. 87, no. 7, pp. 1062-1078, July 1999.