International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064

A Survey of Digital Watermarking Techniques and its Applications

Kusuma Kumari B. M[1]

[1]Tumkur University, University College o Science, B.H Road, Tumkur 572103, Karnataka, India

Abstract: ***Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, and video) within the signal itself. Watermarking tries to hide a message related to the actual content of the digital signal. Digital watermarking is a technology being developed to ensure and facilitate data authentication, security and copyright protection of digital media. The purpose of digital watermarks is to provide copyright protection for intellectual property that is in digital format. This paper incorporate the detail survey about watermarking, it starts with overview, classification, features, techniques, application, challenges, and limitations of watermarking.***

Keywords: watermarking,techniques,requirements,properties, challenges

1. Introduction

A digital watermark is an identification code, permanently embedded into digital data, carrying information on copyright protection and data authentication.

The term digital watermarking was first appeared in 1993, when Tirkel presented two watermarking techniques to hide the watermark data in the images [1].

The enormous popularity of the World Wide Web in the early 1990s demonstrated the commercial potential of offering multimedia resources through the digital networks. Since commercial interests seek to use the digital networks to offer digital media for profit, they have a strong interest in protecting their ownership rights. Digital watermarking has been proposed as one way to accomplish this.

A digital watermark is a digital signal or pattern inserted into a digital image. Since this signal or pattern is present in each unaltered copy of the original image, the digital watermark may also serve as a digital signature for the copies. A given watermark may be unique to each copy (e.g. to identify the intended recipient), or be common to multiple copies (e.g. to identify the document source). In either case, the watermarking of the document involves the transformation of the original into another form. This distinguishes digital watermarking from digital fingerprinting where the original file remains intact, but another file is created that "describes" the original file's content. For example, the checksum field for a disk sector would be a fingerprint of the preceding block of data. Similarly, hash algorithms produce fingerprint files.

Digital watermarking can also be contrasted with public-key encryption, which also transforms original files into another form. It is a common practice nowadays to encrypt digital documents so that they become un viewable without the decryption key. Unlike encryption, however, digital watermarking leaves the original image or file basically intact and recognizable. In addition, digital watermarks, as signatures, may not be validated without special software. Further, decrypted documents are free of any residual effects of encryption, whereas digital watermarks are designed to be persistent in viewing, printing, or subsequent re-transmission or dissemination.

When you submit your paper print it in two-column format, including figures and tables. In addition, designate one author as the “corresponding author”. This is the author to whom proofs of the paper will be sent. Proofs are sent to the corresponding author only.

2. Important Properties of Digital watermarking

Ideal properties of a digital watermark have been stated in many articles and papers [11][12][13].

- **Robustness:** The watermark should be reliably detectable after alterations to the marked documents [2]. Robustness means that it must be difficult (ideally impossible) to defeat a watermark without degrading the marked document severely—so severely that the document is no longer useful or has no (commercial) value. Maintaining the Integrity of the Specifications [9].

- **Imperceptibility or a low degree of obtrusiveness:** To preserve the quality of the marked document, the watermark should not noticeably distort the original document. Ideally, the original and marked documents should be perceptually identical.

- **Security:** Unauthorized parties should not be able to read or alter the watermark. Ideally, the watermark should not even be detectable by unauthorized parties.

- **Fast embedding and/or retrieval:** The speed of a watermark embedding algorithm is important for applications where documents are marked “on-the-fly” (i.e., when they are distributed). The large bandwidth necessary for video also requires fast embedding methods. However, since ownership disputes will likely take weeks or months to resolve, a watermark recovery algorithm may empha - 2 size reliable detection over speed.

- **No reference to original document:** For some applications, it is necessary to recover the watermark without requiring the original, unmarked document (which would otherwise be stored in a secure archive).

- **Multiple watermarks:** It may also be desirable to embed multiple watermarks in a document. For example, an image might be marked with a unique watermark each time it is downloaded.

- **Unambiguity:** A watermark must convey unambiguous information about the rightful owner of a copyright, point of distribution, etc.

3. The Purpose of Digital Watermarking

The two types of digital watermarks are distinguished by their visibility to the casual viewer. Visible watermarks 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. This is done to mark the paper manufacturer or paper type. One might view digitally watermarked documents and images as digitally "stamped".

Invisible watermarks, 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. For this purpose, the objective is to permanently and unalterably mark the image so that the credit or assignment is beyond dispute. In the event of illicit usage, the watermark would facilitate the claim of ownership, the receipt of copyright revenues, or the success of prosecution.

Watermarking has also been proposed to trace images in the event of their illicit redistribution. Whereas past infringement with copyrighted documents was often limited by the unfeasibility of large-scale photocopying and distribution, modern digital networks make large-scale dissemination simple and inexpensive. Digital watermarking makes it possible to uniquely mark each image for every buyer. If that buyer then makes an illicit copy, the illicit duplication may be convincingly demonstrated.

3.1 Visible versus invisible 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. The main advantage of visible watermarks, in principle at least, 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 translucent 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.

Figure 1: Shows Example of Visible and Invisible Water marking

4. Requirements of Digital Watermarks

To be effective in the protection of the ownership of intellectual property, the invisibly watermarked document should satisfy several criteria:

The watermark must be difficult or impossible to remove, at least without visibly degrading the original image.

The watermark must survive image modifications that are common to typical image-processing applications (e.g. scaling, color requantization, dithering, cropping and image compression)

An invisible watermark should be imperceptible so that the view of the image is unaffected.

For some invisible watermarking applications, watermarks should be readily detectable by the proper authorities, even if imperceptible to the average observer [3]. Such decidability without requiring the original, un-watermarked image would be necessary for efficient recovery of property and subsequent prosecution.

One can understand the challenge of researchers in this field since the above requirements are stringent and sometimes clash with one another. The litmus test of a watermarking method would be that it is accepted and used on a large, commercial scale, and that it stands up in a court of law. None of the digital techniques have yet to meet these tests.

5. Techniques for Watermarking

Watermarking techniques tend to divide into two categories, text and image, according to the type of document to be watermarked [4].

Several different methods enable watermarking in the spatial domain [10]. The simplest (too simple for many applications) is to just flip the lowest-order bit of chosen pixels in a grey scale or color 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 (large or small, respectively) of the watermark intensity. One disadvantage of spatial domain watermarks is that picture cropping (a common operation of image editors) can be used to eliminate the watermark.

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

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.

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 code words. For word-shift coding, the spacing between words in a line of justified text is altered. For character coding, a feature such as the end line 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.

6. Digital Watermarking Applications

Copyright protection: Digital watermarking can be used to identify and protect copyright ownership. Digital content can be embedded with watermarks depicting metadata identifying the copyright owners.

Copy protection: Digital content can be watermarked to indicate that the digital content cannot be illegally replicated. Devices capable of replication can then detect such watermarks and prevent unauthorized replication of the content.

Digital right management: Digital right management (DRM) can be defined as ―the description, identification, trading, protecting, monitoring, and tracking of all forms of usages over tangible and intangible assets‖. It concerns the management of digital rights and the enforcement of rights digitally.

Tamper proofing: Digital watermarks which are fragile in nature, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content.

Broadcast monitoring: Over the last few years, the number of television and radio channels delivering content has notably expanded. And the amount of content flowing through these media vehicles continues to grow exponentially. In this highly fragmented and fast changing market, knowing the real broadcast reality has become critical for content owners, copyright holders, distributors and broadcasters.

Fingerprinting: Fingerprints are the characteristics of an object that tend to distinguish it from other small objects. As in the applications of copyright protection, the watermark for finger printing is used to trace authorized users who violate the license agreement and distribute the copyrighted material illegally. Thus, the information embedded in the content is usually about the customer such as customer's identification number.

Access control: Different payment entitles the users to have different privilege (play/copy control) on the object. It is desirable in some systems to have a copy and usage control mechanism to prevent illegal copy of the content or limit the number of times of copying. A robust watermark can be used for such purpose.

Medical application: Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster [5].

Image and content authentication: In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences. A solution to this problem could be borrowed from cryptography, where digital signature has been studied as a message authentication method. One example of digital signature technology being used for image authentication is the trustworthy digital camera [6].

Annotation and privacy control: Multi-bit watermarking can be used to annotate an image. For example, patient records and imaging details related to a medical image can be carefully inserted into the image. This would not only reduce storage space but also provides a tight link between the image and its details. Patient privacy is simply controlled by not keeping the sensitive information as clear text in human readable form, and the watermark can be further secured by encryption. Other usages of annotation watermarking are electronic `document indexing and automated information retrieval.

Media forensics: Forensic watermark applications enhance a content owner's ability to detect and respond to misuse of

its assets. Forensic watermarking is used not only to gather evidence for criminal proceedings, but also to enforce contractual usage agreements between a content owner and the people or companies with which it shares its content.

Communication enhancement: Today's smart phones are becoming the handheld computing device we carry with us 24/7 — no longer are they merely for talking or texting. More and more we look to our mobile phones to provide us with assistance, instant information, and to entertain us.

Content protection for audio and video content*:* Modern digital formats employed for sale or rental of commercial audio and video content to consumers-such as DVD, Blu-Ray Disc, and iTunes-incorporate content protection technologies that control access to and use of the content and limit its unauthorized copying and redistribution. Parties seeking to engage in unauthorized distribution and copying of protected commercial music or video content must circumvent the content protection to obtain a decrypted copy of the content.

Content filtering: The lean-back experience of watching television has radically changed over the last few years. Today people want to watch content in their own time and place. The proliferation of set top boxes (STB) in homes evidences this, as people want to watch video on demand or on a time-shifted schedule. Today, more than a device to watch films/series, sports or even play games, the STB has become an interactive device providing multiple services.

7. Disadvantages of Digital Watermarking

Watermarks keep people from stealing photographs or illustrations from websites, online auctions and image hosts [7]. They add copyright protection and can encourage interested parties to purchase the image instead of using it with an assumption that your labour is free. Increase the odds of making money off a photograph or illustration with watermarks that help a potential buyer identify who owns the image, but don't forget to consider the disadvantages of using watermarks before you make the decision to add them to our work.

- **Obscures Image** Worthwhile watermarks need to obscure the image just enough to make it unusable. Key areas of the illustration or photograph may end up hidden. Unless your photograph or illustration features strong color and composition, your image's appeal may suffer after the addition of a watermark as key areas are hidden beneath the watermark. Good watermarks protect the image without obscuring its appeal: they're often faint but visible enough to be intimidating.
- **Easy to Remove** Over-sized watermarks cover larger areas of an image and obscure the image's clarity. Small watermarks, on the other hand, can easily be removed with the assistance of image-editing software. To overcome these disadvantages, some people place mid-sized watermarks in places where the watermark covers nothing but an irrelevant area of an image, such as on a white background near a bottom corner. Unfortunately, this solution can't beat the thieves who will simply crop out the watermark. Great watermarks have intricate but faint detail that span a large portion of the image. Such watermarks are the hardest to remove.
- **Limited Protection** Professional watermarking services provide invisible but limited digital protection. Advanced watermarking technology that embeds ownership information into photographs or illustrations enable the use of search services to help you find incidents of unlawful use of your images. Unfortunately, professional watermarking search services may not be able to find images when they sit behind firewalls, in Flash-enabled galleries, and database-driven or password-protected websites.
- **Time Consuming** Adding watermarks to your work can be time consuming. If you are already selling large volumes of images, consider if watermarking is worth the time it takes to add them to all of your images. Unless you integrate watermarking into your work-flow, manually adding watermarks to hundreds of images may rob you of valuable time. Automating the watermarking process with a dedicated application may be worth spending money on, especially if you plan to produce, watermark and display lots of images.

8. Challenges and Limitations of Digital Watermarking

There are various technical challenges in watermarking research. The robustness and imperceptibility trade-off makes the research quite interesting. To attain imperceptibility, the watermark should be added to the high frequency components of the original signal. On the other hand, for robustness the watermark can be added to the low frequency components only. Thus, the watermarking scheme can be successful if the low frequency components of the original signal are used as the host for watermark insertion. In this section, we discuss the various technical issues related to watermarking, such as properties of the human visual system and spread-spectrum communication, which are commonly exploited for making watermarking schemes successful [8].

9. Conclusion

Digital Watermarking provides for the protection of intellectual property in the digital world. Just as plagiarism runs loose in the real world, unauthorized copying of data, whether it is audio, visual, or video, exists in the cyber world and is accomplished with the click of a mouse. Digital Watermarking attempts to copyright the digital data that is freely available on the World Wide Web to protect the originator's rights. In this paper I have presented various aspects for digital watermarking like overview, techniques, applications, purpose and properties. Apart from it a brief and comparative analysis of watermarking techniques is presented with their advantages and disadvantages.

References

[1] R.G. Schyndel, A. Tirkel, and C.F Osborne, ―A Digital Watermark‖, Proceedings of IEEE International

conference on Image Processing, ICIP-1994, pp. 86-90, 1994.
[2] C.S. Lu, Multimedia Security: Steganography and Digital Watermarking for Protection of Intellectual
[3] C.-T. Li and F.M. Yang., ―One-dimensional Neighborhood Forming Strategy for Fragile Watermarking‖. In Journal of Electronic Imaging, vol. 12, no. 2, pp. 284-291, 2003.
[4] Jiang Xuehua, ―Digital Watermarking and Its Application in Image Copyright Protection‖, 2010 International Conference on Intelligent Computation Technology and Automation.
[5] G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE'‖A Review of digital image watermarking in health care‖.
[6] Edin Muharemagic and Borko Furht ―A Survey of watermarking techniques and applications‖ 2001.
[7] http://www.ehow.com/info_11403254_disadvantages-watermark.html
[8] Manpreet kaur, Sonia Jindal, Sunny behal, ―A Study of Digital image watermarking‖, Volume2, Issue 2, Feb 2012.
[9] http://www.cl.cam.ac.uk/~fapp2/publications/ih98-attacks.pdf
[10] Avani Bhatia, Mrs. Raj Kumari U.I.E.T, Panjab University: "Digital Watermarking Techniques".
[11] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, vol. 6,no. 12, pp. 1673-1687, Dec. 1997.
[12] M. Swanson, B. Zhu, and A. Tewfik, "Transparent Robust Image Watermarking," Proc. IEEE Int. Conf. on Image Processing, Sept. 1996, vol. III, pp. 211-214.
[13] 3. I. Pitas, "A Method for Signature Casting on Digital Images*," Proc. IEEE Int. Conf. on Image Processing*, Sept. 1996, vol. III, pp. 215-218.

Author Profile

Kusuma Kumari B.M received the M.C.A. degree in Computer Science from University of Mysore, Karnataka, India in 2006 and M.Phil from Vinaya Mission University, Salem, India in 2009. She is currently pursuing PhD at Tumkur University. 7 Years of teaching experience and working as an Assistant Professor, Department of Computer Science in Tumkur University Tumkur, Karnataka, India.