Watermarking Technologies for Copyright Protection

Zoran Bojković, Andreja Samčović

Abstract – **The revolution in digital technology has increased the ease of manipulation, reproduction, retransmission and distribution of digital images. However, it also offers the potential for illegal use, known as a piracy of digital images. Watermarking techology is considered as a tool for protecting these intellectual properties. It attempts to identify the true owner by hiding perceptually invisible information (watermark) inside the digital data. In this paper, some digital watermark techniques are described**.

I. INTRODUCTION

According to the development and growth of the communication technology and network systems, for example the extensive utilization in a networked environment such as World Wide Web (WWW), information can be reliably distributed everywhere over the world. This information, which includes text, still images, audio, video and multimedia, is generally produced, stored and transmitted in the digital format since it provides more advantages than previously proliferated analog type. Digital representation of media facilitates access and potentially improves the portability, efficiency and accuracy of the information presented. Moreover, the reproduction or retransmission of digital media is not only exactly the same (noiseless channel) as the original, but its performance is also very fast and inexpensive [1]. Unfortunately, there are some serious problems about the use of digital technique. Because of its easy reproduction, retransmission and even manipulation, it allows a person (a pirate or organization) who tries to defraud by illegally claiming exploitation rights of the information (digital media), to violate the copyright of the real owner. This fraud includes illegal access to transmitted data in networks, data content modification, reproduction and retransmission without authorization of the owner. The effort to protect the intellectual property rights of digital media has been broadly localized. In particular, the development of reliable and robust schemes for protecting digital media from piracy is significantly required to enhance the rapid evolution and use of digital technology. Many media urgently need to be protected, for example digital versatile disk (DVD), audio compact disc (CD), the audio based on MPEG-1 layer-3 (MP3) standard, and so on. Currently, as shown in Fig.1, there are basically three approaches designed for protecting the intellectual property and securing the system. These are data encryption (criptography), authorization verification (using a signature or password to access the system) and watermarking strategies.

Zoran Bojković, Andreja Samčović
Faculty for Traffic and Transport Engineering
Vojvode Stepe 305, 11040 Belgrade

Based on conventional cryptographic systems, details of the data may be protected from an unauthorized person by applying the published cryptographic algorithms. Only a person who possesses appropriate key (or keys) can decrypt the encrypted data. The weakness of this data protection strategy is that once such data is decrypted, there is no way to protect and track its reproduction, manipulation and retransmission. Also it is impossible to legally prove the rightful ownership. The second strategy for protecting the intellectual property is an authorized verification system. The third approach to protect the intellectual property is watermarking. The basic concept of watermarking strategy is to directly cast an ideally undeletable watermark or a unique signature within the digital media, rather than to encode into a header or wrapper so that information remains intact across varying data file formats. Based on this strategy, the signature used for proving the authentication will be permanently affixed with the information (digital data) and can extensively fulfill the requirements of copyright protection.

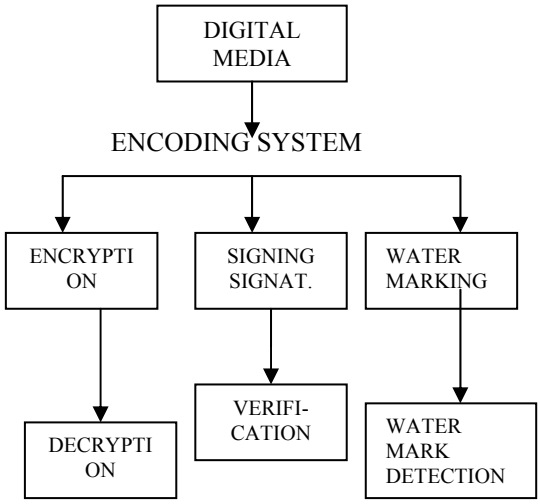

Fig.1 Representation of general digital data security system

Visible copyright mark and digital watermarking are described after the introduction. The third part of the paper takes into account existing invisible watermarking algorithms. One approach on the strength of watermark is given in the fourth part, while the approach on watermark embedding domain is in the fifth part. Finally, watermarking schemes based on image dependency and Human Visual System are presented.

II. VISIBLE COPYRIGHT MARK AND DIGITAL WATERMARKING

The developments in digital watermarking are remarkably expanding due to the urgent need for a variety of intellectual properties and copyright protection schemes. Digital watermarks can be divided based on their visibility or invisibility, that is, a perceptible (visible) mark or an imperciptible (invisible) mark [2]. Perceptible watermark, known as a logo or trademark of an organization, is specially designed and written (overlaid) on the product for identifyingthe copyright owner. It is simple to insert a visible seal placed over an image. The visible watermark works as a sign announcing an alarm system used to warn and deter anyone who may illegally use the product without respecting the ownership. However, a visible watermark is limited in many ways. It degrades the image fidelity and is susceptible to attack through direct image processing. Because of its perceptual property, the size and location of the visible watermark, the attacker has an exactly visible target and can easily remove the watermark without distorting the important and relevant characteristics of the product.

On the other hand, an imperciptible watermark has advantages over visible watermark, in that its location is not shown. It is an invisible, or preferably invisible, identification code that is permanently embedded in the digital media. The attacker cannot easily remove the watermark. This watermarking scheme is considered as an effective tool for providing the copyright protection. More information about visible and invisible watermarks is provided in Table I.

Table I. Characteristics of visible and invisible watermarks

	OBJECTIVE	VISIBLE WATER MARK	INVISIBLE WATER MARK
1	IDENTIFICATION OF SOURCE	X	
2	VERIFICATION OF AUTHENTICATION		X
3	DETERRENCE AGAINST PIRACY	X	X
4	DISCOURAGE DATA REPRODUCTION	X	
5	VALIDATION OF INTENDED RECIPIENT		X

III. REVIEW OF THE EXISTING INVISIBLE WATERMARKING ALGORITHMS

Various imperceptible watermarking techniques have been proposed over the years, mainly seeking intelligent multipurpose data hiding tools for the commercial digital media such as text, audio, color and gray-scale images, video and multimedia services. These digital watermarking techniques are called as information hiding, hidden information, data hiding, invisible communication, electronic watermarking, copyright label or labeling, digital signature, steganography, and invisible watermark methods [3].

Generally speaking, imperceptible watermarking algorithms are divided into three parts, watermark generation process (WGP), watermark embedding process (WEP), and watermark detection process (WDP). In watermarking generation process, the signal intended to be embedded into the host image can be both a meaningful signal (a logo, fingerprint, etc.) and a meaningless (pseudo-random sequence) signal depending on its purpose. However, the presence of any pattern, such as logo, among elements of the watermark sequence will likely make it visible (it is easy to predict), since pattern recognition is one of the most dominant characteristics of Human Visual System (HVS). Certainly, if some parameters of watermark sequence can be predicted, then such watermark can be easily removed by a watermarking attacker (pirate). Therefore, the unpredictability of the parameters of the sequence is required to make the watermark more robust, and is its first line of defense against watermarking attack. The secure watermark sequence may consist of a pseudo-noise signal sequence and each element value in the sequence must vary randomly from its neighbors. Examples of different pseudo random sequences are binary pseudo-noise, zero mean unit variance Gaussian random-noise, bounded normal distributed random sequence, and so forth. The most secure sequences of random values are those generated by strong cryptographic methods.

The heart of watermarking scheme is in watermark embedding process (WEP). To embed the watermark in the original (host) image, it is required to consider the significant features such as imperceptability of the watermark. A good embedding process should provide a non-objectionable degradation in the host image. In addition, robustness to the intended and unintended attacks, which possibly can occur after the owner has published the image, is also essential. This process influences and predetermines the performance of the next process, watermark detection. Most of the recently proposed algorithms use the concepts of spread spectrum technique which provides the ability to hide a significant quantity of information bits within the digital image while avoiding detection by an observer or by computer analysis.

The last process is watermark detection process or the owner verification procedure. This is the most important step in the watermarking strategy. The reliability of such a watermark scheme depends on how much of the embedded watermark signal can be detected. An ideal watermarking scheme should perfectly detect its watermark, with owner's approval (the probability of incorrect detection such as false positive and false negative must be reduced to an acceptable range). It is interesting to note that there are two different approaches for watermark detection process depending on the application. These are, the detection process using the original image (non-blind) and the detection process without using the original image (blind).

So far, many image based watermarking schemes, which particularly concentrate on each of these watermark processes, have been introduced as well as different categories to classify the watermarking schemes. Consequently, we rearrange and classify the proposed watermark algorithms into

several approaches such as watermarking schemes based on: the strength of its structure, watermark embedding domain, exploitation of Human Visual System (HVS), invertibility, resistance to attacks, and the availability of original source.

IV. THE APPROACH ON THE STRENGTH OF WATERMARK

The invisible watermark embedded into the image can be divided into a fragile watermark and a robust watermark. Fragile watermark scheme is generally desired such that the watermark is sensitive to image content manipulation through many sorts of image processing algorithms and geometric distortion operations. If such a watermarked image is altered, the watermark may change or disappear. For the application such as tamper detection in the image, fragile watermarking techniques enable us to distinguish malicious changes of data content, such as replacing/adding features from the original image. Therefore, the common desired properties of fragile watermark: It can be altered by application of most common image processing techniques. It is difficult for an unauthorized person to insert another fake watermark. It can survive image cropping and affine transform. The extracted watermark should indicate where the alteration has taken place.

On the other hand, in the case of robust scheme, watermark has opposing technical properties. The watermark must remain in a watermarked image, even after it has been processed by image processing and geometric distortion operations, including reformatting a watermarked image such as print, scan and photocopy.

V. THE APPROACH ON WATERMARK EMBEDDING DOMAIN

Even though the watermark embedding algorithms can be globally separated into two categories: embedding by modifying pixel's intensities, and embedding by modifying some of the geometric features, at present research seems to favor the former approach. According to the objectives of watermark embedding process, a noise-like signal is embedded into the original image by slightly changing some pixel's intensities. This provides a very high potential in the watermark embedding performance. Watermark embedding algorithms generally can be divided based on the embedding domain into a) spatial domain, b) transform domain.

Watermark embedded in spatial domain: the spatial domain based watermarking schemes involve the insertion of digital watermark by slightly modifying the pixel intensity of the color or monochrome image. For example, it can be done by modifying the Least Significant Bit (LSB). These schemes satisfy the desirable properties of digital watermark such as undetectability and accurate recovery. Moreover, since it relies on modifications of the LSB, the schemes typically achieve both high payload (the length/amount of watermark sequence being embedded) and low perceptibility. While the concept of LSB algorithm is basically sound, these algorithms may be vulnerable to common signal processing attacks such as lowpass filtering, noise addition, redigilization, and also compression standards such as JPEG (Joint Photographic Experts Group), and MPEG (Moving Picture Experts Group).

Entitled patchwork is another example for watermarking scheme based on spatial domain. The insertion of watermark in a patchwork is performed by altering the statistics of the original image. The modification is typically small and is not perceptible to the human vision, but is not necessarily restricted to the LSB.

Watermark Embedding in Transform Domain: Directly adding a noise-like watermark signal to the image content makes the spatial domain based watermarking schemes excellent in terms of imperceptibility, but vulnerable to the noise removal process such as filtering and even image compression. To improve the robustness of the watermarking algorithms, number of techniques based on several transforms such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) have been applied.

It is known that the DWT image/video coding, for example Embedded Zero-tree Wavelet (EZW), Zero-Tree Entropy (ZTE) coding, Set Partitioning in Hierarchical Trees (SPIHT) coding, and Multithreshold Wavelet Codec (MTWC), has been adapted in the latest image/video compression standards, such as JPEG 2000 and MPEG-4. DWT based codec has an excellent performance over the DCT, especially in low bitrate environment. Number of algorithms based on watermarking methods in the wavelet transform domain have been proposed. For example, there is a method based on adding a pseudo random-noise sequence to the large coefficients in the high frequency bands of Embedded Zero-tree Wavelet (EZW) based coder. The large coefficents in high frequency bands, such as HH, HL, and LH subbands (Fig. 2) usually indicate edges in an image. Therefore, adding high energy of watermark signal into these large coefficents makes it difficult for the perception by human eyes and also is hard to remove. Experimentally, these algorithms also show robustness against very high compression ratios. Furthermore, in some applications, it is required to embed watermark into only a certain portion of an image (which is called Region of Interest – ROI). By using spatial-frequency characteristics of DWT, some techniques introduce the novel ROI approach watermark algorithm that inserts the watermark into perceptually significant pixels chosen by the MTWC algorithm.

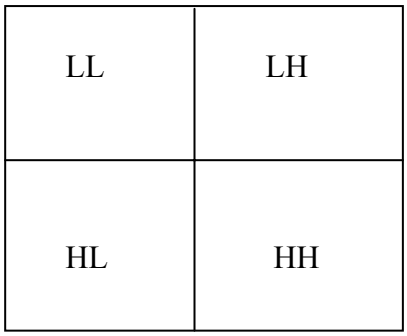

Fig.2 Structure of wavelet decomposition

During the watermark detection process, synchronization of the watermark signal is of the most importance. There is a tradeoff between using a full invariant representation, which may be numerically unstable, and the expensive computation to carry out a search.

VI. WATERMARKING SCHEMES BASED ON IMAGE DEPENDENCY AND HVS

Transparency is one of the most significant requirements of digital invisible watermarking schemes. However, the less energy of the watermark to be embedded, the more vulnerable it is to any kind of attacks. To compromise the tradeoff between robustness and invisibility in watermarking schemes, a strong watermark should be inserted in the insensitive areas of the image and vice versa [4].

Generally, HVS based techniques use explicit information about the HVS to exploit the limited dynamic range of human eye. The characteristics of HVS are exploited to adapt the watermark to the image being signed to improve the watermark invisibility and to enhance its robustness such that watermarks of larger energy content can be embedded. Because of the invisibility constraint of a watermark, the techniques have to use signals of relatively lower power than would othervise be necessary (Fig.3).

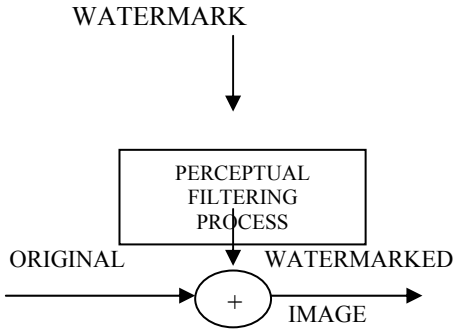

Fig.3 Image independent watermark embedding process

To improve the imperceptibility, a good watermarking technique (Fig.4) has to adapt to the particular image.

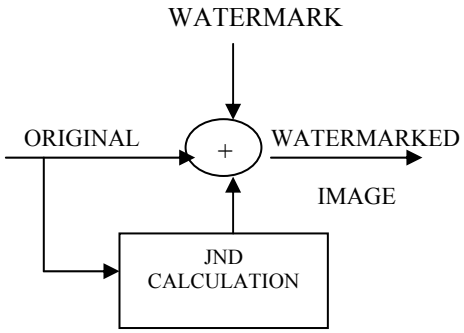

Fig.4 Image dependent watermark embedding process

Recently, visual models have been developed specifically for coding the image data to provide better compression [5]. Visual models derived for data compression are ideally suited for the digital watermarking scheme. One common paradigm for perceptual coding is based on deriving an image dependent mask containing the just noticeable differences (JND) which are used in compression applications to derive perceptually based quantizers and to determine perceptually based bit allocation. Such a model can be directly extended to the watermarking application by providing upper bounds on watermark intensity levels for every pixel of the image, which guarantees transparency while providing the robustness property.

VII. CONCLUSION

In view of the proliferation of digital images and the lack of ability for protecting the current security algorithms, new copyright protection techniques need to be explored. Watermarking is one of the new copyright protection algorithms that provide high potential in identifying the ownership of images. The concept is to hide a specific signature (watermark) in an image. Watermarking requires some special properties such as invisibility and unremovability from the embedding image.

REFERENCES

[1] B.Macq, J.J.Quisquater: “Cryptology for digital TV broadcasting”, Proc. IEEE, Vol.83, pp 944-957, June 1995.

[2] D.J.Fleet: “Embedding invisible information in color images”, Proc. IEEE ICIP’97, Vol.1, pp 532-535, Santa Barbara, CA, October 1997.

[3] G.Voyatzis, I.Pitas: “Digital image watermarking using mixing systems”, Computers&Graphics, Vol.22, pp 405-416, July 1998.

[4] S.W.Kim: “Image watermarking scheme using visual model and BN distribution”, Electronics Letters, Vol.35, pp 212-214, February 1999.

[5] K.R.Rao, Z.Bojković, D.Milovanović: “Multimedia communication systems: techniques, standards and networks”, Prentice-Hall, Upper Saddle River, NJ, 2002.