Asian Journal of Information Technology 5 (10): 1082-1087, 2006

Digital Watermarking Techniques and Principles An Evolutionary Approach

[1]Ashish Bansal and [2]Sarita Singh Bhadauria
[1]Mahakal Institute of Technology Ujjain M.P., India
[2]Centre of Excellence Rajeev Gandhi, Technical University, Bhopal, India

Abstract: A digital watermark is used to insert an imperceptible signal into data which may be in the form of images, audio or video. This has applications in a variety of purposes like copyright control, authenticity, captioning etc. As the watermarks are subjected to wide range of applications, each requiring different sets of properties, a variety of important characteristics and properties of watermarks have been investigated. This study highlights the important properties of watermarks and also gives insight into various trends and approaches prevalent in this area.The study also conducts a literature survey focusing only on noteworthy work and techniques used for images during preliminary and principal development stage of digital watermarking by various researchers with the utility of giving a fundamental understanding of the basic principles of digital watermarking as it has evolved. This may serve as the concrete foundation and the base for understanding further advances in this technology in later years.

Key words: Watermarking, fidelity, multimedia security, digital media, secret communication, stegnography

INTRODUCTION

Data in the form of audio, video or images is represented and transmitted in the digital format. To provide the secrecy, confidentiality and authenticity of the data. Various encryption mechanisms have been proposed which provide data security while transmission. However, after the receipt and decryption, the data is no longer secured. Any number of copies may be reproduced illegally, which is a serious threat to the integrity and confidentiality of data. To overcome the above problem, digital watermarks are used. A digital watermark is a piece of information which is embedded in the digital media and hidden in the digital content in such a way that it is inseparable from the container data. This piece of information known as watermark, serves many applications listed below.

Authentification: Watermark is used to provide authentification. It may be designed in such a way that, any possible alteration in the container data either destroys the watermark or creates a mismatch between the content and the watermark that can easily be detected.

Copy control: Watermark may contain information required by the content owner that decided the policy of copying the digital content. The information contained by the watermark may specify 'content may not be copied' or 'only one copy' etc. Subsequently, the devices used for copying the content may be required by law to contain watermark detector, which follows directives given by the content owner[1,2].

Digital signatures: Watermarks may be used to identify the owner of the content. By having this information the user may contact the owner for acquiring the legal rights to copy or using the content[3].

Fingerprinting: Watermarks may be used to identify the content buyers. This may help in tracing illegal copies. When a digital media is distributed, it can contain the hidden and imperceptible information about the user, which can be detected by a watermark detector. Thus, a licensed copy belonging to a specific user can be ascertained. This also resolves the possible conflicts as regards to the ownership of a digital or intellectual property.This thing is referred to as "Fingerprinting".

Broadcast monitoring: Automatic identification of owners of data may be required to be done and used in systems responsible for monitoring the television and radio broadcasts. This may help in deciding the royalty payments. It also helps in ensuring that commercials of a particular advertiser are played at right time and for a right duration.

Corresponding Author: Ashish Bansal, Mahakal Institute of Technology Ujjain M.P. India

Secret communication: The technique of watermarking is also used in transmitting secretly information from source to destination in a hidden way. This method refers to Stegonography where the important or secret information may be hidden behind an image[4,5]. Several public domain and shareware programs are available which use watermarking for secret communication[6] .

GENERAL STRUCTURE AND FRAMEWORK

The general functioning of a typical watermark can be easily understood.

The original content (image, audio or video) is mixed with the encoded version of the watermark to produce a watermarked digital content at the sender's end. At the receiving end, a normal human being perceives the image and is unable to appreciate the presence of watermark. However, a watermark detector at the receiving end extracts the encoded watermark from the content and decodes it to obtain the original watermark. In the given following notations have been followed.

W = Watermark
SW = Watermarked image
S0 = Original information
S0′ = Perceived information at the receiving end.W- = Detected watermark information.

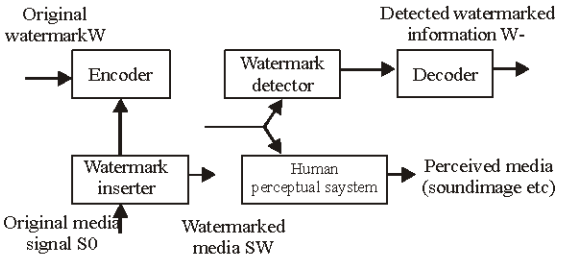

Fig. 1: Natations have been followed.

Thus the first step is to encode watermark bits into a form that will easily combine with the media data. For example in digital images, watermarks may be two dimension spatial patterns. This encoded information is then mixed with the original media content by means of watermark inserter. After insertion of the watermark also the resultant media looks similar to the original one using the peculiarities of the human visual system.Some techniques use the principle that in eight bit gray images, changes to the least significant bit can not be perceived by the human eye Turner[7]. The human visual system looks at only the other seven bits thus ignoring the watermark information so the fidelity of the image is maintained. Other techniques convert the digital image into corresponding frequency domain and mix the watermark information in the high frequency part of the image. Human eye can perceive only low frequency components significantly thus ignoring the higher frequency components which are used by the watermark.. This is similar to the principle used in lossy compression as proposed by author[8]. Methods using a single key are being employed but with different level of access and are termed 'restricted key' and 'unrestricted key' methods. No method using two different keys at sender and receiver is yet known in the area of watermarking.

PROPERTIES OF WATERMARKS

There are a number of important characteristics that watermarks exhibit. Some of the important ones are given below.

Fidelity: This refers to the term imperceptible as it is referred in the literature of watermarks. The watermark should not be identified by normal viewing at the receiving end. It should also not cause any kind of perceptible distortion or deviation in the original media content[9,10]. Either watermarks can be inserted into perceptually insignificant portions of the media, for example least significant bit or high frequency regions or they can also be kept in perceptually significant portions of the image using a new 'spread spectrum technique. The second method is mostly used when robustness is the important concern.

Robustness: The digital media content audio,video or digital image may undergo various kinds of distortions. Some of the common distortions are lossy compression, contrast enhancement, alteration of colors, modification of bass frequencies of audios, A/D or D/A conversions as well as standard geometric transformations like scaling, rotation, cropping etc. After such distortions, the watermarks should be still present in the data and it should be possible to detect these watermarks correctly[11]. Cox has proposed that watermarks exhibit robustness to deformations and distortions of an image if they are placed inside the visually significant portions of the digital content rather than insignificant portions[9,10].

Fragility: This is reverse of robustness. For specific applications where it is required that watermark in a text document should allow copying, but even if there is a small alteration in text, the watermark should be destroyed. Thus if not detected, it can be ascertained that something wrong has happened with the original text. The

watermarks may be designed to withstand various degrees of acceptable modifications in the watermarks on account of distortions in the media content. Here, watermark differs from a digital signature which requires a cent per cent match.

Tamper resistance: In addition to the normal signal distortions, the watermark should be resistant to distortions against the deliberate signal processing operations intended to remove the watermarks. A successful attack on a watermark system can damage or completely remove a watermark. Anticipation of such attacks and resistance against them comes in the category of tamper resistance.

Key restrictions: When the keys are freely available to all detectors, it falls in the category of 'unrestricted watermarks' and if the key is available to a small no of detectors it comes in the category of 'restricted watermarks'. Some watermarking methods create a unique key for each piece of data which is watermarked. Thus the owner of the data has to maintain a database of keys[12].

False positive rate: In many applications, it may be required to distinguish the watermarked data from the un watermarked data. The false positive rate of a watermark detection system is the probability that it will identify an un watermarked piece of data as containing a watermark..

Data payload: Data Payload of a watermark is the amount of information that it contains. If the watermark contains N bits,then there are 2^N possible watermarks. Actually, there are 2^N +1 possibilities because one possibility is that the watermark is not present.

Computational cost: The computational cost refers to the cost of inserting and detecting watermarks in digital media content. This is very important when watermarks need to be inserted or detected in real time video or audio. The speed requirements of inserting and detecting watermarks is highly application dependent. Another important consideration while considering computational cost is scalability.

WATERMARKING TECHNIQUE

Mathematically, if there is an original image S0 and a watermark W, the watermarked image, SW can be obtained by SW = SO + f (SO,W), such that the watermarked image SW is almost visually identical (near about similar) to the original unwatermarked image S0. In general, the function f can be arbitrary, but practically robustness requirements make f to be designed in a specific way. Even if a random noise is added to the original image, the watermark has to be robust. That means, even with a slightly different image say S0 + e, (e = small diff). The same watermarked image should be generated. mathematically as:

$$f(SO,W) = f(SO + e,W)$$

The detection of the watermark, W, is done by correlating the watermark with some function, "g" of the watermarked image.For example, in one of the methods, if in one half of the pixels, the luminance is increased by one unit step and the luminance is kept constant or reduced in the second half set of pixels[13], then detection by summing luminances in the first subset and subtracting the sum of luminances in the second subset is a special case of a correlator.This can be described as:

$$SW = SO + W, \text{ where } f(SO,W) = W$$

Here the detector finds the dot product, SW.W, where. denotes the scalar product of the two vectors. If W is chosen at random, then the distribution of S0.W will cancel out as positive and negative terms. However, W.W of all terms is positive.so we have SW.W = S0.W + W.W which is approximately equal to W.W only. Thus the watermark can be detected. The above technique is just one of the representative samples of a wide variety of methods available for detection of watermarks from a variety of applications. There are a number of common transformations that a watermark should survive. e.g. Affline transformations, compression, noise, geometrical transformations etc. which the generated watermark should be able to survive.Looking at the above requirements, various digital watermarking techniques have been proposed by many researchers from time to time. A brief overview of the contributions by different researchers in this area is given in the next section to follow.

NOTEWORTHY CONTRIBUTION BY VARIOUS RESEARCHERS

The following is only a comprehensive list of important contribution not guaranteeing the complete collection of various proposed methods of digital watermarking during initial research period in digital watermarking. Many watermarking methods have been proposed in the literature. Schyndel,Tirkel and Osborne generated a watermark using a m-sequence generator[14].

The watermark was either embedded or added to the least significant bit of the original image to produce the watermarked image. The watermark was extracted from a suspected image by taking the least significant bits at the proper locations. Detection was performed by a cross-correlation of the original and extracted watermark.. Schyndel *et al.* showed that the resulting image contained an invisible watermark with simple extraction procedures.

The watermark, however, was not robust to additive noise. Cox *et al.* noted that in order for a watermark to be robust to attack, it must be placed in perceptually significant areas of the image[15]. The watermark was based on 1000 random samples of a N(0,1) distribution. These samples were added to the 1000 largest DCT coefficients of the original image and the inverse DCT was taken to retrieve the watermarked image. For detection, the watermark was extracted from the DCT of a suspected image. Extraction was based on knowledge of the original signal and the exact frequency locations of the watermark.

The correlation coefficient was computed and set to a threshold. If the correlation was large enough, the watermark was detected. Their method was robust to image scaling, JPEG coding, dithering, cropping and rescanning.Xia, Boncelet and Arce proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT)[16].The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire, extracted watermark was correlated with the entire, original watermark. This technique proved to be more robust than the DCT method when embedded zero-tree wavelet compression and halftoning were performed on the watermarked images[15]. Improvements on the above schemes were possible by utilizing properties of the human visual system. Bartolini *et al.* first generated a watermarked image from DCT coefficients[17]. Then spatial masking was performed on the new image to hide the watermark.. Kundur and Hatzinakos embedded the watermark in the wavelet domain[12]. The strength of the watermark was determined by the contrast sensitivity of the original image. Both techniques showed resistance to common signal processing operations.Delaigle *et al.* proposed a unique watermarking scheme based on the human visual system. Binary m-sequences were generated and then modulated on a random carrier[13]. This image served as the watermark and then it was masked based upon the contrast between the original signal and the modulated image. The masked watermark was added to the original image to form the watermarked image. Their technique was robust to additive noise, JPEG coding and rescanning.Craver *et al.* noted that certain watermarking techniques were susceptible to counterfeit attacks[18]. They showed that the method proposed by Cox *et al.* could be attacked by creating a fake original image and fake watermark that is indistinguishable from the true original image and watermark. To prevent this scenario, they modified the Cox *et al.* algorithm by making the watermark dependent on the original image. This new scheme was less susceptible to counterfeiting and still maintained robustness. Bas, Chassery and Davoine introduced a watermarking system using fractal codes. A collage map was composed from 8x8 blocks of the original image and from the image's DCT[4]. The watermark was added to the collage map to produce a marked image.

Results showed that fractal coding in the DCT domain performed better than coding in the spatial domain. The DCT-based watermarking technique was robust to JPEG compression, while spatial fractal coding produced block artifacts after compression.A method for casting digital watermarks on images and analyzing its ectiveness was given by I.Pitas and immunity to subsampling was examined and simulation results were provided for the verification of the proposed theme[3]. R.J. Anderson and F.A.P. Petitcolos in his study described an approach to detect hidden messages in images that uses a wavelet-like decomposition to build higher-order statistical models of natural images. Support vector machines are then used to discriminate between untouched and adulterated images[2].

D. Kundur and D. Hatzinakos used wavelet-based image watermarking methods to exploit the frequency information and spatial information of the transformed data in multiple resolutions to gain robustness. Although the Human Visual System (HVS) model offers imperceptibility in wavelet-based watermarking, it suffers high computational cost[12]. I Cox and J.Kilan in his study presented a secure (tamper-resistant) algorithm for watermarking images and a methodology for digital watermarking that may be generalized to audio, video and multimedia data. They advocated that a watermark should be constructed as an independent and identically distributed (i.i.d.) Gaussian random vector that is imperceptibly inserted in a spread-spectrum-like fashion into the perceptually most significant spectral components of the data. They argued that insertion of a watermark under this regime makes the watermark robust to signal processing operations (such as lossy compression, filtering, digital-analog and analog-digital

conversion, requantization, etc.) and common geometric transformations (such as cropping, scaling, translation and rotation) provided that the original image is available and that it can be successfully registered against the transformed watermarked image[9]. We present an approach for still image watermarking in which the watermark embedding process employs multiresolution fusion techniques and incorporates a model of the human visual system (HVS). D. Kundur and D. Hatzinakos demonstrated that the original unmarked image is required to extract the watermark. Simulation results on this demonstrated the high robustness of the algorithm to such image degradations as JPEG compression, additive noise and linear filtering[12]. M. Swanson, B. Zhu and A. Tewfik proposed a watermarking scheme to hide copyright information in an image. The scheme employed visual masking to guarantee that the embedded watermark is invisible and to maximize the robustness of the hidden data. The watermark was constructed for arbitrary image blocks by filtering a pseudo-noise sequence (author id) with a filter that approximates the frequency masking characteristics of the visual system. The noise-like watermark was statistically invisible to deter unauthorized removal[11]. S. Craver, N Memon proposed digital watermarks as a means for copyright protection of multimedia data. They addressed the capability of invisible watermarking schemes to resolve copyright ownership. They showed that, in certain applications, rightful ownership cannot be resolved by current watermarking schemes alone. Specifically, we attack existing techniques by providing counterfeit watermarking schemes that can be performed on a watermarked image to allow multiple claims of rightful ownership.

In the absence of standardization and specific requirements imposed on watermarking procedures, anyone can claim ownership of any watermarked image. In order to protect against the counterfeiting techniques that we develop, they examined the properties necessary for resolving ownership via invisible watermarking. They introduced and studied invertibility and quasi-invertibility of invisible watermarking techniques. They proposed noninvertible watermarking schemes and subsequently gave examples of techniques that were nonquasi-invertible and hence invulnerable against more sophisticated attacks proposed in the study[1]. N.Jayant in his study suggested that digital watermarking consists of hiding subliminal information into digital media content, also called hostdata. It can be the basis of many applications, including security and media asset management. In this study, he focused on the imperceptibility requirement for image watermarking[8]. R.L. Rivest discovered the chaffing and winnowing paradigm for data privacy[6]. L. Marvel, C. Retter presented a new method of hiding information behind digital images called "spread spectrum image steganography". This method conceals a message of sufficient length within digital imagery while maintaining the original image size and dynamic length. The hidden messages can be removed using appropriate keys without any knowledge of the original image[5]. This marvelous work found applications in the areas like band captioning,hidden communication,image tamperproofing, authentification,invisible map overlays,embedded control and revision tracking.

CONCLUSION

In this study we have tried to describe the concept, basic principles, need, applications and characteristics of digital watermarks in the first stage. After this, we have also surveyed many of the earlier proposals for watermarking and attempted to identify their strengths and weaknesses and gradual improvements in short. Thus this study may serve as a ready reference for any new researcher willing to explore the basics and foundation works in the area of digital watermarking since its evolution to the point where it started gaining prominence in the area of digital media control. This study gives a base to understand the recent advances in digital watermarking which may have happened after the previous works described in this study but not covered in this study.

REFERENCES

1. Craver, S. and N. Memon, 1998. Resolving rightful ownership with invisible watermarking tech iques: Limitations, attacks and implications, IEEE Trans, pp: 573-586.
2. Anderson, R.J. and F.A.P. Petitcolos, 1998. On the limits of stegonography, IEEE Trans on Selected area of Communication, pp: 474-481.
3. Pitas, I., 1996. A Method for signature casting on digital images, Proc. IEEE Int. Conf. On Image Processing, pp: 215-218.
4. Bas, P., J. Chassery and F. Davoine, 1998. Using the Fractal Code to Watermark Images, Proc. IEEE Int. Conf. on Image Processing, pp: 469-473.
5. Marvel, L., C. Retter and C. Boncelet, 1998. Hiding Information in Images, Proc. IEEE Int. Conf. On Image Processing, pp: 396-398.
6. Rivest, R.L., 1998. Chaffing and winnowing: confidentiality without encryption http::theory. lcs.mit.edu/rivest/chaffing.txt,1998.
7. Turner, L.F., 1989. Digital data security system Patent IPN WO 89/08915.

8. Jayant, N., 1993. Signal compression based on models of human perception, Proc IEEE, pp: 81-10.
9. Cox, I., J. Kilan, 1996. Secure spread spectrum watermarking for images, audio and video, IEEE Intl. Conference on Image Processing, pp: 243-246.
10. Cox, J. and J. Kilian, 1174. A secure robust watermark for multimedia in Information hiding First Int. Workshop Proc, Of Lecture notes in Computer Science, pp: 185-206.
11. Swanson, M., B. Zhu and A. Tewfik, 1996. Transparent robust image watermarking, Proc. IEEE Int. Conf. on Image Processing, pp: 211-214.
12. Kundur, D. and D. Hatzinakos, 1997. A Robust digital image watermarking method using wavelet-based fusion, Proc. IEEE Int. Conf. on Image Processing, pp: 544-547.
13. Delaigle, J., C. De Vleeschouwer and B. Macq, 1998. Psychovisual approach to digital picture watermarking,, J. Electronic Imaging, pp: 628-640.
14. Schyndel, R., A. Tirkel and C. Osborne, 1994. A Digital Watermark, Proc. IEEE Int. Conf. Image Processing, pp: 86-90.
15. Cox, I., J. Kilian, F. Leighton and T. Shamoon, 1997. Secure spread spectrum watermarking for Multimedia, IEEE Transactions on Image Processing, pp: 1673-1687.
16. Xia, X., C. Boncelet and G. Arce, 1997. A Multiresolution Watermark for Digital Images, Proc. IEEE Int. Conf. on Image Processing, pp: 548-551.
17. Bartolini, F., M. Barni, V. Cappellini and A. Piva, 1998. Mask building for perceptuallyhiding frequency embedded watermarks, Proc. Int. Conf. on Image Processing, pp: 450-454.
18. Craver, S., N. Memon, B. Yeo and M. Yeung, 1998. Resolving Rightful Ownerships withInvisible Watermarking Techniques: Limitations, Attacks and Implications, IEEE J. Selected Areas in Communications, pp: 573-586.