REVIEW : TECHNIQUES AND APPLICATIONS IN DIGITAL WATERMARKING

Neha Singla,

Delhi

ABSTRACT

As the Internet expanded more and more, it enabled the frequent and easy sharing of digital data like audio, video, text and images. Issues like copyright violation, redistribution and illegal copying became more prevalent, and needed to be addressed. Digital watermarking is a technique which is being adopted to tackle the issues related to copyright protection, data security and authentication of digital media. These techniques can be applied to audio, video, images or plain text. This paper presents a detailed study of various digital watermarking techniques and applications.

Keywords: *Digital watermarking, Content protection, Digital properties.*

INTRODUCTION

Many new opportunities have emerged for the creation and delivery of digital content due to the unprecedented expansion of the Internet. Various important applications of the Internet dealing with digital data are digital libraries, electronic advertising, audio and video delivery in real time, and publishing content over the Internet. Data security is a very important issue to be considered in these applications. It has been observed that, for dealing with digital data, present copyright laws are not enough. The enforcement and protection of intellectual proprietary rights for digital content has become very important. There is more interest for developing deterrence for copying digital data and mechanisms for its protection. One such area is based on techniques of digital watermarking. Steganography pays major attention towards making the information invisible, whereas watermarking has most of its attributes paying attention to the robustness of the message and the ability to withstand attempts of removal, like various operations on images such as rotation, filtering, cropping, when images are watermarked. The process of embedding information(which we call the watermark) into digital content (images, audio, video etc) such that the information can be detected or extracted later, for different purposes like copying prevention and control, is called Digital Watermarking. Development of watermarking techniques and its commercialization is being considered essential to help address the various issues being faced by the rapid expansion and distribution of digital content over the Internet.

DIGITAL WATERMARKING

As we know cryptography and steganography are not the same though both have focus on providing secret communication. Cryptography protects the content of a secret message by hiding it from malicious people, whereas steganography conceals even the existence of the message. A new technology, digital watermarking, involves theories and ideas of

different subjects, like signal processing, probability theory and stochastic theory, cryptography and network technology, design of algorithms, and other techniques. Certain algorithms are applied in Digital Watermarking to hide the proprietary information into the digital data. The information to be embedded are often some text, a company logo or an author's serial number, or images of some special significance. The secret information is embedded in the digital data (audio, video and images) to ensure security, to provide data authentication, to enable identification of owner and protection of copyright of information. The watermark can be embedded in the digital data either invisibly or visibly. An efficient watermarking technique is required for a strong watermark embedding. Either spatial or frequency domain can be used to embed the watermark. These domains are entirely different and have their own applications in different scenarios.

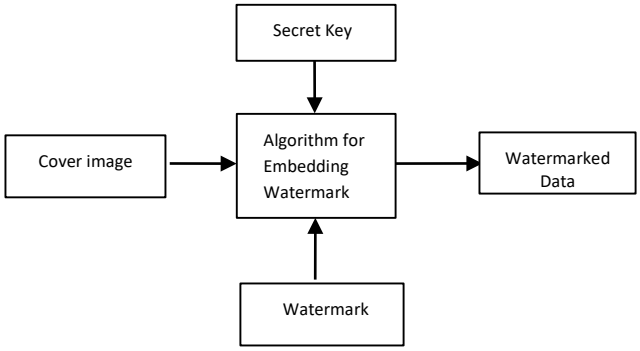

Fig. 1 Process of Watermark Embedding

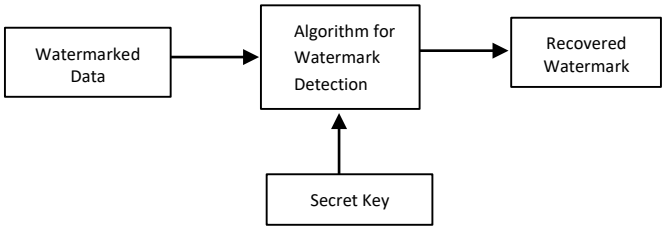

Fig 2. Process of Watermark Detection

APPLICATIONS

Some important and useful applications of Digital Watermarking are:

A. ***Broadcast Monitoring***

Advertisers want to make sure that they receive all of the purchased air time from broadcasters [5, 40]. The non technical method which involves human observation to watch the broadcast and check for originality by hearing or seeing is error prone and

costly. So, there should be some auto-identification system, which stores the identification codes of the broadcast. Several techniques like cryptography can be used, that save the identification code in the header of the file but the data does not survive any modifications, even format change. Digital Watermarking is an appropriate technique for information monitoring. Watermark is embedded in the digital content and is compatible with the installed broadcast equipment. Embedding the identification code is complicated ass compared to the techniques of cryptography where the code is simply placed in the file header. It also affects the visual quality of the data. Still, many companies prefer to protect and monitor their broadcasts by using watermarking techniques.

B. ***Ownership Assertion***

The watermark from digital content can be retrieved by the rightful owner to prove his ownership. Textual copyright notices have their limitations, because they are easily removable. It is not possible to copy the copyright notice printed on the physical document along with the digital content. It is possible to place that text copyright in an unnoticed or unimportant place of the document so that it becomes unobtrusive [41]. Inseparable and imperceptible watermarking is the better option as compared to text watermarking for owner identification. The watermark is used not only for copyright ownership identification but for proving the document ownership as well. The ownership can be confirmed by extracting embedded information from the digitally watermarked document [42].

C. ***Transaction Tracking***

Transaction tracking is, where each copy of the digital data is uniquely identified, just like the fingerprints that identify an individual. The embedded watermark can record the recipient for each authorized distribution of the work. Different watermarks are embedded by the owner in each copy. Visible watermarking is generally used for transaction tracking but invisible digital watermarking is better. For instance, in movie making, the daily videos are distributed to those who are concerned with the making. But sometimes, the videos are leaked to the press, therefore the studios use visible watermark text in the corner of the screen, which can identify the copy of the daily videos. Digital Watermark is preferred as text can be erased easily.

D. ***Content Authentication***

It is the procedure to verify the integrity of watermarked digital data and to ensure that the data is not tampered with – the act of confirming or establishing whether an image is authentic. The term authentication here has a range of meanings. Like, an authority that decides whether a portion of art is fabricated or authentic, authorizing whether the content of some object is intact or not after it has been transmitted on the internet. Many organizations invest money on new technologies for documenting images and constructing digital libraries. Many problems occur when these art works are digitized and published on internet. Usually the digital images that are found on the internet have various differences, and at the same time they pretend to represent the same art work. Use of watermarking for content authentication consists of trusted cameras, remote sensing and video surveillance applications, digital insurance claim evidence, journalistic photography, and management systems for digital rights. Commercially, with the growth of the applications of digital content, the applications of digital watermarking for content authentication are also expected to grow. The digital data can easily be tampered with, by using computer resources. One of the solutions for tamper detection is digital watermarking, in which the authentication mark (watermark) will be destroyed after even the slightest modification.

E. ***Copy Control***

Copy control prevents people from making unauthorized copies of the content. An owner can embed some serial number as watermark into the digital content which identifies the actual buyer of the copy. If unauthorized copies are recovered later,

the origin of illegal copies can be traced by the owner.

DIGITAL IMAGE WATERMARKING

Digital image watermarking has generated a lot of interest in the research community for two main reasons: one is the easy availability and the other is that it conveys sufficient redundant information which can be used for embedding watermarks [2]. The digital image watermarking techniques work in either transform domain or social domain. Spatial domain techniques involve working directly on pixels. It modifies the pixel values to embed the watermark. LSB is the most commonly used spatial domain technique. Transform domain techniques modify the transform domain coefficients to embed the watermark. DCT, DWT and DFT are the most commonly used transform domain techniques. For achieving the imperceptibility and robustness, the techniques of transform domain are more effective as compared to techniques of the spatial domain.

A. *Spatial domain watermarking techniques:*

The spatial domain means the image is represented in the form of pixels. The spatial domain watermarking techniques embed the digital watermark by changing the color and intensity value of some randomly selected pixels [3]. The strengths of spatial domain watermarking techniques are low computational complexity, simplicity and it is less time consuming. The computing speed of the spatial domain watermarking techniques is higher and these techniques are easier than transform domain but they are less robust against attacks. Any image may be watermarked using these techniques. The most important technique is called Least Significant Bit (LSB).

i) Least Significant Bit : It is the simplest watermarking technique where a watermark is embedded in the least significant bit of randomly selected pixels from the original cover image.

The steps used to embed watermark in the original image by using LSB [4]:

1) Convert RGB image into grey scale image.
2) Making double precision for image.
3) Shifting most significant bits to low significant bits of the watermark image.
4) Making least significant bits of the cover image as zero.
5) Adding shifted watermarked image to modified cover image.

The main advantage of this method being the ease with which this technique can be applied to images. It also provides high perceptual transparency. The image quality will not degrade when the watermark is embedded by using LSB technique. The main drawback of this technique is its low robustness to signal processing operations because watermark generated by this technique can be easily destroyed by any signal processing attack. It is not vulnerable to noise and attacks, although it is very much imperceptible.

Other algorithms for spatial domain watermarking are :

ii) *Additive Watermarking:* Here, a pseudo random noise pattern is added to the intensity values of image pixels to embed a watermark. The noise signal usually is integers like (-1, 0, 1) or floating point numbers sometimes. The noise is generated by a key to ensure the detection of the watermark, in a way that correlation between numbers of different keys is very low [5].

iii) *SSM Modulation Based Technique*: Methods in which energy at one or more frequencies is distributed or spread in time. An image is combined linearly with a pseudo noise signal by SSM based digital watermarking algorithms. This noise signal is then modulated by the embedded watermark.

iv) *Patchwork Algorithm:* Patchwork is a data hiding technique based on a pseudorandom, statistical model. The

Patchwork uses a Gaussian distribution to insert a watermark imperceptibly with a particular statistic. Two patches are selected pseudo-randomly. Image data of one patch is brightened and that of the other patch is darkened.

v) *Correlation-Based Technique*: IW(x, y) = I(x, y) + k*W(x, y). Here k represents the gain factor, IW represents the watermarked image and I and x, y represent the cover image. Increasing the gain factor increases the robustness of the digital watermark but decreases the quality of watermarked image.

B. *Frequency domain watermarking techniques:*

Frequency-domain techniques are more widely applied as compared to spatial-domain techniques. Their aim is to embed the watermark in the spectral coefficients of an image. The transform methods that are most commonly used are the Discrete Cosine Transform, Discrete Fourier Transform, and Discrete Wavelet Transform. The characteristics of human visual system are captured better by the spectral coefficients [7]. Some of the main algorithms are as discussed below:

i. ***Discrete cosine transforms (DCT):*** DCT represent data in frequency domain and not in the amplitude domain. This corresponds more to the way that light is being perceived by human eye, so that the part of image which is not being perceived is identified and deleted. These techniques are way more robust than the techniques in spatial domain. Such algorithms, though, are robust against image processing operations like blurring, brightness and contrast adjustment, low pass filtering etc. But, they are more difficult to implement and are computationally expensive. Also, they are weak against geometric operations like scaling, rotation, cropping etc. DCT watermarking is classified into Block Based DCT watermarking and Global DCT watermarking. Most compression algorithms remove the perceptually unimportant portion of the image and so, embedding a watermark in the perceptually important portion of the image has its own advantages.

Block Based DCT Watermarking Algorithm:

- The image is segmented into non-overlapping blocks of size 8x8.
- Each of these blocks is transformed using forward DCT.
- Some block selection criteria is applied (e.g. HVS)
- Applying coefficient selection criteria to select the coefficients that are to be modified for watermarking.
- Modifying the selected coefficients and embedding the watermark.
- Applying inverse DCT on each block.

ii. ***Discrete wavelet transforms (DWT):*** Wavelet Transform is a technique used in compression, digital image processing, watermarking etc. The transforms are based on small waves, called wavelets, of different frequencies and limited duration. The wavelet transform decomposes an image in three spatial directions, i.e. vertical, horizontal and diagonal. Wavelets reflect anisotropic properties of HVS more accurately. The magnitude of DWT coefficients is greater in the lowest band (LL) at each level and is smaller for rest of the bands (LH, HH, and HL). Discrete Wavelet Transform is presently used in many applications of signal processing which include video and audio compression, removal of noise from audio signal, and simulation of wireless antenna. Energy of Wavelets is concentrated in time and they are appropriate for the analysis of transient and time-varying signals. Most of the signals encountered in real time are time varying in nature, and hence the Wavelet Transform has many applications [9]. Achieving a better tradeoff between perceptivity and robustness is one of the major challenges of watermarking. By increasing the strength of embedded digital watermark, robustness can be achieved but it would increase the visible distortion as well [9]. DWT provides a simultaneous spatial localization and a spread of the watermark within the frequency domain of

the host image, and so is more preferred [10]. In discrete wavelet transform in image processing, the image is decomposed into sub-images that are multi-differentiated and are in different spatial domain and independent frequencies [11].

iii. ***Discrete Fourier transform (DFT):***

A continuous function is transformed into its frequency components by DFT techniques. It is robust against attacks like scaling, rotation and cropping, translation etc. DFT is invariant to translation. Phase representation of an image is affected by spatial shifts in the image and the magnitude representation remains unchanged. Also, the magnitude of the Fourier transform is not affected by the circular shifts in spatial domain.

DFT can be used to recover from geometric distortions, because it is not affected by rotation, scaling and translation (RST).

Comparison among different algorithms for watermarking [12][13]

Algorithm	**Advantages**	**Disadvantages**
LSB	1. Easy implementation. 2. Less degradation of image quality 3. Perceptual Transparency is high.	1. Robustness is less. 2. It is vulnerable to noise. 3. It is vulnerable to scaling and cropping.
Correlation	Increase in robustness can be achieved by increasing the gain factor.	High increase in gain factor leads to poorer image quality..
Patchwork	High robustness against majority of different attacks.	Information hiding is limited.
DCT	The visibility of the image does not get affected because the watermark is embedded in the middle frequencies. The watermark is robust against any kind of attack.	1. The invariance properties are destroyed by block wise DCT. 2. Quantization suppresses certain higher frequency components.
DWT	1. Better localization in time and spatial frequency domain. 2. Gives higher compression ratio which has relevance according to human vision.	1. Higher cost of computing, sometimes. 2. Compression time is longer. 3. Blur/Noise near edges of video or image frames

DFT	DFT is used to recover from distortions because it is invariant to rotation, scaling and translation.	1. Implementation is complex. 2. Higher cost of computing, sometimes.

CONCLUSION

Digital watermarking is an efficient technique to send data securely. Security is one of the major issues that are addressed when data travels over the internet. In this paper an overview of Watermarking is presented and various watermarking techniques are discussed briefly. Also, a comparative analysis of watermarking techniques is also presented.

REFERENCES

[1] Jiang Xuehua, —Digital Watermarking and Its Application in Image Copyright Protection‖, 2010 International Conference on Intelligent Computation Technology and Automation.

[2] V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN). [3] N. Chandrakar and J. Baggaa,"Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of computer Application Technology and Research, vol. 2, no. 2, (2013), pp. 126-130. [4] D. Mistry," Comparison of Digital Watermarking Methods" (IJCSE) International Journal on Computer Science and Engineering, vol. 02, no. 09, (2010), pp. 2805-2909.

[5] CHAPTER 2: LITERATURE REVIEW, Source: Internet

[6] http://ippr-practical.blogspot.in

[7] Manpreet kaur, Sonia Jindal, Sunny behal, —A Study of Digital image watermarking‖, Volume2, Issue 2, Feb 2012.

[8] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, —A Survey of Digital Image Watermarking Techniques‖, 2005 3rd IEEE International conference on Industrial Informatics (INDIN).

[9] Evelyn Brannock, Michael Weeks, Robert Harrison, Computer Science Department Georgia State University —Watermarking with Wavelets: Simplicity Leads to Robustness‖, Southeast on, IEEE, pages 587 – 592, 3-6 April 2008.

[10] G. Bouridane. A, M. K. Ibrahim, —Digital Image Watermarking Using Balanced Multi wavelets‖, IEEE Transaction on Signal Processing 54(4), (2006), pp. 1519-1536.

[11] Cox, I.J.; Miller, M.L.; Bloom, J.A., —Digital Watermarking,‖ Morgan Kaufmann, 2001.

[12] Jiang Xuehua, —Digital Watermarking and Its Application in Image Copyright Protection‖, 2010 International Conference on Intelligent Computation Technology and Automation.

[13] Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan, —A Novel Technique for Digital Image Watermarking in Spatial Domain‖, 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.