International Journal of Computer Applications Technology and Research
Volume 5–Issue 3, 147-150, 2016, ISSN:2319–8656

Digital Watermarking Applications and Techniques: A Brief Review

Aaqib Rashid
MCA (Kashmir University)
M.Phil Computer Science (Dr. C.V Raman University)

Abstract: The frequent availability of digital data such as audio, images and videos became possible to the public through the expansion of the internet. Digital watermarking technology is being adopted to ensure and facilitate data authentication, security and copyright protection of digital media. It is considered as the most important technology in today's world, to prevent illegal copying of data. Digital watermarking can be applied to audio, video, text or images. This paper includes the detail study of watermarking definition and various watermarking applications and techniques used to enhance data security.

Index Terms: Watermarking, Techniques, Security, Technology,

I. INTRODUCTION

The advancement of the Internet has resulted in many new opportunities for the creation and delivery of content in digital form. Applications include electronic advertising, real-time video and audio delivery, digital repositories and libraries, and Web publishing. But the important question that arises in these applications is the data security. It has been observed that current copyright laws are not sufficient for dealing with digital data. Hence the protection and enforcement of intellectual property rights for digital media has become a crucial issue. This has led to an interest towards developing new copy deterrence and protection mechanisms. One such effort that has been attracting increasing interest is based on digital watermarking techniques. As steganography pay most attention towards the degree of invisibility, watermarking pay most of its attributes to the robustness of the message and its ability to withstand attacks of removal, such as image operations (rotation, cropping, filtering) etc in case of images being watermarked. Digital watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital content.

II. DIGITAL WATERMARKING TECHNOLOGY

As we know the main purpose of both cryptography and steganography is to provide secret communication. However, they are not same. Cryptography hides the content of a secret message from malicious people, where as steganography even conceal the existence of the message. But a new emerging technology known as digital watermarking involves the ideas and theories of different subject coverage, such as signal processing, cryptography, probability theory and stochastic theory, network technology, algorithm design, and other techniques [1]. Digital watermarking hides the copyright information into the digital data through certain algorithm. The secret information to be embedded can be some text, author's serial number, company logo, images with some special importance. This secret information is embedded to the digital data (images, audio, and video) to ensure the security, data authentication, identification of owner and copyright protection. The watermark can be hidden in the digital data either visibly or invisibly. For a strong watermark embedding, a good watermarking technique is needed to be applied. Watermark can be embedded either in spatial or frequency domain. Both the domains are different and have their own pros and cons and are used in different scenario. Fig 1. Shows Digital Watermark embedding process and Fig. 2. Shows watermark detection process.

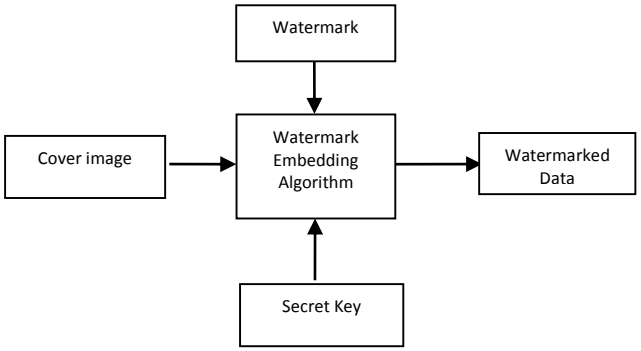

Fig 1. Watermark Embedding Process

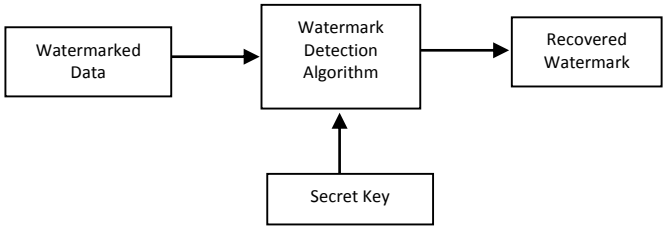

Fig 2. Watermark Detection Process

III. APPLICATIONS

Digital Watermarks are potentially useful in many applications, including:

A. Broadcast Monitoring

Advertisers want to ensure that they receive all of the air time which they purchase from broadcasters (Japan 1997) [5, 40]. A non-technical method in which human observation is used to watch the broadcast and check the originality by seeing or hearing is an error

prone and costly. Thus, there should be an auto-identification system, which may store the identification codes to the broadcast. There are several techniques like cryptography that store the identification code in the file header but the data is unlikely to survive any sort of modifications even format change. Watermarking is obviously a suitable technique for information monitoring. The Watermark exists within the content and is compatible with the installed base of broadcast equipment. Although, embedding the identification code is very complicated compared to the cryptography where the code is placed in the file header. Moreover, it also, affects the visual quality of the work. Still, many companies protect their broadcasts through watermarking techniques.

B. Ownership Assertion

A rightful owner can retrieve the watermark from digital content to prove his ownership. There are limitations with textual copyright notices, as they are easily removable. Copyright notice printed on the physical document cannot be copied along with the digital content. Although, it is possible that text copyright can be placed in an unimportant place of the document to make them unobtrusive [41]. Imperceptible and inseparable watermark is the best solution as compared to the text mark for owner identification. The watermark is not only used for identification of the copyright ownership but for proving the ownership of the document as well. The ownership can be carried out by extracting the embedded information from the watermarked document [42].

C. Transaction Tracking

Transaction tracking is often called fingerprinting, where each copy of the work is uniquely identified, similar to the fingerprint that identifies an individual. The watermark might record the recipient for each legal distribution of the work. The

owner embeds different watermarks in each copy. If the work is misused then will the owner be able to find the traitor? Visible watermarking is adopted for transaction tracking but invisible watermarking is much better. For example, in movie making, the daily videos (also called dailies) are distributed to the persons who are concerned with the movie. Sometimes, the videos are disclosed to the press, so the studios use visible text on corner of the screen, which identifies the copy of dailies. Thus, the watermark is preferred as the text can easily be removed.

D. Content Authentication

The procedure to confirm the integrity of watermarked data and to make sure that the data is not being tampered with i.e. act of establishing or confirming whether image is authentic or not. The term authentication has an extensive range of meanings. For instance, an authority that decides whether a portion of art is authentic or not, can a user view or download it? Finally, the decision is to whether the content of an object is staying intact or not after its transmission on the internet. Many cultural organizations spend time and investing money on new technologies of image documentation and digital libraries construction etc. At the same time, these organizations can guarantee the authenticity of the pieces of art they possess, since they have both the ownership and the experts opinions. When these works of art are digitized and published on the internet, numerous problems take place. Usually several digital images found on the internet have many differences, but at the same time pretending to represent the same piece of art. Use of watermarking related to authentication comprises of trusted cameras, video surveillance and remote sensing applications, digital insurance claim evidence, journalistic photography, and digital rights management systems. Commercially, its applications are expected to grow as does the applications of digital content, for example, GeoVision's GV-Series digital video recorders for digital video surveillance to prevent tampering. The digital work can easily be tampered by using computer resources. A solution to the tamper detection is watermarking, where the authentication mark (watermark) cannot stay with the work after slightest modification. Conversely, the system

does not matter that the work is compressed or significant changes are made. This leads toward semi-fragile watermarking where the system survive the friendly manipulations and fragile against substantial manipulations [5].

E. Copy Control and Fingerprinting

Copy control and fingerprinting are used to prevent people from making illegal copies of the content. This issue is very similar to the transaction tracking of the content. An owner can embed a watermark into digital content that identifies the buyer of the copy (i.e. serial number). If unauthorized copies are found later, the owner can trace the origin of the illegal copies.

IV. DIGITAL IMAGE WATERMARKING TECHNIQUES

In the field of digital watermarking, digital image watermarking has attracted a lot of awareness in the research community for two reasons: one is its easy availability and the other is it convey enough redundant information that could be used to embed watermarks [2]. Digital watermarking contains various techniques for protecting the digital content. The entire digital image watermarking techniques always works in two domains either spatial domain or transform domain. The spatial domain techniques works directly on pixels. It embeds the watermark by modifying the pixels value. Most commonly used spatial domain techniques are LSB. Transform domain techniques embed the watermark by modifying the transform domain coefficients. Most commonly used transform domain techniques is DCT, DWT and DFT. For achieving the robustness and imperceptibility, the transform domain techniques are more effective as compare to the spatial domain.

A. Spatial domain watermarking techniques*:*

The spatial domain represents the image in the form of pixels. The spatial domain watermarking embeds the watermark by modifying the intensity and the colour value of some selected pixels [3]. The strength of the spatial domain watermarking is:

- Simplicity.
- Very low computational complexity.
- Less time consuming.

The spatial domain watermarking is easier and its computing speed is high than transform domain but it is less robust against attacks. The spatial domain techniques can be easily applied to any image. The most important method of spatial domain is LSB.

i. Least Significant Bit (LSB):

The LSB is the simplest spatial domain watermarking technique to embed a watermark in the least significant bits of some randomly selected pixels of the cover image.

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

1) Convert RGB image to grey scale image.
2) Make double precision for image.
3) Shift most significant bits to low significant bits of watermark image.
4) Make least significant bits of host image zero.
5) Add shifted version (step 3) of watermarked image to modified (step 4) host image.

The main advantage of this method is that it is easily performed on images. And it provides high perceptual transparency. When we embed the watermark by using LSB the quality of the image will not degrade. The main drawback of LSB technique is its poor robustness to common signal processing operations because by using this technique watermark can easily be destroyed by any signal processing attacks. It is not vulnerable to attacks and noise but it is very much imperceptible.

Some other algorithms of spatial domain watermarking are briefly discussed below:

ii. Additive Watermarking: The most straightforward method for embedding the watermark in spatial domain is to add pseudo random noise pattern to the intensity of image pixels. The noise signal is usually integers like (-1, 0, 1) or sometimes floating point numbers. To ensure that the watermark can be detected, the noise is generated by a key, such that the correlation between the numbers of different keys will be very low [5].

iii. SSM Modulation Based Technique: Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark.

iv. Texture mapping coding Technique: This method is useful in only those images which have some texture part in it. This method hides the watermark in the texture part of the image. This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage) [3], and cannot be done automatically. This method hides data within the continuous random texture patterns of a picture.

v. *Patchwork Algorithm:* Patchwork is a data hiding technique developed by Bender et al and published on IBM Systems Journal, 1996 [6]. It is based on a pseudorandom, statistical model. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution. A pseudo randomly selection of two patches is carried out where the first one is A and the second is B. Patch A image data is brightened where as that of patch B is darkened (for purposes of this illustration this is magnified).

vi. Correlation-Based Technique: In this technique, a pseudorandom noise (PN) pattern says W(x, y) is added to cover image I(x, y). Iw(x, y) = I(x, y) + k*W(x, y) Where K represent the gain factor, Iw represent watermarked image ant position x, y and I represent cover image. Here, if we increase the gain factor then although it increases the robustness of watermark but the quality of the watermarked image will decrease.

B. Frequency domain watermarking techniques:

Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients [7]. Some of its main algorithms are discussed below:

i. Discrete cosine transforms (DCT): DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image. Steps in DCT Block Based Watermarking Algorithm [8]

1) Segment the image into non-overlapping blocks of 8x8
2) Apply forward DCT to each of these blocks
3) Apply some block selection criteria (e.g. HVS)
4) Apply coefficient selection criteria (e.g. highest)
5) Embed watermark by modifying the selected coefficients.
6) Apply inverse DCT transform on each block.

ii. Discrete wavelet transforms (DWT): Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL). The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well [9]. One of the main challenges of the watermarking problem is to achieve a better tradeoff between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased as well [9]. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image [10]. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequencies [11].

Advantages of DWT over DCT:

Wavelet transform understands the HVS more closely than the DCT. Wavelet coded image is a multi-resolution description of image. Hence an image can be shown at different levels of resolution and can be sequentially processed from low resolution to high resolution. [2]

Disadvantages of DWT over DCT:

Computational complexity of DWT is more compared to DCT'. As Feig (1990) pointed out it only takes 54 multiplications to compute DCT for a block of 8x8, unlike wavelet calculation depends upon the length of the filter used, which is at least 1 multiplication per coefficient [2]

iii. Discrete Fourier transform (DFT):

Transforms a continuous function into its frequency components. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform.

Advantages of DFT over DWT and DCT:

DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions, whereas the spatial domain, DCT and the DWT are not RST invariant and hence it is difficult to overcome from geometric distortions. [2]

Table below shows comparisons of different watermarking algorithms. [12][13]

Algorithm	Advantages	Disadvantages
LSB	1. Easy to implement and understand 2. Low degradation of image quality 3. High perceptual transparency.	1. It lacks basic robustness 2. Vulnerable to noise 3. Vulnerable to cropping, scaling.
Correlation	1. Gain factor can be increased resulting in increased robustness	1. Image quality gets decreased due to very high increase in gain factor.
Patchwork	1. High level of robustness against most type of attacks	1. It can hide only a very small amount of information.
Texture mapping coding	1. This method hides data within the continuous random texture patterns of a picture.	1. This algorithm is only suitable for those areas with large number of arbitrary texture images.
DCT	1. The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not get affected and the watermark will not be removed by any kind of attack.	1. Block wise DCT destroys the invariance properties of the system. 2. Certain higher frequency components tend to be suppressed during the quantization step.
DWT	1. Allows good localization both in time and spatial frequency domain 2. Higher compression ratio which is relevant to human perception.	1. Cost of computing may be higher. 2. Longer compression time. 3. Noise/blur near edges of images or video frames
DFT	1. DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions	1. Complex implementation 2. Cost of computing may be higher.

CONCLUSIONS

In this paper we have presented watermarking overview and also briefly discussed various watermarking techniques. Apart from this a brief and comparative analysis of watermarking techniques is presented with their advantages and disadvantages which can help in the new research areas.

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.

About Author
Aaqib Rashid is a Research Scholar and has completed MCA from Kashmir University and M.Phil in Computer Science from Dr. C.V Raman University India.