International Journal of Computer Network and Security(IJCNS)
Vol 8. No.1 –2016 Pp. 11-16

available at : www.ijcns.com
ISSN: 0976-1345

SURVEY ON DIGITAL WATERMARKING TECHNIQUES

G.SHOBA
Senior Assistant Professor,
Department of Computer Science and Engineering
Christ College of Engineering and Technology
Pondicherry, India

G.JEYALAKSHMY
M.Tech – Scholar
Department of Computer Science and Engineering
Christ College of Engineering and Technology
Pondicherry, India

Abstract- The protection and illegal redistribution of digital media has become an important issue in the digital era. This is due to the popularity and accessibility of the Internet now a days by people. This results in recording, editing and replication of multimedia contents. Digital watermarking can be used to protect digital information against illegal manipulations and distributions. Digital watermarking technique is the process of embedding noise-tolerant signal such as audio or image data in the carrier signal. This technique provides a robust solution to the problem of intellectual property rights for online contents. In this paper, we present a comprehensive survey on various digital watermarking techniques such as robust, fragile and semi fragile watermarking techniques. This paper provides evidence that digital watermarking techniques are of increasing interest and are of gaining popularity.

1. INTRODUCTION

In recent years, as digital media are gaining wider popularity, their security related issues are becoming greater concern. Digital watermarking is a technique which allows an individual to add copyright notices or other verification messages to digital media. Image authentication is one of the applications of digital watermarking, which is used for authenticating the digital images. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate.

The image and assure the integrity of the image. The way to realize this feature is to embed a layer of the authentication signature into the digital image using a digital watermark. In the case of the image being tampered, it can easily be detected as the pixel values of the embedded data would change and do not match with the original pixel values. There are many spatial and frequency domain techniques available for authentication of watermarking. Watermarking techniques are judged on the basis of their performance on a small set of properties. These properties include robustness, transparency, watermarking capacity, blind detection and security. Watermarking schemes are developed according to the requirements of the application and all applications do not require each of these properties in their entirety i.e. watermarking requirements are application dependent and some most desirable properties for these applications are conflicting in nature. A huge trade-off among them is often involved. Digital signature is also an authentication scheme

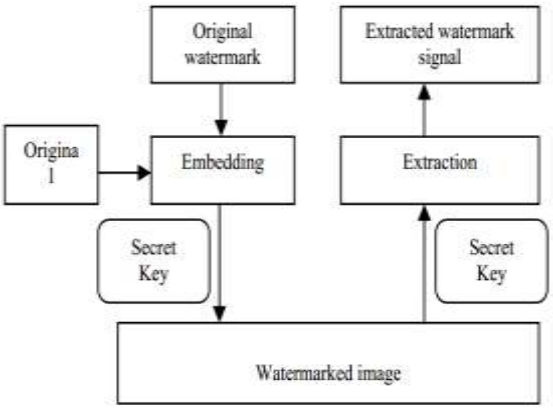
that is used for verifying the integrity and authenticity of the image content. Digital data are distributed across high-speed networks like the Internet and World Wide Web. This data is easily accessible for sharing. Due to this access possibility of tempering data and republishing it as own is increased. This leads the motivation of techniques providing security to this multimedia content. Digital watermarking is the technique used for this purpose. Various techniques of watermarking are used to insert data about ownership of contents, which help to keep the integrity of data.A watermark is information about origin, ownership, copy control etc. This information is embedded in multimedia content with taking care imperceptibly and robustness. The watermark is embedded and extracted as per requirement. Video watermarking is different from image watermarking, because additional data are available here that allows information to be more redundantly and reliably embedded. Digital video is a sequence or collection of consecutive still images. The amount of information that can be embedded in the video sequence is called payload. In reality video watermarking techniques need to meet other challenges than that in image watermarking schemes such as large volume of the inherently repeated sequence of data between frames

2. WATERMARKING PRINCIPLE

A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself.

3. BLOCK DIAGRAM OF WATERMARKING PROCESS

The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark on to the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark.



4. ASPECTS OF VIDEO WATERMARKING

Video sequencing is a collection of consecutive and equally time spaced still images. Apparently any image watermarking technique can be extended to watermark videos, but in reality video watermarking techniques needs to meet other challenges. Watermarked video sequences are very much susceptible to pirate attacks such as frame averaging, frame swapping, statistical

analysis, digital analog (AD/DA) conversion, and lossy compressions. Watermarking systems can be characterized by a number of defining properties including embedding effectiveness, fidelity, data payload, blind or informed detection, false positive rate, capacity, robustness, perceptual transparency, security, cipher and watermark keys, modification and multiple watermark, cost, tamper resistance, unobtrusiveness, ready detection, unambiguous, sensitivity, and scalability. Some of them are common to more practical applications. In this section, such general properties will be listed and briefly discussed and focus will put on video watermarking. These properties are discussed due to their importance in watermarking applications.

A. Perceptual Transparency

Invisibility is the degree at which an embedded watermark remains unnoticeable when a user views the watermarked contents. However this requirement conflicts with other requirements such as tamper resistance and robustness, especially against lossy compression algorithms. To survive the next generation of compression algorithms, it will probably be necessary for a watermark to be noticeable to a trained observer which is asked to compare the original and the marked version of the video.

B. Robustness

Robustness is the resilience of an embedded watermark against removal by signal processing. The use of music, images and video signals in digital form, commonly involves many types of distortions, such as lossy compression. For watermarking to be useful, the mark should be detectable even after such distortions occurred. Robustness against signal distortion is better achieved if the watermark is placed in perceptually significant parts of the signal.Due to large amounts of data and inherent redundancy between frames, video signals are highly vulnerable to pirate attacks, such as frame averaging, frame dropping, rotation, sharpening.

C. Capacity

Capacity is that amount of information that can be expressed by an embedded watermark. Depending on the application at hand, the watermarking algorithm should allow a predefined number of bits to be hidden.

5. WATERMARKING TECHNIQUES

The various watermarking techniques are:

A. SPATIAL DOMAIN TECHNIQUES

Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when

subjected to normal media operations such as filtering or lossy compression. Various spatial domain techniques are as follows:-

Least Significant Bit Coding (Lsb)

LSB coding is one of the earliest methods. It can be applied to any form of watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. In order to retrieve it back this sequence should be known. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component.

Predictive Coding Schemes

Predictive coding scheme was proposed by Matsui and Tanaka for gray scale images. In this method the correlation between adjacent pixels are exploited. A set of pixels where

the watermark has to be embedded is chosen and alternate pixels are replaced by the difference between the adjacent pixels. This can be further improved by adding a constant to all the differences. A cipher key is created which enables the retrieval of the embedded watermark at the receiver. This is much more robust as compared to LSB coding.

Correlation-Based Techniques

In this method a pseudo random noise (PN) with a pattern W(x, y) is added to an image. At the decoder the correlation between the random noise and the image is found out and if the value exceeds a certain threshold value the watermark is detected else it is not.

Patchwork Techniques

In patchwork watermarking, the image is divided into two subsets. One feature or an operation is chosen and it is applied to these two subsets in the opposite direction. For instance if one subset is increased by a factor k, the other subset will be decreased by the same amount. If a[i] is the value of the sample at I in subset 'A' which is increased and b[i] is the value of the sample in the subset 'B' whose value is decreased, then the difference between the two subsets would intuitively result in

$\Sigma(a[i]-b[i]) = 2N$ for watermarked images

$1 <= N <= \infty$

= 0 otherwise

B. FREQUENCY DOMAIN TECHNIQUES

In Frequency domain the secret data are hidden in the lower or middle frequency portions of the protected image, because the higher frequency portion is more likely to be suppressed by compression. But how to select the best frequency portions of the image for watermark is another important and difficult topic. Various frequency domain techniques are as follows:-

Discrete Cosine Transform (Dct) Based Technique

Discrete cosine transform (DCT): It is a process which converts a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with different amplitudes in the frequency domain. The DCT is a linear transform, which maps an n-dimensional vector to a set of n coefficients. It is very robust to JPEG compression, since JPEG compression itself uses DCT. However, DCT methods lack resistance to strong geometric distortions.

Discrete Fourier Transformation (Dft) Based Technique

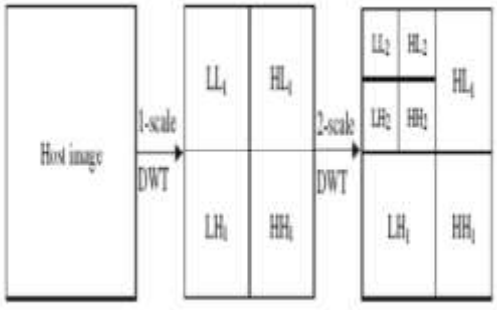
It is translation invariant and rotation resistant, which translates to strong robustness to geometric attacks.DFT uses complex numbers, while DCT uses just real numbers.

Discrete Wavelet Transform (Dwt) Based Technique

DWT-based methods enable good spatial localization and have multi resolution characteristics, which are similar to the human visual system. Also this approach shows robustness to low-pass and median filtering. However, it is not robust to geometric transformations.

C. WAVELET TRANSFORM BASED WATERMARKING

The wavelet transform based watermarking technique divides the image into four sidebands – a low resolution approximation of the tile component and the component's horizontal, vertical and diagonal frequency characteristics. The process can then be repeated iteratively to produce N scale transform.



Digital watermarking techniques are classified according to various criteria like robustness, perceptibility, embedding and retrieval methods. Robustness is an important criterion which means the ability of watermark to resist common image processing operations. Watermarking techniques based on robustness can be further divided into three main categories:

(1) Robust (2) Fragile (3) Semi-fragile

Robust watermarking schemes are applied for proving ownership claims whereas fragile watermarking is applied to multimedia content authentication. These watermarking schemes have their own requirements in terms of robustness. Robust watermarks should be able to survive a wide range of friendly operations and malicious attacks, whereas fragile watermarks are intolerable to both malicious and content preserving operations. Fragile watermarking techniques are designed with a goal to identify and report every possible tampered region in the watermarked digital media. Semi-fragile watermarks are intermediate in robustness between the two and are also used for image authentication. Some critical applications like medical imagining and forensic image archiving also requires the fragile watermarks to be reversible. The different quantitative parameters such as PSNR, True and false positive may be used for the evaluation of the method of watermarking schemes.

6. APPLICATIONS

Digital watermarking can be used for the following purposes:

A. Copyright Protection: This is by far the most prominent application of watermarks. With tons of images being exchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking an image will prevent redistribution of copyrighted images.

B. Authentication: Sometimes the ownership of the contents has to be verified. This can be done by embedding a watermark and providing the owner with a private key which gives him an access to the message. ID cards, ATM cards, credit cards are all examples of documents which require authentication.

C. Broadcast Monitoring: As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not.

D. Content Labeling: Watermarks can be used to give more information about the cover object. This process is named as content labeling.

E. Tamper Detection: Fragile watermarks can be used to detect tampering in an image. If the fragile watermark is degraded in any way then wecan say that the image or document in question has been tampered.

F. Digital Fingerprinting: This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner.

G. Content protection: In this process the content stamped with a visible watermark that is very difficult to remove so that it can be publicly and freely distributed.

7. CONCLUSIONS

This paper provides a comprehensive survey on various digital watermarking techniques, their requirements and applications. The use of different type of watermark is application dependent. Digital watermarking research has generally focused upon two classes of watermarks, fragile and robust. Robust watermarks are designed to be detected even after attempts are made to remove them. Fragile watermarks are used for authentication purposes and are capable of detecting even minute changes of the watermarked content. But neither type of watermark is ideal when considering "information preserving" transformations (such as compression) which preserve the meaning or expression of the content and "information altering" transformations (such as feature replacement) which change the expression of the content. To solve this problem a semi-fragile watermark for still images that can detect information altering transformations even after the watermarked content is subjected to information preserving alterations has to be used.

REFERENCES

[1] Cox, I. J., Kilian, J., Leighton,F. T., andShamoon, T.,"Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, Vol. 6,No. 12, pp. 1673-1687, 1997.

[2] Huang, J. and Shi, Y. Q., "Adaptive Image Watermarking Scheme Based on Visual masking," IEE Electronics Letters, Vol. 34, No. 8, pp. 748-750, 1998

[3] Kim, Y.-S., Kwon, O.-H., and Park, R.-H., "Wavelet Based Watermarking Method for Digital Images Using The Human Visual System," IEE Electronics Letters, Vol. 35, No. 6, pp. 466-468, 1999.

[4] Chen, D.-Y., Ouhyoung, M., and Wu, J.-L.,"A Shift-Resisting Public Watermark System for Protecting Image Processing Software," IEEE Transactions on Consumer Electronics, Vol. 46, No. 3, pp.404-414, 2000.

[5] Aree Ali Mohammed & Haval Mohammed Sidqi," Robust Image Watermarking Scheme Based on Wavelet Technique", International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (4) : 2011

[6] G. Dayalin Leena and S. Selva Dhayanithy," Robust Image Watermarking in Frequency Domain",International Journal of Innovation and Applied Studies ISSN 2028-9324 Vol. 2 No. 4 Apr. 2013, pp. 582-587

[7] H. Guo et al.," A fragilewatermarking scheme for detecting malicious modifications of database relations", Information Sciences 176 (2006) 1350–1378

[8] C.-M. Chou, D.-C. Tseng," A public fragile watermarking scheme for 3D model authentication",Computer-AidedDesign 38 (2006) 1154–1165 Available:www.sciencedirect.com

[9] W.-C. Chen, M.-S. Wang (2009), "A Fuzzy c-Means Clustering based Fragile Watermarking Scheme for Image Authentication", Expert Systems with Applications, Volume 36, Issue 2, Part 1, pp. 1300-1307.
Available:www.sciencedirect.com.

[10] Ankan Bhattacharya, Sarbani Palit, Nivedita Chatterjee, and Gourav Roy (2011), "Blind assessment of image quality employing fragile watermarking", 7th International Sym. on Image and Signal Processing and Analysis (ISPA 2011) Dubrovnik, Croatia, pp. 431-436.