DIGITAL WATERMARKING PROCESSING TECHNIQUE BASED ON OVER COMPLETE DICTIONARY

Aishwarya.R,
B.Sc (Computer Technology),
Department Of Computer Science,
Sri Krishna Adithya College of Arts and Science,
Coimbatore,Tamilnadu,India.

Mounapriya.R,
B.Sc (Computer Technology),
Department Of Computer Science,
Sri Krishna Adithya College of Arts and Science,
Coimbatore,Tamilnadu,India.

Saranya.N,
B.Sc (Computer Technology),
Department Of Computer Science,
Sri Krishna Adithya College of Arts and Science,
Coimbatore,Tamilnadu,India.

Abstract: A novel sparse domain-based information hiding framework is proposed in this paper. The adaptive sparse domain can be utilized to embed watermarking logo with better security and robustness. This can be realized owing to the fact that, not only sparse domain can be customized from the given samples, but also the sparse transform coefficients of the original watermarking signal can be embedded, which provides inherent privacy. This paper provides two kinds of methods that embed watermark directly and embed the sparse representation coefficients of watermarking logo, and analyzes the condition of uniqueness of the sparse solution.

Keywords: Digital watermarking; applications; water marking; relational database over complete dictionary.

I.INTRODUCTION

General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions. The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. 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. Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

II.APPLICATIONS

Digital watermarking may be used for a wide range of applications, such as:

- Copyright protection
- Source tracking (different recipients get differently watermarked content)
- Broadcast monitoring (television news often contains watermarked video from international agencies)
- Video authentication
- Software crippling on screencasting programs, to encourage users to purchase the full version to remove it.

III.CLASSIFICATION

A digital watermark is called robust with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise, and quantization. For video content, temporal modifications and MPEG compression often are added to this list. A digital watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, unwatermarked content.[4] In general, it is easy to create either robust watermarks—or—imperceptible watermarks, but the creation of both robust—and—imperceptible watermarks has proven to be quite challenging.[1] Robust imperceptible watermarks have been proposed as a tool for the protection of digital content, for example as an embedded no-copy-allowed flag in professional video content.

Digital watermarking techniques may be classified in several ways.

Robustness: A digital watermark is called "fragile" if it fails to be detectable after the slightest modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that clearly are noticeable, commonly are not referred to as watermarks, but as generalized barcodes.

A digital watermark is called semi-fragile if it resists benign transformations, but fails detection after malignant transformations. Semi-fragile watermarks commonly are used to detect malignant transformations. A digital watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copy protection applications to carry copy and no access control information.

Perceptibility: A digital watermark is called imperceptible if the original cover signal and the marked signal are perceptually indistinguishable. A digital watermark is called perceptible if its presence in the marked signal is noticeable (e.g. Digital On-screen Graphics like a Network Logo, Content Bug, Codes, Opaque images). On videos and images, some are made transparent/translucent for convenience for consumers due to the fact that they block portion of the view; therefore degrading it.

This should not be confused with perceptual, that is, watermarking which uses the limitations of human perception to be imperceptible.

Capacity: The length of the embedded message determines two different main classes of digital watermarking schemes: The message is conceptually zero-bit long and the system is designed in order to detect the presence or the absence of the watermark in the marked object. This kind of watermarking scheme is usually referred to as zero-bit or presence watermarking schemes. Sometimes, this type of watermarking scheme is called 1-bit watermark, because a 1 denotes the presence (and a 0 the absence) of a watermark.

IV.EMBEDDING METHOD

A digital watermarking method is referred to as spread-spectrum if the marked signal is obtained by an additive modification. Spread-spectrum watermarks are known to be modestly robust, but also to have a low information capacity due to host interference. A digital watermarking method is said to be of quantization type if the marked signal is obtained by quantization. Quantization watermarks suffer from low robustness, but have a high information capacity due to rejection of host interference. A digital watermarking method is referred to as amplitude modulation if the marked signal is embedded by additive modification which is similar to spread spectrum method, but is particularly embedded in the spatial domain.

V.EVALUATION AND BENCHMARKING

The evaluation of digital watermarking schemes may provide detailed information for a watermark designer or for end-users, therefore, different evaluation strategies exist. Often used by a watermark designer is the evaluation of single properties to show, for example, an improvement. Mostly, end-users are not interested in detailed information. They want to know if a given digital watermarking algorithm may be used for their application scenario, and if so, which parameter sets seems to be the best.

Cameras: Epson and Kodak have produced cameras with security features such as the Epson PhotoPC 3000Z and the Kodak DC-290. Both cameras added irremovable features to the pictures which distorted the original image, making them unacceptable for some applications such as forensic evidence in court. According to Blythe and Fridrich, "[n]either camera can provide an undisputable proof of the image origin or its author

A secure digital camera (SDC) was proposed by Saraju Mohanty, et al. in 2003 and published in January 2004. This was not the first time this was proposed. Blythe and Fridrich also have worked on SDC in 2004 for a digital camera that would use lossless watermarking to embed a biometric identifier together with a cryptographic hash.

Reversible data hiding: Reversible data hiding is a technique which enables images to be authenticated and then restored to their original form by removing the digital watermark and replacing the image data that had been overwritten. This would make the images acceptable for legal purposes. The US Army also is interested in this technique for authentication of reconnaissance images.

Watermarking for relational databases: Digital watermarking for relational databases has emerged as a candidate solution to provide copyright protection, tamper detection, traitor tracing, and maintaining integrity of relational data. Many watermarking techniques have been proposed in the literature to address these purposes. A survey of the current state-of-the-art and a classification of the different techniques according to their intent, the way they express the watermark, the cover type, granularity level, and verifiability was published in 2010 by Halder et al. in the Journal of Universal Computer Science

VI.REFERENCES

[1]. Ingemar J. Cox: Digital watermarking and steganography. Morgan Kaufmann, Burlington, MA, USA, 2008

[2]. Frank Y. Shih: Digital watermarking and steganography: fundamentals and techniques. Taylor & Francis, Boca Raton, FL, USA, 2008

[3]. A.Z.Tirkel, G.A. Rankin, R.M. Van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. "Electronic Water Mark". DICTA 93, Macquarie University. p.666-673

[4]. Khan, A. and Mirza, A. M. 2007. Genetic perceptual shaping: Utilizing cover image and conceivable attack information during watermark embedding. Inf. Fusion 8, 4 (Oct. 2007), 354-365

[5]. "CPTWG Home Page". cptwg.org

[6]. Paul Blythe; Jessica Fridrich, Secure Digital Camera

[7]. Raju Halder; Shantanu Pal; Agostino Cortesi, Watermarking Techniques for Relational Databases: Survey, Classification and Comparison (PDF), The Journal of Universal Computer Science, vol 16(21), pp. 3164-3190, 2010.hell0