SURVEY ON DIGITAL WATERMARKING TECHNIQUES

Rutuja Sonar[1], Shivaputra S. Panchal[2]

[1]MTech Student, [2]Assistant Professor, Dept. of Computer Science and Engg,
Dr.P.G.Halakatti Engineering College, Vijayapur

ABSTRACT

A digital watermark is a kind of marker concealed embedded in a noise tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal. Embedding a digital data with information which cannot be removed easily is called digital watermarking. Digital watermarks may be used to verify the authenticity or integrity of the digital data or to show the identity of its owners. This paper provides a comprehensive survey on various digital watermarking techniques such as robust, fragile and semi fragile watermarking techniques.

I. INTRODUCTION

Growth of computer and network technology has led to tremendous opportunities for creation and distribution of digital media content. And the digital data is easy to be edited and illegal duplication, and thus the technology to resolve such issues is in demand. The Digital watermarking technique makes use of a data hiding scheme to insert some information in the image.Digital watermarking is a technique which embeds additional information called digital signature or watermark into the digital content in order to secure it. A watermark is a hidden signal added to images that can be detected or extracted later to make some affirmation about the host image. The major point of digital watermarking is to find the balance among the aspects such as robustness to various attacks, security and invisibility. The invisibleness of watermarking technique is based on the intensity of embedding watermark. Better invisibleness is achieved for less intensity watermark. So we must select the optimum intensity to embed watermark. In general there is a little tradeoff between the embedding strength (the watermark robustness) and quality (the watermark invisibility). Increased robustness requires a stronger embedding, which in turn increases the visual degradation of the images.

II. CLASSIFICATION

The digital image watermarking scheme can be divided into two categories. They are visible digital image watermarking and invisible image watermarking techniques. In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the original document.

In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such. Further, the invisible watermarks are categorized into watermarking techniques as robust, fragile and semi-fragile.

- **Robust** - Generally, a robust mark is generally used for copyright protection and ownership identification because they are designed to withstand nearly all attacks such as lossy compression, filtering operations and

geometric distortions. These algorithms ensure that the image processing operations do not erase the embedded watermark signal.

- **Fragile**– In fragile techniques, even one bit change in image is not allowable. They are mainly applied to content authentication and integrity attestation, because they are sensitive to almost all modifications.
- **Semi-fragile**– Semi-fragile methods are robust to incidental modifications such as JPEG compression, but fragile to other modifications such as high impact additive noises. That is, some incidental image manipulations have to be considered allowable during the process of media transmission and storage, while other malicious modifications (e.g. alteration of content) from attackers should be rejected.

III. WATERMARKING TECHNIQUES

The various watermarking techniques are:

3.1 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. Various spatial domain techniques are as follows:-

- Least Significant Bit Coding (LSB)
- Predictive Coding Schemes
- Correlation-Based Techniques

3.2 Frequency Domain Techniques

In Frequency domain the secret data are hidden in thelower or middle frequency portions of the protected image,because the higher frequency portion is more likely to be suppressed by compression. Various frequency domain techniques are as follows:-

- Discrete cosine transform (DCT) based technique
- Discrete Fourier Transformation (DFT) based technique
- Discrete wavelet transform (DWT) based technique

3.3 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.

3.4 Block-Wise Technique

One of the first fragile block-wise watermarking schemes with tamper localization was proposed by Wong. In this scheme, an image is divided into non-overlapping blocks and watermarking is performed for each block independently. The seven most significant bits (MSBs) of all pixels in a block are hashed using a secure key-dependent hash. The hash is then XORed with a chosen binary logoand inserted into the LSBs of the same block. The verification process starts in the reverse order by calculating the key-dependent hash of the seven MSBs in each block and XOR operation is performed with the LSBs.The tampered blocks can be found by comparing the output with the used logo.

3.5 Literature Survey on Temper Detection in Digital Watermarking

In this paper [1], three public image watermarking techniques are proposed. The first one, called Single Watermark Embedding (SWE), uses the concept of Visual Cryptography (VC) to embed a watermark into a digital image. The second one, called Multiple Watermarks Embedding (MWE) extends SWE to embed multiple watermarks simultaneously in the same host image. Finally, Iterative Watermark Embedding (IWE) embeds the same binary watermark iteratively in different positions of the host image, to improve the robustness.

In this [2] Progressive image transmission (PIT) provides multiple image resolutions that favors a time-critical or a low-band channel environment. Author proposes, a PIT based watermarking for multi-resolution image authentication. The image content with progressive characteristic is taken as the authentication code. The authentication code is then embedded according to multi-resolution image encoding.

In this [3] author proposes a technique which embeds information into a carrier image with virtually imperceptible modification of the image. The present paper found a novel fact that by inserting the watermark using Least Significant Bit (LSB), the grey value of the image pixel either remains same or increases or decreases to one.

In this [4], author present three counterfeiting attacks on the block-wise dependent fragile watermarking schemes. We consider vulnerabilities such as the exploitation of a weak correlation among block-wise dependent watermarks to modify valid watermarked images, where they could still be verified as authentic.

In this [5], author propose a novel multipurpose watermarkingscheme, in which robust and fragile watermarks are simultaneously embedded, for copyright protection and content authentication. By quantizing a host image's wavelet coefficients as masking threshold units (MTUs), two complementary watermarks are embedded using cocktail watermarking and they can be blindly extracted without access to the host image.

In this [6], Watermarking techniques which are fragile to intentional modifications while robust to incidental or unintentional manipulations are referred to as Semi-fragile. This paper proposes a semi-fragile watermarking technique which embeds watermark signal into the host image in order to authenticate it.

This [7], paper presents a novel invisible robust watermarking scheme for embedding and extractinga digital watermark in an image. The novelty lies in determining a perceptually important sub-image in the host image. Invisible insertion of the watermark is performed in the most significantregion of the host image such that tampering of that portion with an intention to remove ordestroy will degrade the esthetic quality and value of the image.

In this [8] paper, author propose an efficient image tamper detection method using block-wise technique which is able to detect the tamper locations. In the proposed method, a digital signature is generated from the hash code of the blocks of the final level where the watermark is inserted and the blocks of the upper level where those blocks are included in the image division process and this signature is used as the watermark, which is randomly inserted into selected image blocks. The proposed method was confirmed to be able to detect the tampered parts of the image without testing the entire block of the watermarked image. The image block-wise watermarking method was proposed by using digital signature. The tampered blocks could be detected faster by testing the hash code of the upper level first without testing all inserted blocks with watermarks inserted.

IV. APPLICATIONS

Digital watermarking can be used for the following purposes:

- **Copyright Protection:**This is by far the most prominent application of watermarks. With tons of images beingexchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking an image will prevent redistribution of copyrighted images.
- **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.
- **Broadcast Monitoring:** As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio.
- **Content Labeling:** Watermarks can be used to give more information about the cover object. This process is named as content labeling.
- **Tamper Detection:** Fragile watermarks can be used todetect tampering in an image. If the fragile watermark isdegraded in any way then we can say that the image ordocument in question has been tampered.
- **Digital Fingerprinting:**This is a process used to detectthe owner of the content. Every fingerprint will beunique to the owner.
- **Content protection:**In this process the content stampedwith a visible watermark that is very difficult to removeso that it can be publicly and freely distributed.

V. CONCLUSION

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 hasgenerally 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. And it provides the temper detection of digital watermarking image using bloc-wise technique.

REFERENCES

[1] B. Surekha and D. N. Swamy, “A Spatial Domain Public Image Watermarking”, International Journal of Security and its Applications, vol. 5, no. 1, (2011), pp. 1-12.

[2] P. Tsai, Y.-C.Hu, H.-L.Yeh and W.-K. Shih, “Watermarking for Multi-Resolution Image Authentication”, International Journal of Security and its Applications, vol. 6, no. 2, (2012), pp. 161-166.

[3] G.RoslineNesaKumari,B.VijayaKumar, L.Sumalatha, and DrV.V.Krishna, “Secure and Robust Digital Watermarking on Grey Level Images”, International Journal of Advanced Science and TechnologyVol. 11, October, 2009

[4] M. Holliman and N. Memon, "Counterfeiting Attacks on Oblivious Block-Wise Independent Invisible Watermarking Schemes", IEEE Transaction on Image Processing, vol. 9, no. 3, (2000), pp. 432-441.

[5] Chun-Shien Lu and Hong-Yuan Mark Liao, "Multipurpose Watermarking for Image Authentication and Protection", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 10, OCTOBER 2001, pp. 1579-1592

[6] Dr.M.Mohamed and SathikS.S.Sujatha, "Authentication of Digital Images by using a semi-Fragile Watermarking Technique", Volume 2, Issue 11, November 2012 ISSN: 2277 128X, pp. 39-44

[7] Saraju P. Mohanty and Bharat K. Bhargava, "Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks", ACM Journal Name, Vol. V, No. N, February 2008, Pages 1–24.

[8] Chan-Il Woo and Seung-Dae Lee, "Digital Watermarking for Image Tamper Detection using Block-Wise Technique", International Journal of Smart Home Vol.7, No.5 (2013), pp.115-124 ISSN: 1975-4094 IJSH.