Survey on Digital Image Watermarking Techniques

K T Abinesh[1], S.Abhinaya[2], Dr. V,Belmer Gladson[3]
[1]Student, [2]Assistant Professor, [3]Associate Professor,
Department of Artificial Intelligence and Data Science, Adhi College of Enggineering and Technology, Tamilnadu

Abstract **- In recent years, digital media are widely popular, their security related issues are becoming greater importance. Watermarking is the process of hiding digital data in a carrier signal. Embedding a digital signal such as audio, video or image with the information which cannot be removed easily is called digital watermarking. Digital watermarking mainly used to verify the authenticity, integrity of the carrier signal or to show the identity of its owners. In this paper, we present a survey on various digital watermarking techniques. This paper mainly concentrates a detailed survey of all watermarking techniques on image watermarking types in today's world.**

Index Terms **- Digital watermarking, spatial domain, Least Significant Bit (LSB), Frequency domain, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT).**

I.INTRODUCTION

The term digital watermarking was first emerged in 1993, Tirkel introduce two watermarking techniques to hide the watermark data in the images [1].In recent years digital media are gaining widely popular, and their security related issues are becoming greater importance. The protection and property rights for digital media have become an important issue [2]. Digital watermarking is a technique that provides security, authentication and copyright protection to the digital media. Image authentication is one of the applications of digital watermarking, which is used for authenticating the digital images. Watermarking is used for following reasons, Proof of Ownership, Copying Prevention, Broadcast Monitoring, Authentication, and Data Hiding. The main objective is not to protect the contents from being stolen, but is to provide a method to authenticate the image. Watermarking consists of two modules watermark embedding module and watermark detection and extraction module. The digital watermarking is a process of information hiding.

There are various techniques for hiding the information in the form of digital contents like image, text, audio and video. Digital watermarking method is also used for the tamper proofing and authentication[3].The application of digital watermarking are Broadcast Monitoring [4], Digital Fingerprinting [5], Transaction Tracking [6], Copyright protection [7], Temper Detection [8], Data Hiding [9] and Content Authentication [10] etc. The two techniques of digital watermarking are spatial and frequency domain techniques available. These watermarking techniques are judged on the basis of their performance on a small set of properties. Digital signature is also an authentication scheme that is used for verifying the integrity and authenticity of the image content. Watermarking stands for embedding a signal, called watermark into a digital cover, in order to verify ownership, check authenticity of the cover. Digital watermarking is a process of embedding some marks into digital content. These marks are typically invisible that can later be detected or extracted .The concept of digital watermarking is associated with Steganography. Steganography is defined as covered writing. Therefore, digital watermarking is a way to hide a secret or personal message to protect a product's copyright. Watermark may contain security feature such as document serial number. Watermarked document can give the information about modifications or upgrading by comparing the watermarked data to original data.The major drawback of digital signature is that it can detect if an image has been modified, but it cannot locate the regions where the image has been modified. To solve this problem, many researchers have proposed watermarking based schemes for image authentication. In order to evaluate the quality of algorithm or method some performance metrics are used such as the Mean Square Error (MSE)

and the Peak Signal Noise Ratio (PSNR). Hiding the data from the third party is a challenging task.

II.WATERMARKING FRAMEWORK

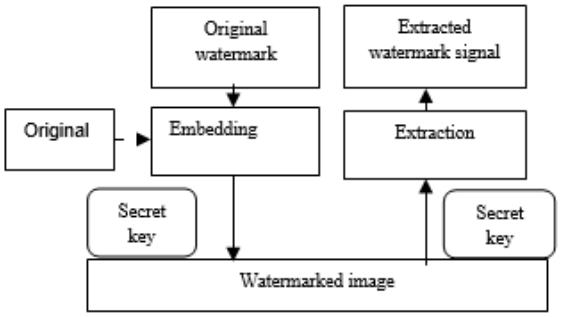

Fig. 1 Block diagram of Watermarking Process

The original image and the original watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in order to retrieve the original watermark signal. It is the reverse process of embedding scheme. The 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.

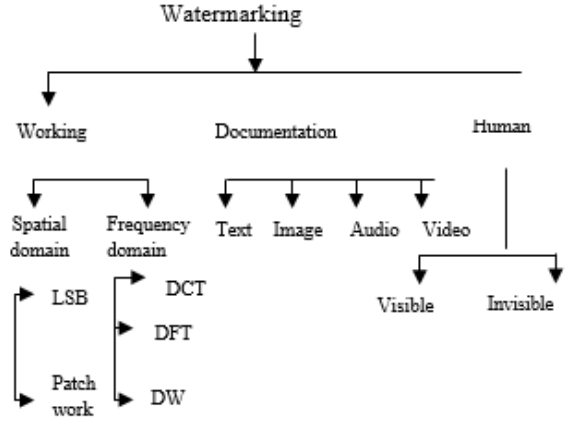

Fig. 2 Classification of Digital Watermarking

Based on transparency level the watermarks are divided into invisible and visible watermarking. In visible watermarking, a secondary image is embedded into host image or video, so that watermark is detectable to Human Visual System (HVS). Where as in invisible watermarking the embedded watermark is not detectable to Human Visual System (HVS) but it can be extracted for authentication purpose. Watermarking can be categorized into spatial domain and Transform domain. When the watermark is embedded by altered the pixel values of the host image directly by the determined embedding scheme then this scheme is spatial domain techniques. In the transform domain watermarking, the image is express in the form of frequency. In the transform domain watermarking techniques, the original image is converted by a predefined transformation. As a result it becomes hard to take away the embedded watermark proving Transform- domain technique to be more effective and more robust than spatial domain technique. The commonly used transform domain techniques are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Now a day's Discrete Wavelet Transform (DWT)is employed because of its multi resolution characteristics.

III.WATERMARKING TECHNIQUES

A.Spatial Domain Techniques

The spatial domain illustrates the image in the form of pixels. The spatial domain watermarking embeds thewatermark by altering the intensity and the color value of some selected pixels[11].This technique is not reliable to normal media operations such as filtering or lossy compression. Various spatial domain techniques are as follows:-

Least Significant Bit Coding (LSB)

The LSB is the simplest spatial domain watermarking technique to embed a watermark in the least significant bits of randomly selected pixels of the Original image [11]. The main advantage of this method is that it is easily performed on images. The steps used to embed the watermark in the original image by using the LSB [12]:

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.

Patchwork Techniques

Patchwork is an excellent watermarking algorithm for images [18]. Bender et al. proposed the core idea. This algorithm embeds a special statistic into a original image. The two major steps in the algorithm are: (i)

choose two patches Pseudo-randomly and (ii) add the small constant value to the sample values of one patch and subtract the same value from the sample values of another patch.

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 used for the signal processing. It converts a signal from the spatial domain to the frequency domain. DCT is applicable in many fields like data compression, pattern recognition and every field of image processing. DCT watermarking is more robust than the spatial domain watermarking techniques. The main steps which used in DCT [13]

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. Embedded watermark by modifying the selected Co- efficient. 6) Apply inverse DCT transform on each block.

Discrete Fourier Transformation (DFT) based technique

Discrete Fourier Transform (DFT) provides robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT dissolve an image in sine and cosine form. The DFT based watermark embedding techniques are divided in to two types: (i) direct embedding and (ii) template based embedding.DCT uses just real numbers, while DFT uses complex numbers.

Discrete wavelet transform (DWT) based technique

Discrete wavelet transform (DWT) of the image produces multi resolution representation of an image. DWT divides the image into high frequency and low frequency quadrants. The low frequency quadrant is again split into two more parts of high and low frequencies and this process is repeated until the signal has been entirely degraded. The single DWT transformed two dimensional image into four parts: one part is the low frequency of the original image, the top right contains horizontal details of the image, the one bottom left contains vertical details of the original image, the bottom right contains high frequency of the original image. The low frequency coefficients are more robust to embed watermark because it contains more information of the original image [3].The reconstruct of the original image from the degraded image is performed by IDWT [14]. The digital wavelet transform are scalable in nature and it is not robust to geometric transformations.

IV.APPLICATIONS OF DIGITAL WATERMARKING

Watermarking technologies is applied in various digital media where security and owner identification is needed [15]. A few most common applications are listed hereby

Copyright protection: Digital watermarking can be used to identify and protect copyright ownership. Digital content can be embedded with watermarks identifying the copyright owners.

Copy protection: Illegal copying is also prevent by watermarking with copy protect bit. This protection requires copying devices to be integrated with the watermark detecting circuitry.

Digital right management: Digital right management (DRM) can be defined as the description, identification, trading, protecting, monitoring, and tracking of all forms of usages over tangible and intangible assets‖. It concerns the management of digital rights and the enforcement of rights digitally.

Tamper proofing: Digital watermarks which are fragile in nature, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content.

Broadcast monitoring: Over the last few years, the number of television and radio channels delivering

content has notably expanded. And the amount of content flowing through these media vehicles continues to grow exponentially. In this highly fragmented and fast changing market, knowing the real broadcast reality has become critical for content owners, copyright holders, distributors and broadcasters.

Fingerprinting: Fingerprints are the characteristics of an object that tend to distinguish it from other small objects. As in the applications of copyright protection, the watermark for finger printing is used to trace authorized users who violate the license agreement and distribute the copyrighted material illegally. Thus, the information embedded in the content is usually about the customer such as customer's identification number.

Access control: Different payment entitles the users to have different privilege (play/copy control) on the object. It is desirable in some systems to have a copy and usage control mechanism to prevent illegal copy of the content or limit the number of times of copying. A robust watermark can be used for such purpose.

Medical application: Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster.

Image and content authentication: In an image authentication application the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences. A solution to this problem could be borrowed from cryptography, where digital signature has been studied as a message authentication method. One example of digital signature technology being used for image authentication is the trustworthy digital camera.

Annotation and privacy control: Multi-bit watermarking can be used to annotate an image. For example, patient records and imaging details related to a medical image can be carefully inserted into the image. This would not only reduce storage space but also provides a tight link between the image and its details. Patient privacy is simply controlled by not keeping the sensitive information as clear text in human readable form, and the watermark can be further secured by encryption. Other usages of annotation watermarking are electronic `document indexing and automated information retrieval.

Media forensics: Forensic watermark applications enhance a content owner's ability to detect and respond to misuse of its assets. Forensic watermarking is used not only to gather evidence for criminal proceedings, but also to enforce contractual usage agreements between a content owner and the people or companies with which it shares its content.

Communication enhancement: Today's smart phones are becoming the handheld computing device we carry with us 24/7 — no longer are they merely for talking or texting. More and more we look to our mobile phones to provide us with assistance, instant information, and to entertain us.

Content protection for audio and video content: Modern digital formats employed for sale or rental of commercial audio and video content to consumers-such as DVD, Blue-Ray Disc, and iTunes-incorporate content protection technologies that control access to and use of the content and limit its unauthorized copying and redistribution. Parties seeking to engage in unauthorized distribution and copying of protected commercial music or video content must circumvent the content protection to obtain a decrypted copy of the content.

Table II. Comparisons of Different Watermarking Techniques

TECHNIQUES	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.
Patchwork	1.High level of robustness against most type of attacks.	1.It can hide only a very small amount of information.

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 quantizations tep.
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	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.

V.PEROFORMANCE EVALUATION & ATTACKS

Attacks:

There are so many threats for watermarking (Image) by which this process needs protected every time. As the watermarking techniques developed by researchers, hackers are developed new methods to attacks to destroy watermark. So every time algorithms need to be more robust for preventing attacks [16]. A few of the more obvious attacks are [17]:

- Image Compression - Lossy compression can result in the destruction of an image's watermark.
- Geometric transformations - the rotation, translation, sheering, or resizing of an image.
- Image Enhancements - Sharpening, colour calibration, contrast change.
- Image Composition - The addition of text, windowing with another image, etc.
- Information Reduction - Cropping
- Image filtering and the introduction of noise.
- Digital-to-analog conversion In addition some sophisticated attacks are:
- Multiple watermarking – add second watermark to image that creates a problem of validating the owner information.
- Collusion attacks - Multiple receiving of the same host image.
- Forgery - Multiple recipients of different images

Performance Metrics:

Mean square error (MSE)

The mean squared error (MSE) in an image watermarking is to estimate or measures the average of the squares of the "errors", between host image and watermark image [17].

$$MSE=\frac{1}{\square}[\Sigma \quad \Sigma \quad (\square(i,j)-\square(i,j)))^{\wedge}2] \qquad (1)$$

Where

X and Y are height and width respectively of the image.

The c(i,j) is the pixel value of the cover image and e (i, j) is the pixel value of the embedded image.

Peak signal to noise ratio (PSNR)

PSNR (Peak Signal to Noise Ratio) is used to determine the Efficiency of Watermarking with respect to the noise. The noise will degrade the quality of image. The visual quality of watermarked and attacked images is measured using the Peak Signal to Noise Ratio [5]. It is given by P

$$PSNR=10.\square_{10}(\frac{\square\square\square\square^2}{\square\square\square\square}) \qquad (2)$$

Where

MAXi represents the maximum possible pixel value of the image and when the pixels are represented using 8 bits per sample, this is 255. The extraction fidelity NC which is given by:

$$NC=\frac{\sum_i \sum_j RW(i,j)\, EW(i,j)}{\sqrt{\sum_i \sum_j RW(i,j)^2}\,\sqrt{\sum_i \sum_j EW(i,j)^2}} \quad (3)$$

Where
RW is the Reference watermark
EW is the extracted watermark

REFERENCES

[1] R.G. Schyndel, A. Tirkel, and C.F Osborne, ―A Digital Watermark‖, Proceedings of IEEE International conference on Image Processing, ICIP-1994, pp. 86-90, 1994.

[2] Christine I. Podilchuk, Edward J. Delp, ―Digital watermarking: Algorithms and applications‖, IEEE Signal processing Magazine, July 2001.

[3] N. Tiwari, M. k. Ramaiya and Monika Sharma, "Digital watermarking using DWT and DES", IEEE (2013).

[4] L. Li and X. Li," Watermarking Protocol for Broadcast Monitoring", International Conference on E business and E-Government (ICEE) (2010).

[5] D. Zhang, S. Xu, Y. Wang, J. Zhang and Y. Li, "A Digital Fingerprinting Scheme of Digital Image". International Conference on Computational Intelligence and Software Engineerin (CISE) (2010).

[6] S. Emmanuel, A. P. Vinod, D. Rajan and C.K. Heng, "An Authentication Watermarking Scheme with Transaction Tracking Enabled", Digital Ecosystem and Technologies Conference, 2007.DEST'07 Inaugural IEEE-IES.

[7] Y.-C. Wang and J.-f. Niu, "Research on Digital Content Copyright Protection System", IEEE International Conference on Network Infrastructure and Digital Content, 2009. IC-NIDC (2009).

[8] S.-L. Hsieh, C.-P. Yeh and I-J. Tsai, "An Image Copyright Protection Scheme with Tamper Detection Capability", Symposia and Workshops on Ubiquitous, Autonomic and trusted Computing,2009.UIC-ATC'09

[9] Z. Ni, Y.Q. Shi, N. Ansari, W. Su, Q. Sun and X. Lin, "Robust Lossless Image Data Hiding Designed for Semi- Fragile Image Authentication", IEEE Transactions on Circuits and Systems for Video Technology, vol. 18, no. 4.

[10] J. Zhu, Q. Wei, J. Xiao and Y. Wang," A Fragile Software Watermarking Algorithm for Content Authentication", IEEE Youth Conference on Information, Computing and Telecommunication, 2009.YCICT'09.

[11] 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.

[12] D. Mistry," Comparison of Digital Watermarking Methods" (IJCSE) International Journal on Computer Science and Engineering, vol. 02, no. 09, (2010), pp. 2805- 2909.

[13] V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).

[14] S. S. Gonge and J. W. Bakal, "Robust Digital Watermarking Techniques by Using DCT and Spread Spectrum", International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084, vol. 1, no. 2, (2013)

[15] Mei Jiansheng, Li Sukang, "A Digital Watermarking Algorithm Based On DCT and DWT", Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107

[16] Chunlin Song , Llewellyn-Jones, "Analysis of Digital Image Watermark Attacks", Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE

[17] Scott McCloskey, "Hiding Information in Images: An Overview of Watermarking", Cryptography Research Paper ,11-9-2000

[18] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Syst. J., vol. 35, no. 3/4, pp. 313–336, 1996.