ISSN No:-2456 – 2165

A Review on Different Digital Watermarking Techniques

Vasudha B. Sankpal[1], Prof.R.N.Patil[2]
[1]Student, Department of Electronics Engg, DKTE's Textile and Engineering Institute, Ichalkarnji, Maharashtra
[2]Assistant Professor, Department of Electronics Engg, DKTE's Textile and Engineering Institute, Ichalkarnji, Maharashtra
vasudhasankpal12@gmail.com[1], rnpatil@dktes.com[2]

Abstract—Now a days it is very easy to use digital information available on internet because of the fast development in Information Communication Technology (ICT) sector. To provide facility of data authentication, security and copyright protection of digital media the technology being developed is a Digital Watermarking. For text or image, audio, video digital watermarking can be applied. In this paper it is focused only on image watermarking. In general, watermark can be embedded in transform domain or spatial domain technique of an image. A review of various watermarking techniques is presented in this paper. The paper also includes definition of watermarking features, requirements and performance of various watermarking techniques.

Keywords—DigitalWatermarking, Techniques,DCT,,DWT ,SVD.

I. INTRODUCTION

The rapid growth of internet technology increased, also exchange and transmission of digital information increased, the prevention of tampering and illegal distribution of the digital data is becomes very essential. Digital watermarking one of the techniques used to achieve copyright protection and authenticity of digital data. Digital watermarking is the process of hiding a data associated to a digital signal (i.e. video, song, and image) inside the signal itself. It tries to hide a message associated to the actual content of the digital signal [1].Digital Watermarking has several applications such as Broadcast Monitoring, Owner Identification, Proof Ownership, Transaction Tracking and Content Authentication [2] [3].It has become a very important to study about information hiding. Watermarking consists of two modules; watermark embedding module and watermark detection & extraction module .These two modules are same for all types of watermarking techniques. Fig 1. Shows the watermark embedding process in which the watermark is embedded on the cover image by using the embedding algorithm and the embedded watermark is recovered by using detection algorithm is as shown in Fig 2.watermark detection process. This paper shows the core technologies of digital watermarking and explores the application in the digital image. The paper is structured as follows: Section II describes the various watermarking techniques. Section III describes the Features and requirements .Section IV describes the various parameters used to evaluate the performance of watermarked image and watermarking applications. Section V is the Conclusion.

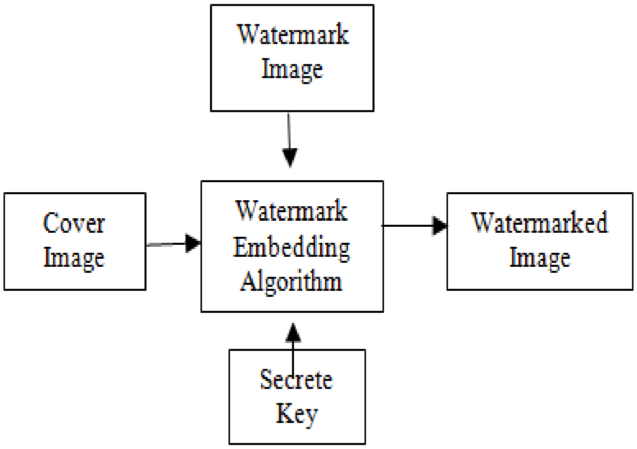


Fig.1: Watermark Embedding Process

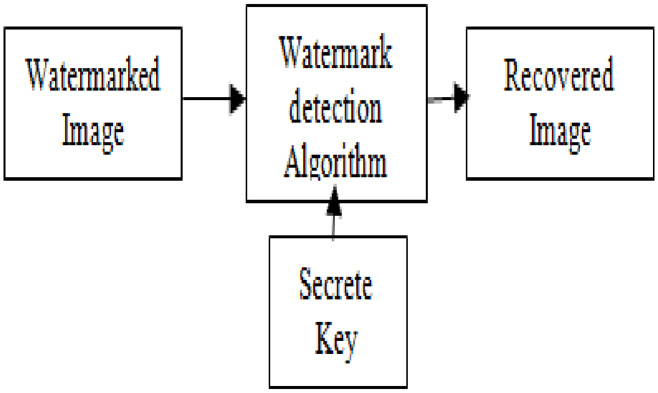


Fig. 2: Watermark Detection Process

II. WATERMARKING TECHNIQUES

The watermarking techniques fall into two categories as shown in Fig 3. Spatial - Domain methods and Frequency Transform Domain methods [4] [5]. In Spatial Domain, it directly handles digital data to hide the watermark. Its main advantage is low computational complexity.

However, this method is susceptible to various attacks. In frequency domain, data to be protected are changed into a frequency domain. It needs more computation as compared to spatial domain methods but it can provide better robustness from different attacks [6].

According to differentiation, the watermarking system can be classified as Blind, Semi-Blind and Non-Blind [7].

Blind:
The Blind watermarking scheme is called as public:

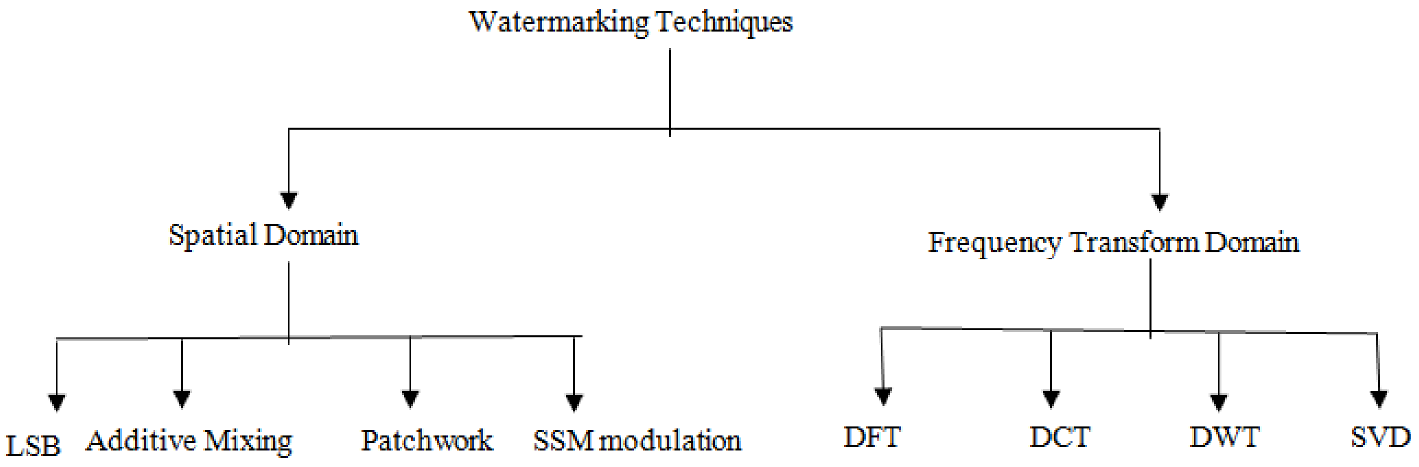


Fig.3: Classification of Watermarking Techniques

The watermark may be spread throughout the image or Watermarking scheme. The most challenging type of watermarking system is blind watermarking as it does not requires the cover (original data), or the embedded watermark , n bits of the watermark data is extracted from the watermarked data (i.e. the watermarked image) by this system.

Semi-blind:
It is called as semi-private watermarking scheme. This system does not need original data for detection.

Non-Blind:
It is also known as private watermarking scheme. This system requires at least original data for detection. The System extracts the watermark from the possibly distorted data and uses the original data as a hint.

A. Spatial Domain Watermarking Methods:

a). Additive Watermarking:
To add pseudo random noise pattern to the intensity of image pixels is the most straight forward method to embed the watermark in spatial domain. The noise signal is floating point numbers or usually integers like (-1, 0, 1).To ensure that the watermark can be noticed, the noise is made by a key, such that the relationship between the numbers of different keys will be very low [8].

b). Least Significant Bit:
Least Significant Bit [16] is a spatial domain technique which is a very simple and straight forward method. The least significant bits of the original image is used to embed the watermark. It requires very less time to embed image (watermark). This technique has many drawbacks, a simple attacks can destroy or remove watermark but sometime it may survive against some of the transformations. Recently some of improvements on LSB substitution suggested like embed watermark at single bit rate, multi bit rate or using a pseudo-random number generator. Pixel can also be selected with help of key. Performing loss in compression and addition of noise [17] can easily degrade the image quality or remove or disrupt or destroy watermark.

It lacks the basic strength. In case, if the algorithm is discovered, it becomes very easy for attacker to modify or remove watermark.

c). SSM Modulation Based Technique:
In this technique the least significant bits are used for embedding watermarks. This method is robust against different attacks and is very easy for implementation. By

selecting a group of pixels the embedding operation is performed and replaces this selected group with the pixels of watermarks. But this technique does not stand for common signal processing attacks and is not suitable for practical applications.

d). Texture mapping coding Technique:

It is useful for those images which have some texture part in it. In this method the watermark embedded in the texture part of the image. This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage) [9], and cannot be done automatically. This method hides data in the continuous random texture patterns of a picture.

e). Patchwork Algorithm:

Patchwork is a data hiding method proposed by Bender et al and published on IBM Systems Journal, 1996[10]. 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).

B. Frequency Domain Watermarking Methods:

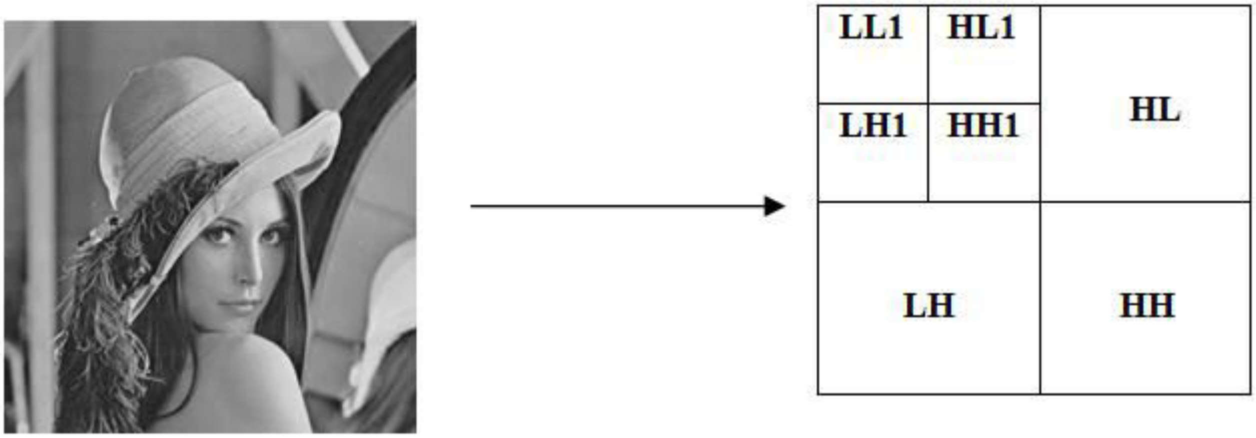
These methods are more widely applied than others. The characteristics of the human visual system (HVS) are better captured by the spectral coefficients [11] ,so frequency domain method is popularly used for watermarking. That is human eye is less sensitive against high frequency component and more sensitive against low frequency component. The most commonly used transformations are Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier Transform (DFT). Some of its main algorithms are discussed below:

a). Discrete Cosine Transforms (DCT):

DCT is a Fourier Transform; it represents data in terms of frequency space rather than an amplitude space. Compared to spatial domain techniques DCT based watermarking techniques are more robust. Such algorithms are robust against simple image processing operations like low pass filtering, blurring, brightness and contrast adjustment, etc. However, they are very difficult for implementation and are more expensive. Along with this, they are weak against Geometric attacks like scaling, rotation, cropping etc. DCT domain watermarking can be classified into Block based DCT watermarking and Global 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.

b). Discrete Wavelet Transforms (DWT):

The multi resolution representation of an image is produced by discrete wavelet transform (DWT) of the image.



a) Host image b) DWT Transform

Fig.4: Two Level Decomposition

The multi resolution representation provides a simple framework for interpreting the image information. The DWT analyses the signal at multiple resolution. DWT divide the image into low frequency quadrants and high frequency quadrants .The low frequency quadrants is again split into two more parts of low and high frequencies and this process is repeated until the signal is entirely decomposed. The signal 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 original image. The low frequency coefficients are more robust to embed watermark because it contains more information of original image [12].The reconstruct of the original image from the decomposed image is performed by IDWT. The digital wavelet transform are scalable in nature. DWT more frequently used in digital image watermarking because of excellent spatial localization and multi resolution techniques. To recognize the area in the cover image in which the watermark is embedded efficiently the excellent spatial localization property is very convenient.

The DWT is applied on host image to decompose the image into four non overlapping multi resolution coefficients is as shown in Fig 4.

And then the detector is used to extract the embedded spread spectrum watermark [13] The DFT is used for the periodic digital signal or discrete-time f(x).

c). Discrete Fourier Transforms (DFT)

Discrete Fourier Transforms (DFT) offers robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT decomposes an image in sine and cosine form .The DFT based watermark embedding techniques are divided in two types: one is the direct embedding technique and the other one is the template embedding.

By modifying DFT magnitude and phase coefficients the watermark is embedded in direct embedding technique. The concept of templates is introduced by template based embedding technique. In DFT domain a template is structure which is embedded to estimate the transformation factor. Once the image undergoes a transformation this template is searched to resynchronize the image, And then the detector is used to extract the embedded spread spectrum watermark [13] The DFT is used for the periodic digital signal or discrete-time f(x).

d). Singular Value Decomposition (SVD):

Singular Value Decomposition transform is a linear algebra transform which is used for factorization of a real or complex matrix. Which has numerous applications in various fields of image processing? As a digital image, can be represented in a matrix form with its entries giving the intensity value of each pixel in the image, SVD of an image M with dimension in mxm is given by.

$$M=U*S*V^T \qquad \text{Eqn. 1}$$

Where, U and V are orthogonal matrices and S is called as singular matrix is a diagonal matrix which carries non-negative singular values of matrix M. The columns of U and V are call left and right singular vectors of M, respectively. They basically specify the geometry details of the original image. Left singular matrix, i.e. V represents the vertical details of the original image, i.e.,U represents the horizontal details and right singular matrix, The diagonal value of Matrix S is arranged in decreasing order which shows that importance of the entries is decreasing from the first singular value for the last one, this feature is working in SVD based compression methods. [15] There are two main properties of SVD to employ in digital watermarking scheme.

- Small Variation in singular values does not affect the quality of image and
- Singular Values of an image have high stability so; they don't change after various attacks.

III. FEATURES AND REQUIREMENTS

A. Features of Digital watermarking Invisible/Inaudible

Information is embedded without digital content degradation, because of the level of embedding operation is too small for human to notice the change.

a). Inseparable

The embedded information can survive after some processing, compression and format transformation.

b). Unchanging Data File

Information is embedded directly into the media due to which data size of the media is not changed before and after embedding operation.

B. Requirements of Digital watermarking

A watermark can exhibit a number of important characteristics. The most important properties of digital watermarking techniques are transparency, robustness, security, capacity, invert ability (reversibility) and complexity and possibility of verification. Transparency relates to the properties of the human sensory. A transparent watermark causes no artifacts.

a). Robustness:

Watermarked in image should survive basic image processing operation such as contrast or brightness enhancement, gamma correction etc.

b). Perceptual transparency:

The algorithm must embed data without affecting the perceptual quality of the underlying host signal.

c). Security:

A secure data embedding procedure cannot be broken unless the unauthorized user access to a secret key that controls the insertion of the data in the host signal.

d). Complexity:

This is important property considering in Real time applications like video. Complexity property is concerned with amount of effort needed to extract or retrieve the watermark from content.

e). Capacity:

This factor shows the maximum amount of data, which can be embedded into an image without noticeably reducing image quality. The influence of capacity on the robustness and imperceptibility of watermarked image is not negligible; for instance, by increasing the data payload, the robustness will decrease and the Imperceptibility will increase.

Capacity requirement always struggle against two other important requirements, that is, imperceptibility and robustness (Fig 5). A higher capacity is usually obtained at the expense of either robustness strength or imperceptibility, or both.

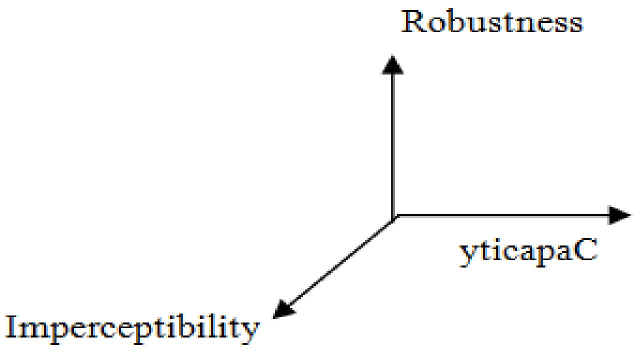


Fig 5: The Tradeoffs among Imperceptibility, Robustness, and Capacity

f). Imperceptibility:
This factor is about the amount of distortion that appears on a watermarked image after inserting a watermark. For invisible watermarks, this factor should be low.

g). Reliability:
To ensure that the project application returns the correct watermark each time. In spite of the loss of watermarking information by the optimizer, we should always be able to obtain correct and accurate results from the project.

IV. PERFORMANCE PARAMETERS

- *Peak Signal to Noise Ratio (PSNR)-*

It measures the similarity between images before and after watermarking. PSNR is defined in the following way:

$$\mathrm{PSNR} = 10\mathrm{Xlog}_{10}\frac{\mathrm{max}^2}{\mathrm{MSE}}\ \mathrm{dB} \qquad \mathrm{Eqn.\,2}$$

- *Mean Squared Error (MSE)-*

It is simplest function to measure the perceptual distance between watermarked and original image. MSE can be defined as:

$$\mathrm{MSE} = \frac{1}{\mathrm{mn}}\sum_{\mathrm{i}}^{\mathrm{m}}\sum_{\mathrm{j}}^{\mathrm{n}}(\mathrm{H}_{\mathrm{i,j}} - \mathrm{H'}_{\mathrm{i,j}})^2 \qquad \mathrm{Eqn.\,3}$$

Where,

m and n are height of the image
$\mathrm{H}_{\mathrm{i,j}}$ is the pixel value of cover image.
$\mathrm{H'}_{\mathrm{i,j}}$ is the pixel value of embed image.

- *Normalized Cross Correlation (NC)-*

Normalized Cross Correlation (NC) can be used to evaluate the robustness of the watermarking method.

- *Bit error ratio(BER)-*

The difference between the original image and watermarked images is manipulated using the Bit- Error-Rate (BER).

.

$$\mathrm{BER} = \frac{1}{\mathrm{PSNR}} \qquad \mathrm{Eqn.\,4}$$

A. Applications of Digital Watermarking

a). Copyright protection - Watermarking can be used to protect digital material distributed on internet to verify the ownership of material.
b). Content Achieving - It can hide identity of digital material such as image, video, audio etc. within its material reduce possibility of tempering it.

c). Mete-data insertion - Meta-data is the data that describe the data. This data can be inserted using watermarking such as audio file can carry singer name or video file carry the subtitle.

d). Broadcast monitoring - Broadcast monitoring refers to the technique of cross verifying whether the content that was supposed to be broadcasted has really been broadcasted or not.

e). Tamper detection - Data transfer over internet can be tamper or alter by other party which is detect by watermarking.
f). Medical Applications: digital watermarking provide both confidentiality and authentication without affecting the medical data.

V. CONCLUSION

This paper gives a detailed study on various digital water marking techniques spatial domain and transform domain (DCT, DWT, DFT) and their applications. We have presented various aspects of digital watermarking like overview, techniques and requirements. Apart from it a brief analysis of watermarking techniques is presented which can help the new researchers in related area.

We tried to provide the comprehensive information regarding the digital watermarking which will assist the new researchers to acquire the maximum knowledge in this domain.

REFERENCES

[1]. M. Durvey and D. Satyarthi, "A Review Paper on Digital Watermarking," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 3, no. 4, pp. 99-105, 2014.

[2]. Cox, M. L. Miller and J. A. Bloom, "Digital Watermarking," Morgan Kaufmann Publishers, 2002.

[3]. R. G. Schyndel, A. Z. Tirkel and C. F. Osborne, "A Digital Watermark," in Proceedings of 1994 International Conference, Austin, Texas, 1994.

[4]. H. Daren, L. J. H. Jiwu and L. Hongmei, "A DWT Based Image Watermarking Algorithm," in Proceedings of the IEEE International Conference on Multimedia and Expo, 2001.

[5]. M. Barni, F. Bartolini, V. CappeAini and A. Piva, "A DCT-Domain System for Robust Image Watermarking," Vols. 66, No.3, pp. 357-372, 1998.

[6]. S. Madhesiya and S. Ahmed, "Advanced Technique of Digital Watermarking based on SVD-DWT-DCT and Arnold Transform," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vols. 2, No 5, May 2013.

[7]. H. Jahankhani, D. L. Watson, G. Me and F. Leonhardt, "Authentication," in Handbook of Electronic Security and Digital Forensics, Singapore, World Scientific Publishing Co. Pte. Ltd, 2010, p. 40.

[8]. CHAPTER 2: LITERATURE REVIEW, Source: Internet Jiang Xuehua, ―Digital Watermarking and Its Application in Image Copyright Protection‖, 2010 International Conference on Intelligent Computation Technology and Automation.

[9]. http://ippr-practical.blogspot.in

[10]. Manpreet kaur, Sonia Jindal, Sunny behal, ―A Study of Digital image watermarking‖, Volume2, Issue 2, Feb 2012.

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

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

[13]. Manpreet kaur, Sonia Jindal, Sunny behal, ―A Study of Digital image watermarking‖, Volume2, Issue 2, Feb 2012.

[14]. N. Bisla and P. Chaudhary, "Comparative Study of DWT and DWT-SVD Image Watermarking Techniques," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 6, pp. 821-825, 2013.

[15]. D. Samanta, A. Basu, T. S. Das, V. H. Mankar, Ankush Ghosh, Manish Das and Subir K Sarkar, SET Based Logic Realization of a Robust Spatial Domain Image Watermarking," Proc. in 5th International Conference on Electrical and Computer Engineering-ICECE 2008, Dhaka, Bangladesh, pp. 986-993, Dec. 2008.

[16]. J. L., Dugelay, S. Roche, C. Rey, G. Doërr, "Still-image watermarking robust to local geometric distortions," IEEE Trans. on Image Proc., vol. 15, no. 9, pp. 2831- 2842, 2006.

[17]. Dhanalakshmi and Dr.T.Ravichandran, "A SURVEY OF WATERMARKING PROCESS," S. Dhanalakshmi et al. / IJAIR Vol. 2 Issue 2 ISSN: 2278-7844. [5] Mr. Gaurav N Mehta, Mr. Yash Kshirs.