ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Survey of Digital Watermarking Techniques

Ashwini.R
Student,
Department of ECE,
BMSCE (Autonomous Under VTU),
Bangalore.

Geethanjali.C
Student,
Department of ECE,
BMSCE (Autonomous Under VTU),
Bangalore.

Lakshmi
Student,
Department of ECE,
BMSCE (Autonomous Under VTU),
Bangalore.

Manjula.R
Student,
Department of ECE,
BMSCE (Autonomous Under VTU),
Bangalore.

Dr. A.Meera
Professor,
Department of ECE,
BMSCE (Autonomous Under VTU),
Bangalore.

Abstract:

This paper presents a review on different digital watermarking techniques and their properties. Also describes few techniques to achieve robustness. The main reason for development of digital watermarking research is to protect intellectual properties and copyright protection of the digital world. The digital watermarking is a field of information which hides the crucial information in the original data for protection against illegal duplication, distribution and ownership rights of the multimedia data. The embedded information can't be detected by human eye but some attacks and operations can damage that information to breach protection. The effectiveness of digital watermarking technique is indicated by the robustness of embedded watermarks against various attacks.

Keywords:
Digital watermarking, spatial domain, Transform domain, Encryption, Decryption, Attacks.

1.Introduction:

Digital image processing is a rapidly developing area with various applications. It is very important field for the research work because its techniques are used in almost all kinds of task like human computer interface,Medical visualisation, image enhancement, law enforcement, artistic effects, image restoration and digital watermarking for security purposes [6]. There are many approaches like Cryptography, Watermarking and Steganography to transfer the data/image to the intended user at destination without any modification. Watermarking is a secondary image which is overlaid on the primary image, and provides a means of protecting the image.

Digital Watermarking is a method used to improve the ownership over image by replacing low level signal directly into image. The Digital Watermarking method is also used for the authentication, copy prevention, broadcast monitoring and data hiding [12].

2.DIGITAL IMAGE WATERMARKING WORKING:

Digital Watermarking is a technique which is used in digital signal processing by embedding hidden information into multimedia data. This information is not usually visible, only dedicated detector or extractor can see and extract that information. Digital Image Watermarking uses digital image for embedding the hidden information, after embedding the watermarked image is generated which is more robust against attacks. Basically working of Digital Image Watermarking can be divided in three stages [6].

2.1 Embedding Stage:

The embedding stage is the first stage in which the watermark is embedded in the original image by using the embedding algorithm. Then the watermarked image is generated which is transmitted over the network[6].

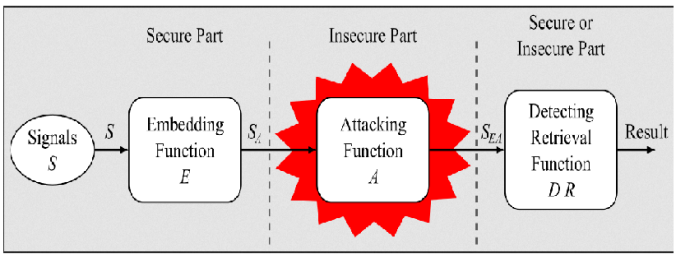
2.2 Attack Stage:

In this stage, when the data is transmitted over the network either some noise is added to the watermarked image or watermarked image is affected by some attacks, which causes watermarked data to be either modified or destroyed[6].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

2.3 Detection Stage:

In the detection stage, watermark is detected or extracted by the authorised detector from the watermarked image by applying some detection algorithm[6].



3. Attributes of Digital Watermarking:

An effective image watermarking algorithm must have the following features [8]:

a)Imperceptibility: The watermark must be imperceptible, i.e. the perceived quality of the watermarked image should not be noticeable.

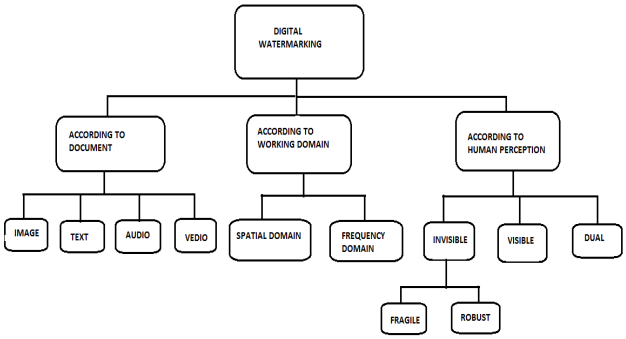
b)Robustness: The watermark should be difficult, rather impossible, to remove or to degrade, intentionally or unintentionally, by image processing attack.

c)Low computational complexity: The watermarking algorithm should not be computationally complex for embedding as well as extracting the watermark, especially for real time applications.

4.WATERMARKING TECHNIQUE:

Watermarking is an efficient method to hide the secret information into the digital media using some appropriate algorithm. Algorithm plays a vital role in Watermarking as, if the used watermarking technique is efficient and strong then the watermark being embedded using that technique cannot be easily detected.

The attacker can only detect or destroy the secret information only if he knows the algorithm otherwise it is critical to know the watermark. There are various algorithms present in the today scenario that are used to hide the information [1].



4.1.ACCORDING TO DOCUMENT:

a)Image watermarking: This is used to hide the special information into the image and to later detect and extract that special information for the author‘s ownership.

b)Video watermarking: This adds watermark in the video stream to control video applications. It is the extension of image watermarking. This method requires real time extraction and robustness for compression.

c)Audio watermarking: This application area is one of the most popular and hot issue due to internet music, MP3.

d)Text watermarking: This adds watermark to the PDF, DOC and other text file to prevent the changes made to text. The watermark is inserted in the font shape and the space between characters and line spaces [2].

4.2.ACCORDING TO WORKING DOMAIN:

4.2.1 Spatial Domain Watermarking:

The spatial domain represents the image in the form of pixels. The spatial domain watermarking embeds the watermark by modifying the intensity and the colour value of some selected pixels. 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. The spatial domain techniques can be easily applied to any image. The most important method of spatial domain is LSB. The spatial domain watermarking is easier and its computing speed is high than transform domain but it is less robust against attacks. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression [6].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

a)Least Significant Bit (LSB) Technique:

This method is one of the simplest to implement. It involves adding the watermark signal to the lowest order bit of each pixel. The detection method is just as simple as the embedded method. The last bit of each pixel is read, in turn, to disclose the watermark data. The extent of the image degradation depends on how many of the lower order bits are used. The advantage of this method is that even if a part of the watermarked image is cropped the receiver can still get the required message, as the message is embedded a number of times. This technique doesn't show robustness to watermarked image [4].

b)Patchwork technique:

It is basically a pseudo random, 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). Patchwork being statistical methods uses redundant pattern encoding to insert message within an image [4].

c)Predictive Coding Scheme:

In this method the correlation between adjacent pixels are exploited. A set of pixels where the watermark had to be embedded are chosen and alternate pixels were replaced by the difference between the adjacent pixels. This was further improved by adding a constant to all the differences. A cipher key was created which enabled the retrieval of the embedded watermark at the receiver. This was much more robust when compared to LSB [4].

d)SSM Modulation Based Technique:

Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded Watermark [4].

e)Texture mapping coding Technique:

This method is useful in only those images which have some texture part in it. This method hides the watermark in the texture part of the image. This algorithm is only suitable for those areas with large number of arbitrary texture images (disadvantage), and cannot be done automatically. This method hides data within the continuous random texture patterns of a picture [4].

f)Correlation-Based Technique:

In this technique, a pseudo random noise (PN) pattern says W(x, y) is added to cover image I(x, y).

$$Iw(x, y) = I(x, y) + k*W(x, y)$$

Where,

K represents the gain factor,

Iw represent watermarked image ant position x, y and I represent cover image.

Here, as we increase the gain factor then although it increases the robustness of watermark but the quality of the watermarked image will decrease [4].

g)Frequency-domain techniques (spectral watermarks):

The frequency-domain techniques modify the values of some transformed coefficients. The frequency domain technique first transforms an image into a set of frequency domain coefficients. The watermark is then embedded in the transformed coefficients of the image such that the watermark is invisible and more robust for some image processing operations. Finally, the coefficients are inverse transformed to obtain the watermarked image [4].

4.2.2 DFT (Discrete Fourier Transform):

Discrete Fourier Transform (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 and the other one is the template based embedding.According to the direct embedding technique the watermark is embedded by modifying DFT magnitude and phase coefficients, while in the template based embedding technique it introduces the concept of templates. A template is structure which is embedded in the DFT domain to estimate the transformation factor.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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. The output of the DFT is always in complex value and it requires more frequency rate. Its computational efficiency is very poor. So, the DFT not used because of these disadvantages.[9]

4.2.3 DCT (Discrete Cosine Transform):

A DCT based information hiding system was proposed in which the image was first segmented into non-overlapping blocks of 8x8 and forward DCT was applied to each of the block [8]. After that a selection criteria was applied followed by applying coefficient selection criteria. The watermark was embedded by modifying the selected coefficients and the final watermarked image was obtained by applying, Most of the energy in the DCT domain is concentrated in the low frequencies. As is known low frequencies are perceived very well by human eye, hence the chances of the watermark being perceptible was high where as high frequencies are prone to attacks such as compression and scaling. Thus the middle frequency bands were chosen such that they avoid the most visual important parts of the image without over-exposing themselves to removal through compression and noise attacks [9].

4.2.4 DWT (Discrete wavelet transform):

Discrete wavelet transform (DWT) of the image produces multi-resolution representation of an image. The multi-resolution representation provides a simple framework for interpreting the image information. The DWT analyses the signal at multiple resolution. As most of the energy is concentrated in the approximation (LL) sub band having low frequency sub bands, any change in these low frequency sub bands would cause a severe degradation of image. As the human eyes are not sensitive to high frequency sub bands, the secret information is embedded in either vertical, horizontal or diagonal (LH, HL or HH respectively) sub bands. 1-level DWT alpha blending technique was proposed which embeds the invisible watermark into the salient features of the original image using Daubeche in wavelets. In this approach the decomposed components of both the images were multiplied by a scaling factor and then added. Extraction of watermark was dependent only on the values of the scaling factors k and q.

The digital wavelet transform are scalable in nature. DWT more frequently used in digital image watermarking because of its excellent spatial localization and multi resolution techniques. The excellent spatial localization property is very convenient to recognize the area in the cover image in which the watermark is embedded efficiently [11].

4.3.ACCORDING TO HUMAN PERCEPTION:

4.3.1 Visible:

The watermark is visible which can be a text or a logo used to identify the owner. Any text or logo to verify or hide content[3].

$$Fw= (1-a) F+ a*W$$

Where,
Fw = Watermarked Image,
a =constant; 0<=a<=1, IF a=0 No watermark,
if a=1 watermark present
F =original image
W =watermark

4.3.2 Invisible:

The watermark is embedded into the image in such a way that it cannot be perceived by human eye. It is used to protect the image authentication and prevent it from being copied. Invisible watermark can be further divided into two types[3]:

a)Robust Watermark: It aims to embed information in a file that cannot be easily destroyed. They are designed to resist any manipulations that may be encountered. All applications where security is the main issue uses robust watermarks.

b)Fragile Watermark: They are designed with very low robustness. They are used to check the integrity of objects.

4.3.3 Dual watermarking:

This technique is a combination of visible and invisible watermark. It contains both visible and invisible watermark inside the cover [3].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

5.Overview of Attacks on Watermarking:

Attacks are the factors or processes that can degrade the digital watermark strength. Attacks can be broadly classified into these main categories.
1. Removal Attacks
2. Geometric Attacks
3. Cryptographic Attacks
4. Protocol Attacks.

1. Removal Attacks:

These type of attacks affects the watermark in such a way that it completely or nearly removes or destroys watermark data. Example of these attacks are de-noising, quantization (e.g., for compression), remodulating, and collusion attacks.[12]

2. Geometric Attacks:

These types of attacks affects on the pixels of an image, like pixels shifting, scaling of image, rotation of image without any higher visual changes. The aim of these attacks is to degrade the quality of watermark.[12]

3. Cryptographic Attacks:

In these kinds of attacks the attackers find the loop holes in main embedding algorithm and remove the watermark information. Examples are brute force attack and oracle attack. But if the embedding algorithm is complex then these attacks are easily restricted.[12]

4. Protocol Attacks:

These attacks are intentionally done by attackers to change or destroy the ownership information from the watermarked image. Example of these attacks is copy attack and changing of watermark. Beyond these attacks there are many attacks continuously developed by hackers to affect the watermarking algorithms and watermark [12].

6.PERFORMANCE EVALUATION OF WATERMARKING ALGORITHMS:

Performance evaluation is very important part in the any algorithmic design in watermarking. The main task of this is to evaluate the quality matrices of algorithm or method to find out, how much it is effective. Some of the quality matrices an image watermarking method or algorithm are MSE and PSNR.

6.1 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[5].

$$MSE = 1 \div MN \sum_{i}^{M} \sum_{j}^{N} (Wij - Hij)\text{^}2$$

Where
M, N is pixel values in host image.
Wij= Pixel value in Watermarked Image.
Hij= Pixel value in Host Image.

6.2 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 Imperceptibility of image is determined by this factor. Higher PSNR shows that watermarked image is perceptible or watermark is not recognized by naked eyes.
PSNR = 10 log10 (L*L/MSE)
L is the peak signal value of the cover image which is equal to 255 for 8 bit images [5].

7.Comparative analysis on various techniques:

Watermarking 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	High level of robustness against most type of attacks.	It can hide only a very small amount of information.
DCT	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 quantization step. 3. DCT technique doesn't work with scaling attacks.
DWT	1. Allows good localization both in time and spatial frequency domain 2. Higher compression ratio which is relevant to human perception. 3. More robust to cropping. 4. It has multi resolution characteristics and is hierarchical. 5. DWT has effective also in structural attacks.	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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CONCLUSION:

Significant number of watermarking techniques can be found in the literature used in the variety of applications because of their advantages over the alternative methods. The overall study in this paper shows that the spatial methods are relatively fast and requires low resources and even they can provide comparable performance over scaling and additive noise attacks. On the other hand, frequency domain methods are computationally complex but performs exceptionally well in terms of robustness, pay load capacity, image operations and imperceptibility.

REFERENCES:

(1)Monika Patel, Priti Srinivas Sajja, Ravi K Sheth, "Analysis and Survey of Digital Watermarking Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, October 2013.

(2)Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, March 2013.

(3)Sasmita Mishra, Amitav Mahapatra,Pranati Mishra, " A Survey on Digital Watermarking Techniques", International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013.

(4)Barun Pandhwal, D.S. Chaudhari, "An Overview of Digital Watermarking Techniques", International Journal of Soft Computing and Engineering (IJSCE), Volume-3 March 2013.

(5)Lalit Kumar Saini, Vishal Shrivastava, "A Survey of Digital Watermarking Techniques and its Applications", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2, May-Jun 2014.

(6)Preeti Parashar, and Rajeev Kumar Singh, PG Scholar, "A Survey: Digital Image Watermarking Techniques", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6 (2014).

(7)Surya Pratap Singh, Paresh Rawat, Sudhir Agrawal, "A Robust Watermarking Approach using DCT-DWT", International Journal of Emerging Technology and Advanced Engineering ,Volume 2, August 2012.

(8)Nidhi H. Divecha, N. N. Jani. "Image Watermarking Algorithm using DCT, DWT and SVD", National Conference on Innovative Paradigms in Engineering & Technology (NCIPET-2012).

(9)Blossom Kaur, Amandeep Kaur, Jasdeep Singh, "Steganographic Approach for Hiding Image in DCT Domain", International Journal of Advances in Engineering & Technology, July 2011.

(10)Seema Malshe(Gondhalekar), Hitesh Gupta, Saurabh Mandloi,"Survey of Digital Image Watermarking Techniques to achieve Robustness", International Journal of Computer Applications Volume 45– No.13, May 2012.

(11)P. Bala Srinivas, B. Venkatesh, "Comparative Analysis of DWT, SWT, DWT&SWT and DTCWT-Based Satellite Image Resolution Enhancement", IJECT Vol. 5, Issue 4, Oct - Dec 2014.

(12)Namita Chandrakar, Jaspal Bagga, "Performance Comparison of Digital Image Watermarking Techniques", International Journal of Computer Applications Technology and Research Volume 2– Issue 2, 126 - 130, 2013.