ISSN: 2277-9655
Impact Factor: 4.116

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW OF IMAGE WATERMARKING METHODS

Ankush R. Patil*, V. K. Patil
[*] E & TC, M.E., D. N. Patel COE, Shahada, MH, India

DOI: 10.5281/zenodo.56916

ABSTRACT

Due to the recent progress in internet technology and evolution of very high speed networks operating everywhere, protection of digital content is must. So, it has become a tough task to protect copyright of an individual's creation. The purpose of digital watermarking is to incorporate concealed information in multimedia content to ensure a security amenity or simply a labeling application. This paper then categorizes the various watermarking techniques into numerous categories dependent upon the domain in which the concealed data is inserted. We have also provided the comparative analysis of these techniques that can help us to know the positive and negative of these techniques. This comparison can further be used to improvise and propose various new techniques for the same.

KEYWORDS:Watermarking, DCT, DWT, DFT, Spatial Domain, Steganography, Information hiding, Cryptography, LSB embedding, PSNR, MSE.

INTRODUCTION

In recent years, as digital media are gaining wider popularity, their security related issues are becoming greater concern. Digital watermarking is a technique which allows an individual to add copyright notices or other verification messages to digital media. Image authentication is one of the applications of digital watermarking, which is used for authenticating the digital images. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. The way to realize this feature is to embed a layer of the authentication signature into the digital image using a digital watermark. In the case of the image being tampered, it can easily be detected as the pixel values of the embedded data would change and do not match with the original pixel values. There are many spatial and frequency domain techniques available for authentication of watermarking. Watermarking techniques are judged on the basis of their performance on a small set of properties. These properties include robustness, transparency, watermarking capacity, blind detection and security. Watermarking schemes are developed according to the requirements of the application and all applications do not require each of these properties in their entirety i.e. watermarking requirements are application dependent and some most desirable properties for these applications are conflicting in nature. A huge trade-off among them is often involved. Digital signature is also an authentication scheme that is used for verifying the integrity and authenticity of the image content. There is need of a system is to hide (generally encrypted) data into other data. The "secrecy" of the embedded data is essential in this area.

RELATED WORK

Digital image watermarking techniques can be broadly classified into two major categories:
i) Spatial Domain Watermarking
ii) Frequency Domain Watermarking

i) 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 color value of some selected pixels. The strength of the spatial domain watermarking is Simplicity, Very low computational complexity, Less time consuming. The spatial domain watermarking is easier and its computing speed is high than transform domain but it is less robust against attacks. The spatial domain techniques can be easily applied to any image. The most important method of spatial domain is LSB.

Additive Watermarking: The most straightforward method for embedding the watermark in spatial domain is to add pseudo random noise pattern to the intensity of image pixels. The noise signal is usually integers like (-1,0,1) or sometimes floating point numbers.

Least Significant Bit Modification: A digital image version of this analogue image contains sampled values of the function at discrete locations or pixels. These values are said to be the representation of the image in the spatial domain or often referred to as the pixel domain. Spatial embedding inserts message into image pixels.

ii). Frequency Domain Watermarking:
In the Frequency domain the watermark is embedding into frequency coefficients of host image. Frequency domain watermarking provides more information hiding capacity and high robustness against various geometrical attacks. Frequency domain watermarking is more robust than spatial domain watermarking due to the embedding of watermark into the altered frequency coefficients of the transformed image [11]. Some well-known watermarking transform domain are Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) [13], [14], [15], [16]. In transform domain we have various techniques, Fourier Transform (FT), Short Time Fourier Transform (STFT), and Continuous Wavelet Transform (CWT), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) or Combination of DCT and DWT.

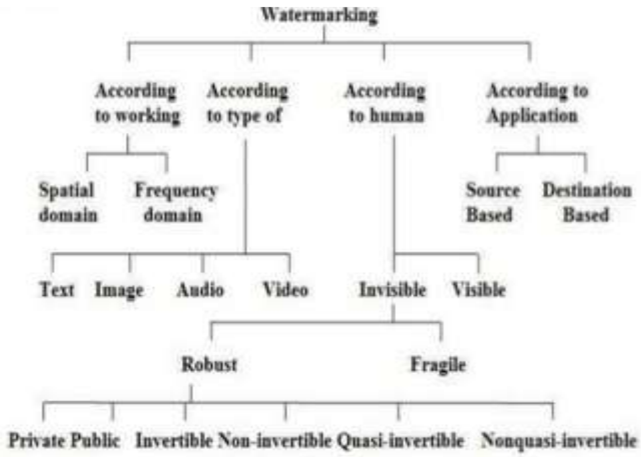


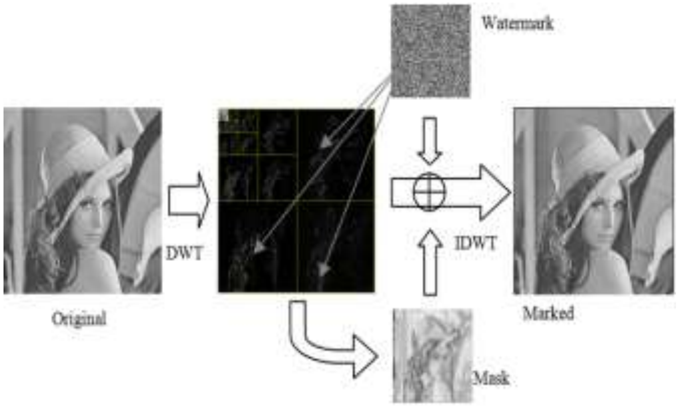
Fig. 1.Classification of watermarking techniques.

DIGITAL IMAGE WATERMARKING USING DISCRETE COSINE TRANSFORM

DCT watermarking can be classified into Block based DCT watermarking and Global DCT watermarking One of the first algorithms presented by Cox et al. (1997)used global DCT to embed a robust watermark in the perceptually significant portion of the Human Visual System (HVS). Embed the watermarking the perceptually significant portion of the image has many advantage because most compression algorithms remove the perceptually insignificant portion of the image. It represents the LSB in spatial domain howeverit represents the high frequency components [3]in the frequency domain. Fourier Transform (FT) is an operation that transforms a continuous function into its frequency components. The equivalent transform for discrete valued function requires the Discrete Fourier Transform (DFT). Discrete Cosine Transform is related to DFT in a sense that it transforms a time domain signal into its frequency components. The DCT however only uses the real parts of the DFT coefficients. In terms of property, the DCT has a strong energy compaction property and most of the signal information tends to be concentrated in a few low-frequency components of the DCT. The JPEG compression technique utilizes this property to separate and remove insignificant high frequency components in images. With the character of discrete Fourier transform (DFT), discrete cosine transform (DCT)turn over the image edge to make the image transformed into the form of even function. It's one of the most common linear transformations in digital signal process technology.

DIGITAL IMAGE WATERMARKING BASED ON DISCRETE WAVELET TRANSFORM

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. A wavelet series is a representation of a square-integrable function by a certain ortho-normal series generated by a wavelet. Furthermore, the properties of wavelet could decompose original signal into wavelet transform coefficients which contains the position information. The original signal can be completely reconstructed by performing Inverse Wavelet Transformation on these coefficients. Watermarking in the wavelet transform domain is generally a problem of embedding watermark in the sub bands of the cover image.



The basic idea of discrete wavelet transform(DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district. Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency district(LL) and three high-frequency districts(LH,HL,HH). If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. A two- dismensional image after three-times DWT decomposed can be shown as Fig.1. Where, L represents low-pass filter, H represents high-pass filter. An original image can be decomposed of frequency districts of HL1, LH1, HH1.The low-frequency district information also can be decomposed into sub-level frequency district information of LL2, HL2, LH2 and HH2. By doing this the original image can be decomposed for N level wavelet transformation.

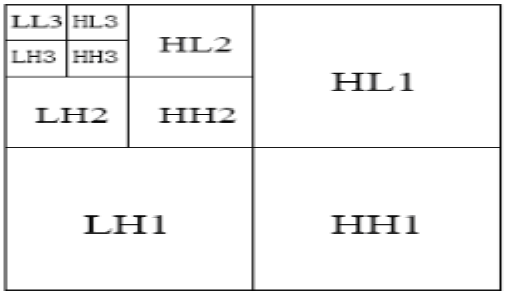


Fig. 2.Sketch Map of Image DWT Decomposed

The information of low frequency district is a image close to the original image. Most signal information of original image is in this frequency district. The frequency districts of LH, HL and HH respectively represents the level detail, the upright detail and the diagonal detail of the original image.

IMAGE WATERMARKING BASED ON RCM(REVERSIBLE CONTRAST MAPPING)

Most of the reversible watermarking approaches proposed so far incorporate a lossless data compression stage. The use of an elaborate data compression stage increases the mathematical complexity of the watermarking. There are some watermarking schemes that do not rely on additional data compression, as for instance, the circular histogram interpretation schemes, but they have the drawback of a low embedding capacity. Here, we discuss a spatial domain reversible watermarking scheme that achieves high-capacity data embedding without any additional data compression stage. The scheme is based on the reversible contrast mapping (RCM) transform, is a simple integer transform defined on pairs of pixels. For some pairs of pixels, RCM is invertible, even if the least significant bits (LSBs) of the transformed pixels are lost. The data space occupied by the LSBs is suitable for data hiding. The embedded information bit-rates of the proposed spatial domain reversible watermarking scheme are close to the highest bit-rates reported so far. The scheme does not need additional data compression, and, in terms of mathematical complexity, it appears to be the lowest complexity one proposed up to now. A very fast lookup table implementation is proposed. Robustness against cropping can be ensured as well.

STEGANOGRAPHY

The objective of steganography is to hide a secret message within a cover-media in such way that others cannot discern the presence of hidden message. Technically in simple words "steganography means hiding one piece of data within another".

Steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following elements
1) The cover media(C) that will hold the hidden data.
2) The secret message (M) may be plain text, cipher text or any type of data.
3) The stego function (Fe) and its inverse (Fe-1).
4) An optional stego-key(K) or password may be used to hide and unhide the message. The stego function operates over cover media and the message (to be hidden) along with a stego- key (optionally) to produce stego media(s).The schematic of steganographic operation is shown below-

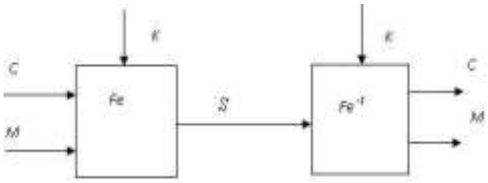


Fig. 3.Steganographic operation.

The most widely technique today is hiding of secret message into a digital image. This technique exploits the weakness of human visual system. HVS cannot detect variation in luminance of color vectors at higher frequency side of visual spectrum. A picture can be represented by the collection of color pixels. The individual pixels can be represented by their optical characteristics like brightness, Chroma etc. Each of these characteristics can be digitally expressed in terms of 1's and 0's.

This technique can be directly applied on digital image on bitmap format as well as the compressed image format like JPEG. In JPEG format, each pixel of the image is digitally coded using discrete cosine transformation (DCT). The LSB of encoded DCT components can be used as the carriers of the hidden message.

The details of above techniques are explained below:
Modification of LSB of a cover image in 'bitmap' format.
In this method binary equivalent of the message (to be hidden) is distributed among the LSBs of each pixel. For example we will try to hide the character 'A' into an 8-bit color image.

We are taking eight consecutive pixels from top left corner of the image. The equivalent binary bit pattern of those pixels may be like this: -
00100111 11101001 11001000 00100111 11001000 11101001
11001000 00100111
Then each bit of binary equivalence of letter 'A' i.e. **01100101** are copied serially
(from the left hand side) to the LSB's of equivalent binary pattern of pixels,

resulting the bit pattern will become like this: -

**00100110 11101001 11001001 00100110 11001000 11101001
11001000 00100111**

While at the detection end extract the last bit of every pixel to get the equivalent binary pattern of hidden data. This operation can perform by using masking operation. Mask the data with 0x1 so that we can get the last bit of each pixel. The mask operation is as follows -

**00100110&00000001 = 0
11101001& 00000001 = 1
11001001& 00000001 = 1
00100110& 00000001 = 0
11001000& 00000001 = 0
11101001& 00000001 = 1
11001000& 00000001 = 0
00100111& 00000001 = 1**

So this way can able to extract the hidden data 'A' i.e. **01100101.**But during this process we are not able to recover the one bit of original image or data which cause loss of quality of original image. So the problem with this technique is that it is very vulnerable to attacks such as image compressing and formatting.

WATERMARKING PRINCIPLE

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. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself. Figure shows the basic block diagram of watermarking process.

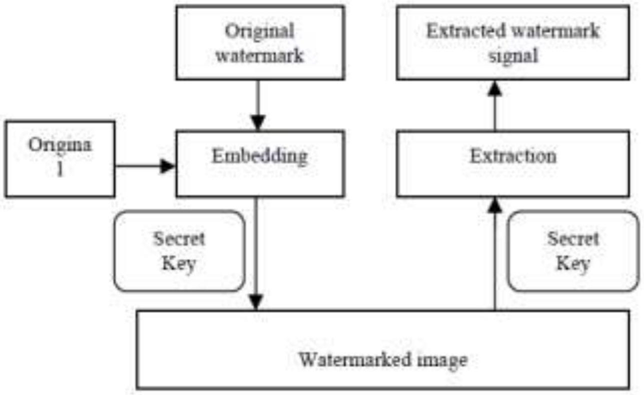


Fig. 4.Block diagram of watermarking process.

The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different 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.

WATERMARKING PROPERTIES

Watermarking need some desirable properties based on the application of the watermarking system [2].
Some of the properties are presented here:

1. Effectiveness:

This is the most important property of watermark that the watermark should be effective means it should surely be detective. If this will not happened the goal of the watermarking is not fulfilled.

2. Host signal Quality:

This is also important property of watermarking. Everybody knows that in watermarking, watermark is embedded in host signal (image, video, audio etc.). This may put an effect on the host signal. So the watermarking system should be like as, it will minimum changes the host signal and it should be unnoticeable when watermark is invisible.

3. Watermark Size

Watermark is often use to owner identification or security confirmation of host signal and it always use when data is transmitted. So it is important that the size of watermark should be minimum because it will increases the size of data to be transmitted.

4. Robustness

Robustness is crucial property for all watermarking systems. There are so many causes by which watermark is degraded, altered during transmission, attacked by hackers in paid media applications. So watermark should robust, So that it withstand against all the attacks and threats.

5. Capacity or Data Payload

This property describes how much data should be embedded as a watermark to successfully detect during extraction. Watermark should be able to carry enough information to represent the uniqueness of the image. Different application has different payload requirements.

Performance Evaluation

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 he is effective?
Some of the quality matrices an image watermarking method or algorithm.

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].

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

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

$$\mathrm{PSNR} = 10 * \log (\mathrm{P}^2/\mathrm{MSE})$$

Where p= maximum value in host image.
Imperceptibility of image is determined by this factor. More the PSNR shows that Watermarked image is perceptible or watermark is not recognized by naked eyes.

APPLICATIONS

Digital watermarking can be used for the following purposes:
A. Copyright Protection: This is by far the most prominent application of watermarks. With tons of images being exchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking an image will prevent redistribution of copyrighted images.

B. 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.

C. Broadcast Monitoring**:** As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not.

D. Content Labeling**:** Watermarks can be used to give more information about the cover object. This process is named as content labeling.

E. Tamper Detection**:** Fragile watermarks can be used to detect tampering in an image. If the fragile watermark is degraded in any way then we can say that the image or document in question has been tampered.

F. Digital Fingerprinting: This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner.

G. Content protection: In this process the content stamped with a visible watermark that is very difficult to remove so that it can be publicly and freely distributed.

CONCLUSION

This paper provides thorough outline of Digital Image Watermarking techniques. In Spatial domain as well as transform domains. The Transform domain based watermarking techniques are recommended to achieve robustness. This survey on different digital watermarking techniques shows different robustness level on different attacks. Spatial domain based technique (LSB technique) which is one the most popular technique of spatial domain image watermarking technique shows less robustness against different geometric attacks. Transformed domain techniques like DWT based watermarking techniques, DCT and DWT based composite watermarking technique, Multi-channel DWT based technique are better than Spatial domain based technique.

REFERENCES

[1] Unseen Visible Watermarking: A Novel Methodology for Auxiliary Information Delivery via Visual Contents Hun-Hsiang Huang, Shang-Chih Chuang, Yen-Lin Huang, and Ja-Ling Wu, Fellow, IEEE, JUNE 2009.

[2] Very Fast Watermarking by Reversible Contrast Mapping DinuColtuc and Jean-Marc Chassery, JUNE 2007.

[3] Reversible Watermark Using the Difference Expansion of a Generalized Integer TransformAdnan M. Alattar, Member, IEEE, AUGUST 2004.

[4] I. Cox, J. Killian, T. Leighton, T. Shamoon, “Secure Spread Spectrum atermarking for Multimedia,” IEEE Trans. Image Processing, Vol. 6, No. 12, pp. 1673-1687, 1997.

[5] Song Qiang, Zhang Hongbin”, Colour Image Self Embedding and atermarkingBased on T”, 20 0 International Conference on Measuring technology and Mechatronics Automation, pp: 978-0-7695-3962.

[6] Optimization-IntensiveWatermarkingTechniques for Decision Problems Jennifer L. Wong, Student Member, IEEE, Gang Qu, Member, IEEE, and MiodragPotkonjak, Member, IEEE, JANUARY 2004.

[7] Chirag Sharma, eepakPrashar, “ T based robust technique of watermarking applied on igital Images”, International Journal of Soft Computing and Engineering (IJSCE),Volume-2,Issue-2,May 2012.

[8] Mohamed A. Suhail, Mohammad S. Obaidat, “ igital Watermarking-Based DCT and JPEG Model”, IEEE Transactions on Instrumentation and Measurement, Vol. 52, No. 5, October 2003.

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

[10] Vaishali S. Jabade, Dr. Sachin R. Gengaje,”Litrature Review of Wavelet Based Digital Watermarking techniques”, International Journal of Computer Applications, Volume 31, No.1,pp-28-35.