Reviews On Watermarking Techniques : A Survey

Sheenu Gupta, Manshi Shukla
Research Scholar(Department of Computer Science),Rimt-Iet,Mandi Gobindgarh
Asst.Professor(CSE Dept),Rimt-Iet,Mandi Gobindgarh

Abstract
Neural networks have been used in the development of intelligent systems that simulate pattern recognition and object identification. Coin identification by machines relies currently on the assessment of the physical parameters of a coin. An intelligent coin identification system that uses coin patterns for identification helps preventing confusion between different coins of similar physical dimensions. This paper represents algorithm for recognition of the coins of different denomination. Based on the radius of the coin, the coins of different denomination are classified.

Keywords
neural networks,DCT,DWT.

1. Introduction

The success of the Internet and digital consumer devices has profoundly changed our society and daily lives by making the capture, transmission, and storage of digital data extremely easy and convenient. However, this raises a big concern is how to secure these data and preventing unauthorized use. This issue has become problematic in many areas. For example the music and video industry loses billions of dollars per year due to illegal copying and downloading of copyrighted materials from the Internet. As a solution, Digital watermarking is used very frequently. Hence, digital watermarking becomes very attractive research topic. Digital watermarking is a technology that creates and detects invisible markings, which can be used to trace the origin, authenticity, and legal usage of digital data. Ideally, they should be hard to notice, difficult to reproduce, and impossible to remove without destroying the medium they protect. In the future the main development of digital watermarking is like this: copyright protection, pirate tracking, copying protection, image authentication, cover-up communication. [1][3]. Robustness means that the watermark is able to withstand with some changes in the watermark-embedded signal; while imperceptibility represents the invisibility to human eyes, or for audio clips, the inaudibility to human ears. A good watermark algorithm should be by all means is simultaneously robust and imperceptible.

In terms of the embedding domain, watermarking algorithms are mainly divided into two groups: spatial domain method which embed the data by directly modifying the pixel values of the original image and transform domain method which embed the data by modulating the transform domain coefficients. A frequency-domain watermarking, value of certain frequencies is altered from their original & embeds the watermark into the transformed image. This is more robust than the spatial domain technique.

In frequency-domain technique multiple transforms used for watermarking purpose such as DCT, DFT, DWT. The most commonly used transforms for digital watermarking are DFT (Discrete Fourier Transform) DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform). Now Frequency domain watermarking is more useful for all practical internet applications. DCT based frequency domain watermarking useful in pan card, i-card of employee of companies, fingerprint identification, medical imaging where is low cost required, whereas DWT based frequency domain watermarking mainly used when we want to transfer more confidential matter through internet to anyone, in military application, government application, broadcast monitoring i.e. entertainment & advertisements, & banks application .[1]

2. Disital Watermark Technique

A watermarking algorithm embeds watermark in different kind of data like, text, audio, video etc.. The embedding process is done by use of a private key which decided the locations within the multimedia object (image) where the watermark would be embedded. Once the watermark is embedded it can happens several attacks because the online object can be digitally processed. The attacks can be unintentional ,Hence the watermark has to be very robust against all attacks which is possible. When the owner wants to check the watermarks in the attacked and damage multimedia object, she/he depends on the private key that was used to embed the watermark. Using the secrete key, the embedded watermark can be detected. This detected watermark may or may not combine the original watermark because the image might have been attacked. Hence to validate the presence of watermark, the original data is used to compare and extract the watermark signal (non-blind watermarking) or a correlation method is used to detect the strength of the watermark signal from

Manuscript received July 5, 2015
Manuscript revised July 20, 2015

the extracted watermark (blind watermarking). In the correlation, detected watermark from the original data is compared with the extracted watermark.

There are three main Properties of digital watermarking technique

A. Transparency or Fidelity: The digital watermark should not affect the quality of the original image after it is watermarked. Watermarking should not introduce visible distortions because if such distortions are introduced it reduces the commercial value of the image.

B. Robustness: Watermarks could be removed intentionally or unintentionally by simple image processing operations like contrast or brightness enhancement, gamma correction etc. Hence watermarks should be robust against variety of such attacks.

C. 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 [1].

3. Watermarking Applications

The main applications of digital watermarking are presented as: A. Copyright Protection: Watermarking can be used to protecting redistribution of copyrighted material over the untrusted network like Internet or peer-to-peer (P2P) networks. Content aware networks (p2p) could incorporate watermarking technologies to report or filter out copyrighted material from such networks.

Figure 1 Applications in Copyright

B. Content Archiving: Watermarking can be used to insert digital object identifier or serial number to help archive digital contents like images, audio or video. It can also be used for classifying and organizing digital contents. Normally digital contents are identified by their file names; however, this is a technique as file names can be easily changed. Hence embedding the object identifier within the object itself reduces the possibility of tampering and hence can be effectively used in archiving systems.

Figure 2 Applications in Contents Archiving

C. Meta-data Insertion: Meta-data refers to the data that describes data. Images can be labelled with its content and can be used in search engines. Audio files can carry the lyrics or the name of the singer. Journalists could use photographs of an incident to insert the cover story of the respective news. Medical X-rays could store patient records.

D. Broadcast Monitoring: Broadcast Monitoring refers to the technique of cross-verifying whether the content that was supposed to be broadcasted (on TV or Radio) has really been broadcasted or not. Watermarking can also be used for broadcast monitoring. This has major application is commercial advertisement broadcasting where the entity who is advertising wants to monitor whether their advertisement was actually broadcasted at the right time and for right duration.

E. Tamper Detection: Digital content can be detected for tampering by embedding fragile watermarks. If the fragile watermark is destroyed or degraded, it indicated the presence of tampering and hence the digital content cannot be trusted. Tamper detection is very important for some applications that involve highly sensitive data like satellite imagery or medical imagery. Tamper detection is also useful in court of law where digital images could be used as a forensic tool to prove whether the image is tampered or not.

Figure 3 Applications in Digital Fingerprinting

F. Digital Fingerprinting: Digital Fingerprinting is a technique used to detect the owner of the digital content. Fingerprints are unique to the owner of the digital data. Hence a single digital content can have different fingerprints because they related to different users.

4. Watermarks And Watermark Detection

There are mainly two types of watermarks that can be embedded in an image.
A. Pseudo-Random Gaussian Sequence: A Gaussian sequence watermark is a sequence of numbers contains 1 and -1 and which has equal number of 1's and -1's is denoted as a watermark. It is consider as a watermark with zero mean and one variation. Such watermarks are used for original data detection using a correlation measure.
B. Binary Image or Grey Scale Image Watermarks: Some watermarking algorithms embed meaningful data like logo image instead of a pseudo-random Gaussian sequence. Such watermarks are considered as binary image watermarks or grey scale watermarks. Such watermarks are used for original data detection. Based on the type of watermark embedded, an appropriate decoder has to be used to detect the existent of watermark.

5. Image Watermarking Embedding Domain

Based on domain used for watermark embedding process, the watermarking techniques can be classified into the following types:
1) Spatial watermarking
Spatial watermarking can also be applied using colour partition such that the watermark appears in only one of the colour bands. However, the watermark appears when the colours are separated for printing. Spatial domain process involves addition of fixed amplitude pseudo-noise into the image. These approaches modify the least significant bits of original contents. The watermark can be hidden into the data to assume that the LSB data are visually irrelevant.

2)Transformation based watermarking There are many techniques proposed based on transformation based watermarking. Watermarking can be applied in the transform domain; including such transforms are discrete Fourier, discrete cosine, and wavelet. In this first the host or main data is transformed and then modifications are applied to transformed coefficients. Watermark is embedded in DFT, DCT and DWT domain coefficients.

6. Dct Domain Watermarking

DCT based watermarking techniques are more robust as compared to spatial domain watermarking techniques. this algorithm is robust against simple image processing operations like low pass filtering, contrast and brightness adjustment, etc. However, they are difficult to implement and are computationally more costly. And also they are weak against geometric attacks like scaling, rotation and cropping etc. 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 watermark in 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 however it represents the high frequency components [3] in the frequency domain

7. Dwt Domain Watermarking

In the last few years wavelet transform has been widely used in signal processing in watermarking ,general and image compression schemes . In some applications wavelet based watermarking schemes better than DCT based approaches.
A. Characteristics of DWT
1) The wavelet transform decomposes the image into three spatial directions, i.e. vertical, horizontal and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely.
2) Wavelet Transform is mathematically efficient and can be implemented by using filter convolution simply.
3) Magnitude of DWT coefficients is high in the lowest bands (LL) at each level of decomposition and is least for other bands (HH, LH, HL) .
4) The high magnitude of the wavelet coefficient the more significant.
5) Detecting watermark at lower resolutions level is effective because at every resolution level there are few frequency bands present.
6) High resolution sub bands helps to easily positioned edge and patterns of textures in an image.
B. Advantages of DWT over DCT
1) Wavelet transform in HVS more closely than the DCT.
2)Wavelet transformed image is a multi-resolution description of image. Hence an image is shown at different resolution levels and can be continuously processed from low resolution to high resolution.
3) Visual artifacts introduced by wavelet transformed images are less marked compared to DCT because

wavelet transform doesn't decompose the image into blocks for processing. At high compression ratios blocking artifacts are noticeable in DCT; but in wavelet coded images it is much clearer.
4) DFT and DCT are full frame transform, and hence any change in the transform coefficients affects the entire image except if DCT is implemented using a block based approach. However DWT has spatial locality property, which means if signal or any watermark is embedded it will affect the image locally . Hence a wavelet transform provides both frequency and spatial information for an image.
C. DWT watermarking DWT based watermarking schemes use the same guidelines as DCT based schemes, i.e., concept is the same; however, transformation process of an image into its transform domain varies and hence the resulting coefficients are different.

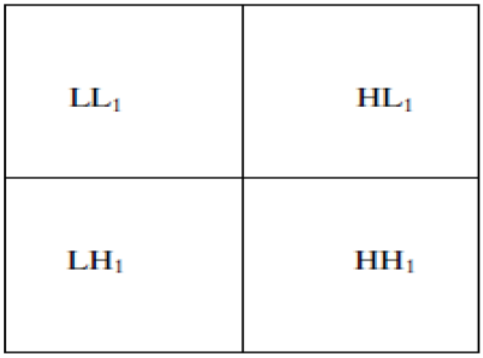

Figure 4: Single level decomposition using DWT.

Wavelet transforms use different kind of filters to transform the image. There are many filters, but the most commonly used filters for watermarking are Haar Wavelet Filter, Daubechies Bi-Orthogonal Filters and Daubechies Orthogonal Filters. Each of these filters decomposes the image into many frequencies. Single level decomposition gives four frequency sub band of the images. These four representations are called the LL, LH, HL, HH sub bands as shown in Fig.8.1. In this part, we discuss wavelet based watermarking algorithms. We classify these algorithms based on their decoder requirements as Non-blind Detection or Blind Detection. In, blind detection , original image for detecting the watermarks doesn't require; but, non-blind detection requires the original image.

8. Dft Domain Watermarking

DFT domain has been studied by researches because it provides robustness against geometric attacks like scaling, cropping, rotation, translation etc. In this part we discuss some watermarking algorithms based on the DFT domain.
A. Characteristics of DFT
1) DFT of a original image is generally complex valued, which results in the magnitude and phase representation of an image.
2) DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform.
3) DFT is resistant to cropping because effect of cropping leads to the blurring of spectrum. If the watermarks are embedded in the magnitude, these are normalized coordinates, there is no synchronization are needed.
4) The powerful components of the DFT are the main components which contain the low frequencies.
5) Image scaling results in amplification of retrieved signal and can be detected by correlation coefficient. Image translation has no result on extracted signal.
6) Image rotation results in cyclic shifts of retrieved signal and can be detected by exhaustive search .
7) Scaling in the spatial domain causes inverse scaling in the frequency domain. spatial domain rotation causes the same rotation in the frequency domain .
B. Coefficient Selection Criteria
1) The low frequency coefficients modification can cause visible artifacts in the spatial domain. That's why, low frequency coefficients should be avoided in DFT.
2) High frequency coefficients are not well suited because they are removed during JPEG compression.
3) The location to embed the watermark is the mid level frequency is best to avoid the both lower and higher frequencies weakness.

9. Image Watermarking Survey

In image watermarking field, recently some work have been done, which is discussed here. 1. Qing Liu,Jun Ying(2012),"Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis" In this paper, firstly, original image is transformed by using the DWT (Discrete wavelet transform) upto the 3-layers, means apply 3 times ,so that image is divided into the different sub band(LL,LH,HL and HH) and watermarked image is embedded into the intermediate frequency sub band. Spread spectrum technology is also used in this paper and blind watermarking technique is used to extract the watermark. Spread spectrum technology provides Secure communications because signal is "hidden" like noise but it increases bandwidth of signal and increases the complexity and also used blind detection technique to extract the watermark is used. 2. Zhaoshan Wang, Shanxiang Lv,Yan Shna (2012)"A Digital Image Watermarking Algorithm Based on Chaos and Fresnel Transform"

In this paper, a digital image watermarking algorithm based on chaos and Fresnel transform is proposed. The original image is transformed by using the concept of Fresnel diffraction plane by distance parameter, and watermark image is embedded after scrambled by chaotic sequence. The watermark image can be retrieved without original image, and there is little changes on the original image after embedding. Chaotic scrambling can encrypt watermark information.
3. Jithin VM,K K gupta (2013)"Robust invisible QR code image watermarking in DWT domain" In this paper, QR code is used as watermark image, this makes watermarked image more robust but if the embedding algorithm is known to unauthorized person then by using the QR code scanner software ,watermarking key can be easily extracted. 4. Nan Lin; Jianjing Shen; Xiaofeng Guo; Jun Zhou, (2011) "A robust image watermarking based on DWT-QR decomposition". A novel blind watermarking technique based on QR decomposition in still images is proposed. The method is implemented in wavelet domain and its robustness has been evaluated against some image processing attacks and the results have been compared with two traditional methods i.e., SVD and DCT. It is shown that while the proposed scheme has low computational complexity, it has better robustness against some image processing attacks in comparison with SVD and DCT methods. 5. Naderahmadian, Y.; Hosseini-Khayat, S.,(2010) "Fast Watermarking Based on QR Decomposition in Wavelet Domain". Copyright protection and authentication have become increasingly more important in daily life. The digital watermark is one of the techniques invented to tackle this issue. In this paper, a digitally invisible watermark is embedded in a QR code image by means of wavelet transform. In the embedding process, a binary image, logo, is transformed into a corresponding watermark and then embedded into a selected sub band. The experimental results illustrated that, for all the cases considered in this paper is more robustness to attacks and as such it can serve as a viable copyright protection and authentication tool.

10. Conclusion

In this paper we surveyed the current literature on digital image watermarking,. We classified watermarking algorithms based on the transform domain in which the watermark is embedded. Also, study the watermarking properties, applications and techniques used. This paper shows the different techniques and discusses the important technology called QR code which can be used in future work.

References

[1] Cox, IJ, Miller, ML & Bloom, JA 2002, Digital Watermarking, Morgan Kaufmann Publisher, San Francisco, CA, USA 2002.
[2] I.J Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia" in IEEE Transactions on Image Processing, vol. 6, no. 12, Dec.1997, pp:1673 -1687.
[3] Guan-Ming Su, "An Overview of Transparent and Robust Digital Image Watermarking", 2001.
[4] Kundur. D., Hatzinakos, D., "Digital Watermarking using Multiresolution Wavelet Decomposition", Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing, Seattle, Washington, vol. 5, pp. 2969-2972, May 1998.
[5] Qing Liu,Jun Ying(2012),"Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis" .
[6] Zhaoshan Wang, Shanxiang Lv,Yan Shna (2012)"A Digital Image Watermarking Algorithm Based on Chaos and Fresnel Transform", 2012.
[7] Jithin VM,K K gupta (2013)"Robust invisible QR code image watermarking in DWT domain",2013.
[8] Nan Lin; Jianjing Shen; Xiaofeng Guo; Jun Zhou, "A robust image watermarking based on DWT-QR decomposition," Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.684,688, 27-29 May 2011.