A Survey of Digital Watermarking Techniques and Performance Evaluation Metrics

Hemani[1] & Samridhi Singh[2]

[1]Student, Department of Information Technology, G.B.P.U.A&T, Pantnagar, India
[2]Student, Department of Information Technology, G.B.P.U.A&T, Pantnagar, India

Abstract

Data security is always the most important concern for everyone. In this paper, we are going to study the Watermarking Techniques, Performance Evaluation Metrics associated with watermarking. Watermarking is not new to anyone, but this method is always the most talked about. Digital watermarking has become an active and important area of research, and development and knowledge of watermarking techniques are being deemed essential to help in getting rid of some of the challenges faced by the rapid propagation of digital content.

keywords: *Watermarking, Spatial domain, Image Transforms, Discrete Wavelet Transform, Discrete Cosine Transform, Discrete Fourier Transform*

I. Introduction

Digital watermarking places an important role in transmitting a data from an insecure medium. It has been recognized for quite some time that current copyright laws are inadequate for dealing with digital data. This led to an increasing interest on Digital Watermarking Techniques.

This paper is organized as follows sections:

- Overview of Digital Watermarking Techniques
- Performance Metric of Watermarking Algorithm

II. Digital Watermarking Techniques

Watermarking is defined as the process of embedding watermarks in digital media e.g. audio, video, image etc.. using an appropriate algorithm. The traditional information security technology based on cryptography theory mostly has its limitations.[1] On the internet application, we embed some logo, trademark or an image in multimedia objects to prevent it from misuse. The digital communication technology i.e. The Internet confronts various troubles related to the privacy and security of the data.[2] Hence, watermarking can be used for solving many purposes like tamper detection, data authentication, security, copyright protection. Watermarking is done by using some particular, strong and appropriate algorithms which play an important role in watermarking. This is because if the technique which is used in the watermarking process is strong, efficient and effective, then the embedded watermark cannot be easily extracted. One can only extract the secret data if he knows the appropriate algorithm otherwise it is difficult to get the watermark. There are many algorithms which are being used to hide the secret information. These algorithms are basically bifurcated into two domains called Frequency domain and Spatial domain. Digital watermarking provides copyright protection of data. For image watermarking, the algorithms can be categorized into one of the two domains: spatial domain or transform domain [3,4]. The basic idea of spatial and frequency domain is shown in figure 1.1 as given below

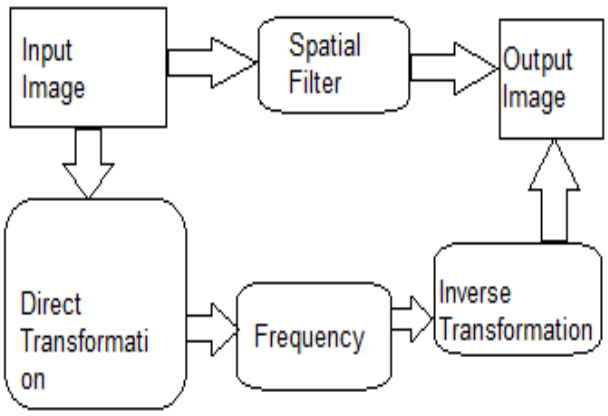

Fig 1.1

Digital Watermarking Technique is basically classified into two major parts, these are

- Spatial Domain
- Frequency Domain

The Algorithm used for a spatial domain are less robust for various attacks as the changes are made at Least Significant Substitution (LSB) of original data. While in the transform domain the

watermark is embedded by changing the magnitude of coefficients in a transform domain with the help of discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT), and singular value decomposition (SVD) techniques [5,6].

A. Spatial Domain

In Spatial domain, digital watermarking algorithms directly load the raw data into the original image[1]. There should be minor changes in the pixel value intensity. The significant portion of the low-frequency component of images should be modified in order to insert the watermark data in a reliable and robust way[2]. Even if the Spatial domain watermarking is less robust against attacks, Its computing speed is higher than transform domain The spatial domain algorithm are specifically divided into two parts

- Correlation based Techniques
- Least Significant Bit

1) Correlation based Technique

In this technique, the watermark W(x,y) is added to the original content O(x,y) according to the equation.

$$Ow(x,y) = O(x,y)+ kW(x,y)$$

where k is a gain factor and Ow is the watermarked content. As we increase the value of k, it will expense the quality of watermarked contents.

Advantage

1. Increases the robustness of watermark by increasing the gain factor.

Disadvantage

1. Due to very high increment in gain factor, image quality may decrease.

2) Least Significant Bit

It is an important technique to embed a watermark in the least significant bits of the cover image which are randomly selected pixels. Two LSB techniques proposed by Van et al. In the first method the LSB of the image was replaced with a pseudo-noise(PN) sequence While in the second a PN sequence was added to the LSB.

An Example of least significant bit watermarking [3]:

Image: 10010101 00111011 11001101 01010101….

Watermark: 1 0 1 0…..

Watermarked Image: 10010101 00111010 11001101 01010100…..

The steps used to embed the watermark in the original image by using the LSB [4]:

1. Convert RGB image to grey scale image.
2. Make double precision for the 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.

Advantages

1. Low degradation of image quality.
2. Easy to implement and understand.
3. High perceptual transparency.

Disadvantages

1. Very sensitive to noise.
2. Vulnerable to cropping, scaling attacks.
3. Very less robust against attacks.

The benefit of this method is that it is easily performed on images. And it also provides high perceptual transparency. The quality of the watermark doesn't degrade after embedding the watermark using LSB. Using this technique watermark can easily be destroyed by any signal processing attacks as the demerit of LSB technique is its poor robustness to common signal processing operations. It is imperceptible but not vulnerable to attacks and noise.

B. Frequency Domain

The prime aim of the frequency domain algorithm is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are Discrete Cosine Transform(DCT), Discrete Fourier Transform(DFT), Discrete Wavelet Transform(DFT),(SVD).

1) Discrete Cosine Transform

The discrete cosine transform is a technique for converting a signal from the spatial domain to the elementary frequency components. It is generally used for image compression. In many fields of image processing DCT is applied such as data compression, pattern recognition.

DCT Block Based Watermarking Algorithm:

1. Divide the image into non-overlapping blocks of 8*8 sizes.

2. Apply forward DCT to each block.

3. Then after, apply block selection technique.

4. Then, apply coefficient selection criteria

5. Embed Watermark after modifying the selected coefficients.

6. Apply inverse DCT on each block of an image.

2) Discrete Fourier Transform

It transforms a continuous function into its frequency components. It has the robustness against geometric attacks like rotation, scaling, cropping, and translation etc. DFT shows the translation robustness to attack. In spatial shifting in the image affects the phase representation of the image but not the magnitude representation and circular shifts in the spatial transform don't affect the magnitude of the Fourier transform.

Characteristics of DFT

1. DFT of an 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 affect 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 the effect of cropping leads to the blurring of a 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 a 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.

Comparison

Advantages of DFT over DWT and DCT

DFT is a rotation, scaling, and translation (RST) invariant. Hence it can be used to recover from geometric distortions, whereas the spatial domain, DCT and the DWT are not RST robust and difficult to robust from geometric distortions.

3) Discrete Wavelet Transform

DWT is a wavelet transform in which the wavelets are discretely sampled. A Key advantage of it over Fourier transforms is a temporal resolution: it captures both frequency and location information.

Comparison

Advantages of DWT over DCT

1. The Wavelet transforms in HVS more closely than the DCT.
2. Wavelet transformed an image is a multi-resolution description of an image..
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 the 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.

Disadvantages of DWT over DCT:

1. The Computational complexity of DWT is more as compared to DCT'.
2. Feig (1990) pointed out that, it only takes 54 multiplications to compute DCT for a block of 8x8, but in wavelet, calculation depends upon the length of the filter used, which is at least 1 multiplication per coefficient of an image.

III. Performance Evaluation Metric

Performance Evaluation always plays one of the essential roles in designing the algorithm in watermarking. The main Objective of this performance evaluation metric is to check whether the proposed algorithm performance is up to the expectation or not or we can say it is effective or not.

Measuring the performance of an algorithm is one of a crucial section.

Some of the performance metrics of an image watermarking methods and algorithm have are as follows:

A. Mean Square Error

The MSE is an average squared difference between a reference image and a distorted image. The formula to measure MSE are as follows:

$$MSE = 1/XY\left[\sum_{i=1}^{X}\sum_{j=1}^{Y}(c(i,j)-e(i,j))\text{^}2\right]$$

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.

B. Signal to Noise Ratio

SNR measures the signal strength related to the background noise. We can also say that it measures the sensitivity of the image. And the formula to measure SNR is as follows:

$$SNR_{dB} = 10\log_{10}\left(\frac{P_{signal}}{P_{noise}}\right)$$

C. Peak Signal to Noise Ratio

PSNR is used to determine the efficiency of watermarking with respect to the noise. The noise used to degrade the quality of the noise. The visual quality of watermarked and attacked images is measured using the Peak Signal to Noise Ratio.

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

Where P=Maximum value in host image

D. Bit Error Ratio

This ratio describes how many bits received in error over the number of the total bits received. BER can be simply calculated by comparing bit values of embed and cover image.

$$BER=P/(H*W)$$

where H and W are height and width of the watermarked image. P is the count number initialized to zero and it increments by one if there is any bit difference between cover and embeds an image.

IV. Conclusion

We just want to summarize this paper by saying that, Digital watermarking is such a vast topic to study and here we just surveyed the digital watermarking technique and the performance evaluation metric of digital watermarking. We also compared the techniques.

References

1. Jiang Xuehua, "Digital Watermarking and Its Application in Image Copyright Protection ",2010 International Conference on Intelligent Computation Technology and Automation.
2. Tanu dua, Bhupesh Kumar Singh,"Image Authentication Using Digital Watermarking", 2015 International Journal of Computational Engineering Research
3. Reddy, R., M. V. N. Prasad, and D. S. Rao. "Robust Digital Watermarking of Images using Wavelets." International Journal of Computer and Electrical Engineering, vol.1, no.2, pp.1793-8163, 2009
4. Sang, Jun, and Mohammad S. Alam. "Fragility and robustness of binary-phase-only-filter-based fragile/semifragile digital image watermarking." Instrumentation and Measurement, IEEE Transactions , vol. 57, no.3, pp. 595-606, 2008
5. Liu, Ruizhen, and Tieniu Tan. "An SVD-based watermarking scheme for protecting rightful ownership." Multimedia, IEEE Transactions, vol. 4, no.1, pp.121-128, 2002.
6. Nikolaidis, Athanasios, and Ioannis Pitas. "Asymptotically optimal detection for additive watermarking in the DCT and DWT domains." Image Processing, IEEE Transactions, vol.12, no.5, pp. 563-571, 2003
7. D. Mistry, "Comparison of Digital Watermarking Methods" (IJCSE) International Journal of Computer Science and Engineering, vol. 02, no. 09, (2010), pp. 2805-2909
8. 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.
9. 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.
10. Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", IJEIT, ISSN: 2277-3754, Vol. 2 Issue 9, March-2013.
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. Singh, Surya Pratap, Paresh Rawat, and Sudhir Agrawal "A robust watermarking approach using DCT-DWT." *International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 8* (2012).
13. Al-Haj, Ali "Combined DWT-DCT digital image watermarking." *Journal of computer science* 3, no. 9 (2007): 740.
14. Anthony T.S.Ho et.al "A Robust Digital Image-in-Image Watermarking Algorithm Using the Fast Hadamard Transform", *Springer*, 2011

15. Mansouri, A., A. Mahmoudi Aznaveh, and F. Torkamani Azar "SVD-based digital image watermarking using complex wavelet transform." *Sadhana* 34, no. 3 (2009): 393-406.
16. T. Serre, L. Wolf, S. Bileschi, M. Riesenhuber, and T. Poggio, "*Object recognition with cortex-like mechanisms,*" *IEEE Trans. on PAMI* vol. 29, no. 3, 2007.
17. Alexander Sverdlov, "Secure DCT-SVD Domain Image Watermarking: Embedding Data in All Frequencies", Proceedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific, Bangalore, India, October 14-17, 2003
18. Palak Patel, Yash Patel," Secure and Authentic DCT image steganography through DWT-SVD based Digital watermarking with RSA encryption", IEEE, 2015