International Journal of Computer Applications Technology and Research
Volume 2– Issue 2, 126 - 130, 2013, ISSN: 2319–8656

Performance Comparison of Digital Image Watermarking Techniques: A Survey

Namita Chandrakar
Department of Electronics and Telecommunication
Shri Shankaracharya Technical Campus
Bhilai, India

Jaspal Bagga
Department of Information and Technology
Shri Shankaracharya Technical Campus
Bhilai, India

Abstract: Digital watermarking is the processing of combined information into a digital signal. A watermark is a secondary image, which is overlaid on the host image, and provides a means of protecting the image. In order to provide high quality watermarked image, the watermarked image should be imperceptible. This paper presents different techniques of digital image watermarking based on spatial & frequency domain, which shows that spatial domain technique provides security & successful recovery of watermark image and higher PSNR value compared to frequency domain.

Keywords: Image watermarking, Spatial domain, Frequency domain, Least Significant Bit (LSB), PSNR (Peak Signal to Noise ratio), MSE (Mean Square Error).

1. INTRODUCTION

Electronic commerce, commonly known as e-commerce, is the buying and selling of product or service over electronic systems such as the internet & other computer networks. So the growth of e-commerce applications in the world wide web requires the need to increase the security of data communications over the internet. To provide security to these applications data encryption and information hiding techniques were introduced & developed.

There are many approaches like Cryptography, Watermarking and Steganography to transfer the data/image to the intended user at destination without any modifications [1]. A watermark is a secondary image, which is overlaid on the primary image, and provides a means of protecting the image [2].

Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Cryptography only provides security by encryption and decryption. There is no protection after decryption & only protected content of the messages but watermarks can protect content even after they are decoded.

Watermarking is a pattern of bits inserted into digital image, audio, video or text file that identifies the file's copyright information such as author and rights [3]. Thus, watermarking is an approach to make sure the data are protected. Watermarking is designed to be completely invisible. Once the watermarking is done, user can send the watermarked image to other computer so that other user is able to read the watermark or the hidden message in the image only if the same algorithm is used. Thus, the watermark can be protected without being revealed.

It may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography literally means, "covered writing". An ideal steganographic system would embed a large amount of information, perfectly securely with no visible degradation to the cover object. Steganographic methods are in general not robust, that is the hidden information cannot be recovered after data manipulation. Watermarking is robust against attacks. If the existence of the hidden information is known it is difficult, ideally impossible for an attacker to destroy the embedded watermark.

Imperceptibility, robustness, inseparability, security, are the features of digital watermarking.

2. TYPES OF DIGITAL WATERMARKS

Watermarks and watermarking techniques can be divided into various categories in various ways.

1) According to the type of document to be watermarked, watermarking techniques can be divided into four categories as follows:
   i. Text Watermarking
   ii. Image Watermarking
   iii. Audio Watermarking
   iv. Video Watermarking
2) In other way, the digital watermarks can be divided into three different types as follows:
   i. Visible watermark: Visible watermark is a secondary translucent overlaid into the primary image.

   ii. Invisible-Robust watermark: The invisible-robust watermark is embed in such a way that alternations made to the pixel value is perceptually not noticed and it can be recovered only with appropriate decoding mechanism.

   iii. Invisible-Fragile watermark: The invisible-fragile watermark is embedded in such a way that any modification of the image would alter or destroy the watermark.

A robust watermark should survive a wide variety of attacks both incidental and malicious [4, 5]. These watermark attacks can be Simple, Detection-disabling, Ambiguity and Removal attacks. Incidental attacks are those which is applied with a purpose other than to destroy the watermark. Malicious attacks are those which is designed to remove or weaken the watermark.

3. DIGITAL IMAGE WATERMARKING

Figure 1 shows the gereral block diagram of digital image watermarking. Digital Image Watermarking can protect image, video, audio from unauthorized person, noise, copyright etc. The best known image watermarking method that works in the spatial domain is the Least Significant Bit (LSB), which replaces the least significant bits of pixels selected to hide the information.

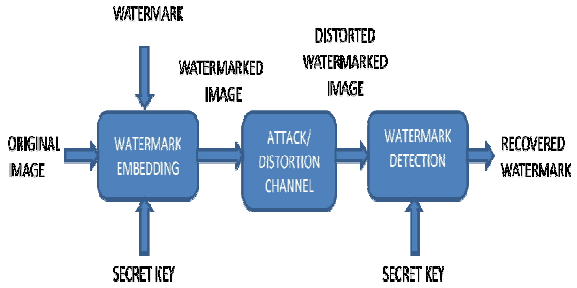

Figure 1. Block Diagram of Digital Image Watermarking

4. PREVIOUS WORKS

The image watermarking techniques can be classified into two categories:

4.1 Spatial-domain techniques (spatial watermarks) :

The spatial-domain techniques directly modify the intensities or color values of some selected pixels. No transforms are applied to the host signal during watermark embedding. Spatial techniques are not very robust against attacks. The main strengths of pixel domain methods are that they are conceptually simple and have very low computational complexities. spatial domain technique, is less time consuming as compare to wavelet or frequency domain techniques.

4.1.1 Least Significant Bit (LSB) Technique

The simplest spatial-domain image watermarking technique is to embed a watermark in the least significant bits (LSBs) of some randomly selected pixels of the cover image. Example of least significant bit watermarking

Image:
10001010 01110100 00011011 01000001 ...
Watermark:
0 1 1 0 ...
Watermarked Image:
1000101**0** 0111010**1** 0001101**1** 0100000**0** ...

Schyndel *et al.* [6] proposed a technique in which a watermark is generated using a m-sequence generator. The watermark was embedded to the least significant bit(LSBs) of the original image to produce the watermarked image. The watermark was extracted from a suspected image by taking the least significant bits at the proper locations. Detection was performed by a cross-correlation of the original and extracted watermark. They showed that the resulting image contained an invisible watermark with simple extraction procedures. But the watermark, was not robust to additive noise. Mohamed Ali HAJJAJI *et al.* [7] proposed watermarking of medical image, in which a set of data is inserted in a medical image. The watermarking method is based on the least significant bits (LSBs) in order to check the integrity and confidentiality of medical information and to maintain confidentiality for patient and hospital data. For 10% compression rate, the watermark is successfully recovered. Disadvantage of these technique is that, all the substituted data cannot properly extract when a Gaussian noise is applied in the watermarked image. Puneet Kr Sharma and Rajni, [1] proposed image watermarking & different security issues. To hide logo (secret image) into the cover image they used LSB algorithm. LSB of each of the pixel of the cover image is replaced by the bits of the secret image. Then 2nd LSB of each pixel of the cover image is replaced by the bits of the secret image and so on. Then PSNR and MSE are calculated for different bit substitution from LSB to MSB in image. The PSNR and MSE found for 1st LSB bit substitution was 55.8784 and 0.1680 respectively. Deepshikha Chopra *et al.* [8] proposed invisible watermarking technique and a visible watermarking technique using Least Significant Bit (LSB) algorithm, which replaces the least significant bits of pixels selected to hide the information. They applied various attacks on the watermarked image and their impact on quality of images are measured using MSE and PSNR. Koushik Pal *et al.* [9] proposed biomedical image watermarking technique, modified bit replacement algorithm in spatial domain, which is much better than the conventional simple LSB technique. They embedded multiple copies of the same information in several bits of the cover image starting from the lower order to the higher orders. So even if some of the information is lost due to an attack , they still collect the remaining information and recover the watermark from the cover image using the bit majority algorithm. Some author name which works on spatial domain with their features and results is shown in Table 1.

Table 1. SPATIAL DOMAIN TECHNIQUE

AUTHOR NAME	FEATURES	RESULT
Mohamed Ali HAJJAJI *et al.* [7]	Data insertion: i) SHA-1 (Secure Hash Algorithme) ii) Error Correcting Code (ECC): Turbo Code Data detection: Harris Corner Detector	For 10% compression rate, the watermark is successfully recovered (for the IRM and Echographic medical images).
Puneet Kr Sharma and Rajni [1]	i) Pseudo-random number generator ii) LSB embedding algorithm	LSB or 1st Bit Substitution PSNR = 55.8784 & MSE = 0.1680 8th Bit Substitution PSNR = 14.3467 & MSE = 2.3900e+003
Chopra *et al.* [8]	Least Significant Bit (LSB) algorithm	LSB or 1st Bit Substitution PSNR = 54.87 & MSE = 0.21 MSB or 8th Bit Substitution PSNR = 14.3467 &

		MSE = 2.3900e+003
Sharma *et al.* [16]	i)A pseudo random number generator ii)The information hiding and extraction system iii)Visual Cryptography iv)Two different cover images are used for covering the secret share	Watermarked image for baboons PSNR(with one LSB) (db) = 54.45 PSNR(with three LSB) (db)= 44.15 Watermarked image for leena PSNR(with one LSB) (db) = 51.15 PSNR(with three LSB) (db)= 44.17

4.2 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. Discrete Cosine Transformation (DCT), Discrete Fourier Transformation (DFT) and Discrete Wavelet Transformation (DWT) are the three main methods of data transformation. This technique is complex and watermark cannot be easily recovered at the receiver end as compared to the spatial domain technique.

Xiang-Gen Xia *et al*. [10] proposed a watermarking technique based on the Discrete Wavelet Transform (DWT). They performs two–level decomposition using the Haar wavelet filters. The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the DWT transformed image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire. This technique proved to be more robust than the DCT method when embedded zero-tree wavelet compression and halftoning were performed on the watermarked images. Maha Sharkas *et al*. [11] Senior Members IEEE, proposed a dual digital image watermarking technique for improved protection and robustness. They applied frequency domain technique (DWT) into the primary watermark image and then embedded secondary watermark in the form of a PN sequence. The resulting image is embedded into the original image to get the watermarked image. They applied compression, low pass filtering, salt and pepper noise and luminance change attack into the watermarked image to increase the robustness of the technique. In all four attacks secondary watermark was detectable. Cheng *et al*. [12] proposed an algorithm which was based on embedding the watermark image in three times at three different frequency bands, namely, low, medium and high and the results proved that the watermark cannot be totally destroyed by either low pass, medium or high pass filter. P.Ramana Reddy *et al*. [13] proposed an algorithm that embeds and extracts the watermark in frequency domain and it is checked for salt and pepper & Gaussian noise attacks. They applied watermark in the DWT coefficients of the original image.

$$I_w(x,y)= I(x,y) +k.w(x,y) \quad (1)$$

Where $I_w(x,y)$ represents watermarked image, k denotes the gain factor. Robustnest of the watermarked image increases with the increase in gain k but the quality of the final watermarked image is reduced. Preeti Gupta, [14], proposed cryptography based blind image watermarking technique that embed more number of watermark bits in the gray scale cover image. They applied blind watermarking technique that uses watermark nesting and encryption. An extra watermark is embedded into the main watermark then main watermark is embedded into the DWT domain of the cover image. This technique embeds more number of bits in the cover image. Mistry, [15], proposed digital image watermarking and compared different digital watermarking methods. Image or video is embedded information data within an insensible form for human visual system but in a way that protects from attacks such as common image processing techniques. This paper introduced Spatial domain (like LSB) and transform domain (like DCT, DWT) methods. Authors found that DCT and DWT watermarking is comparatively much better but complex than the spatial domain encoding. Some author name which works on frequency domain with their features and results is shown in Table 2.

Table 2:FREQUENCY DOMAIN TECHNIQUE

AUTHOR NAME	FEATURES	RESULT
Harpuneet Kaur [3]	i) Watermark nesting (at level 2), Means embed one watermark in other and encryption. ii) Used DWT based technique	PSNR of main watermark after embedding watermark1 in it = 17.3239 dB PSNR of gray scale cover image after embedding watermarked watermark = 37.1587dB
Xia-mu Niu *et al.* [17]	i)Gray level digital watermark ii) Stack filter's threshold decomposition technique iii) DCT	PSNR = 30.7 dB Disadv- due to the multiple watermarks, the PSNR of the watermarked image isnot very high compared with traditional method.
Xiang-Gen Xia *et al.* [10]	i)Multiresolution watermarking method,	They test algorithm with common image

	ii)DWT, iii)Pseudo-random codes, iv) Haar DWT	distortions. Signature can be detected using DWT compared to DCT approach.
Maha Sharkas *et al.* [11]	i)Dual watermarking technique ii) DWT domain	PSNR = 44.1065dB Disadv-Secondary watermark was still detectable when multi threshold DWT tech was applied on the watermarked image.

Table 1 and Table 2 shows comparision of two digital image watermarking techniques, which is based on PSNR values and their results. From table it is clear that we cannot embed too much data in the frequency domain because the quality of the host image will be distorted significantly. And also complexity of embedding and extracting watermark in frequency domain is increases and more difficult compared to spatial domain. Spatial domain provides successful recovery of watermark at receiver end.

Here different watermarking methods have been presented . Most watermarking methods are based on small, pseudorandom changes are applied to selected Coefficients in the spatial or transform domain. Spatial domain watermarking schemes are in general less robust toward noise like attacks [5]. But the big advantage of using Spatial domain watermarking schemes is that the watermark may easily be recovered if the image has been cropped or translated. This is less obvious if the frequency domain is used. Cropping in the spatial domain results in a substantially large distortion in the frequency domain, which usually destroys the embedded watermark. In the case of DCT domain, if DCT blocks are watermarked, it is important to know the block position for successful watermark decoding. The similar drawbacks in the case of wavelet domain, because the wavelet transform is neither shift nor rotation invariant. Due to the simplicity and efficiency of the spatial domain, watermark in the spatial domain is most used.

5. CONCLUSION

Different techniques of digital image watermarking, based on spatial and frequency domain techniques have been discussed. On the basis of above survey it is clear that spatial domain is most widely used technique because the watermark can successfully & easily be recovered if the image has been cropped or translated. as compared to frequency domain.

On the other hand frequency domain provides more security but at the same time recovery of watermark at the receiver end is more difficult because the complexity increases. Successful recovery of watermark cannot be provided by the frequency domain techniques.

6. RESULT

Literature survey shows that the watermark may be of visible or invisible type and each method has its own strengths and weaknesses.The quality of watermarked images is measured in terms of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error). In ideal case the value of PSNR & MSE should be infinite and zero respectively . But it is not possible for watermarked image. So, large PSNR and small MSE is desirable.

7. REFERENCES

[1] Puneet Kr Sharma and Rajni, "*Analysis of Image Watermarking using Least Significant Bit Algorithm*" International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012, pp. 95-101.

[2] Manpreet Kaur , Sonika Jindal , Sunny Behal "*A Study of Digital Image Watermarking*" IJREAS Volume 2, Issue 2 (February 2012) ISSN: 2249-3905, pp. 126-136.

[3] Harpuneet Kaur, "*Robust Image Watermarking Technique to Increase Security and Capacity of Watermark Data*" Computer Science & Engineering Department, Thapar Institute of Engineering & Technology. May 2006, pp. 1-69.

[4] A. Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidi (Oct. 2001), "*A survey on watermarking application scenarios and related attacks*", IEEE international Conference on Image Processing, Vol. 3, pp. 991– 993.

[5] Frank Hartung, Martin Kutter, "*Multimedia Watermarking Techniques*", Proceedings of
The IEEE, July 1999, Vol. 87, No. 7, pp. 1085 – 1103.

[6] R. Schyndel, A. Tirkel, and C. Osborne, "*A Digital Watermark*," *Proc. IEEE Int. Conf. on Image Processing*, Nov. 1994, vol. II, pp. 86-90.

[7] Mohamed Ali HAJJAJI Abdellatif MTIBAA El-bey BOURENNANE, "*A Watermarking of Medical Image: Method Based "LSB"*", Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 12, December 2011, ISSN 2079-8407, pp. 714-721.

[8] Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C., Anil Gupta, "*Lsb Based Digital Image Watermarking For Gray Scale Image*" IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1 (Sep-Oct. 2012), pp. 36-41.

[9] Koushik Pal, Goutam Ghosh, Mahua Bhattacharya, *" A Comparative Study between LSB and Modified Bit Replacement (MBR) Watermarking Technique in Spatial Domain for Biomedical Image Security"* International Journal of Computer Applications and Technology (2278 - 8298) Volume 1 – Issue 1, 2012, pp. 30-39

[10] Xiang-Gen Xia, Charles G. Boncelet, and Gonzalo R. Arce, "*A Multiresolution Watermark for Digital Images*" Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 548-551.

[11] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy, Senior Member IEEE, "*A Dual Digital-Image Watermarking*

Technique" World Academy of Science, Engineering and Technology 5 2005, pp. 136-139.

[12] Lu, W., Lu, H. and Chung, F.L. (2006) "*Robust digital image watermarking based on subsampling*" Applied Mathematics and Computation, vol. 181, pp. 886-893.

[13] P.Ramana Reddy, Munaga. V.N.K. Prasad, D. Sreenivasa Rao, "*Robust Digital Watermarking of Color Images under Noise attacks*" International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009, pp. 334-338.

[14] Preeti Gupta, "*Cryptography based digital image watermarking algorithm to increase security of watermark data*" International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September 2012 1 ISSN 2229-5518, pp. 1-4.

[15] Darshana Mistry, "*Comparison of Digital Water Marking methods*," 21st Computer Science Seminar SA1-T1-7. IJCSE, Vol. 02, No. 09, ISSN : 0975-3397 , 2010, pp. 2905-2909.

[16] Mr. Abhay Sharma, Mrs. Rekha Chaturvedi, Mr. Naveen Hemrajani, Mr. Dinesh Goyal, *" New Improved and Robust Watermarking Technique based on 3rdLSB substitution method*" International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012 ISSN 2250-3153, pp. 1-4.

[17] Xia-mu Niu, Zhe-ming Lu and Sheng-ho Sun, "*Digital Watermarking of Still Images with Gray-Level Digital Watermarks*" Department of Automatic Test and Control Harbin lnstitute of Technology Harbin, P. R. China, IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, February 2000, pp. 137-145.