High Frequency Component based Addition Algorithm of Digital Image Watermarking

Amol R. Madane Research Scholar, JJT University, Jhunjhunu, Rajasthan-333 001, India Uttam D. Kolekar Research Guide, Parshvanath College of Engineering, Thane (W), Mumbai-400 615, India

ABSTRACT

This paper gives the idea of the method digital image watermarking algorithm which is new popular topic for research. The Discrete wavelet is the tool used for digital image watermarking. Wavelet transform has been applied widely in watermarking research as its excellent multiresolution analysis property. The watermark logo is embedded based on the frequency coefficients of the discrete wavelet transform. The detailed wavelet coefficients of high frequency band of the host image are altered by the watermark logo. The algorithm has been tested for different types of host images under the presence of attacks like Jpeg compression, bit planer reduction, cropping, warping etc. The watermark logo is added in the host image in frequency domain which gets spread over the whole part of the host image in time domain. The existing system is robust to provide the security.

General Terms

Digital image watermarking, discrete wavelet transforms, security, algorithms.

Keywords

Correlation Coefficients, Discrete Wavelet Transform, Inverse Discrete Wavelet Transform, Mean Square Error, Peak Signal to Noise Ratio.

1. INTRODUCTION

Digital image watermarking describes methods and technologies that hide secrete information in the host image. For example, image or text in digital media, such as images, video or audio. 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. The hiding process has to be such that the modifications of the media are imperceptible to the human eye. For images this means that the modifications of the pixel values have to be invisible. Furthermore, the watermark must be either robust or fragile, depending on the application. In case of robust watermark, we mean the capability of the watermark to resist manipulations of the media, such as lossy compression (where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, just to enumerate some. In some cases, the watermark may need to be fragile. "Fragile" means that the watermark should not resist tampering, or would resist only up to a certain, predetermined extent.

In this paper, we will discuss the addition algorithm of watermarking using Discrete Wavelet Transform (DWT). Section 2 reviews the literature survey on digital image watermarking using DWT. Section 3 will define the problem. Section 4 discusses the proposed algorithm. Section 5 will give an idea about the performance parameters used to check

the robustness, imperceptibility of the algorithm. Section 6 discusses the results and summary of discussion.

2. LITERATURE SURVEY

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. 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. Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

Mauro Barni, Franco Bartolini, Alessandro Piva[1] explain the improved wavelet-based watermarking through pixel wise masking. In [2], authors highlighted that the invisible digital image watermarking can carry the significant information. Authors [3] discussed the algorithm to increase the robustness and protection. In paper [4], A. Essaouabi, E. Ibnelhaj, F. Regragui explained watermarking scheme that can embed a watermark to an arbitrarily shaped object in an image. Authors [5] presented a method for digital image watermarking using Biorthogonal wavelet transform. A DWT based algorithm is proposed in [6] where in both blind and non-blind algorithms are used for copyright protection. In [7], authors successfully explained the digital image watermarking technique on digital images based on discrete wavelet transform by analyzing various values of PSNR's and MSE's.

3. PROBLEM DEFINITION

In the previously published algorithms, the secrete information are inserted in the host image by different tools which are present in the market. This type of applications can be used for copyright protection and authentication purpose.

The proposed algorithm provides new approach to add the secrete information in the host image to improve the chances of copyright protection and robustness of algorithm. The performance of proposed algorithm is better than the previously published algorithms if we compare the performance parameters as peak signal to noise ratio, mean square error, and correlation coefficient.

4. PROPOSED ALGORITHMS

4.1 Embedding Algorithm

- a) Consider any square gray scale image.
- b) Decompose the input image by using 2D discrete wavelet transform (DWT). Store the first level approximation coefficients i.e. ILL₁, horizontal coefficient ILH₁, vertical coefficient IHL₁, diagonal coefficient IHH₁ as first level watermark key coefficients of input image.
- c) Approximation coefficient of first level of input image is ILL₁ which is further decomposed into new coefficients i.e. ILL₂, horizontal coefficient ILH₂, vertical coefficient IHL₂, diagonal coefficient IHH₂ as second level watermark key coefficients of input image using 2D discrete wavelet transform.
- d) Approximation coefficient of second level of input image is ILL₂ which is further decomposed into new coefficients i.e. ILL₃, horizontal coefficient ILH₃, vertical coefficient IHL₃, diagonal coefficient IHH₃ as third level watermark key coefficients of input image using 2D discrete wavelet transform.
- e) Consider the secrete information.
- f) Decompose the secrete information by using 2D discrete wavelet transform. Store the first level approximation coefficients i.e. SLL₁, horizontal coefficient SLH₁, vertical coefficient SHL₁, diagonal coefficient SHH₁ as first level watermark key coefficients of secrete information.
- g) Approximation coefficient of first level of secrete information is SLL₁ which is further decomposed into new coefficients i.e. SLL₂, horizontal coefficient SLH₂, vertical coefficient SHL₂, diagonal coefficient SHH₂ as second level watermark key coefficients of secrete information using 2D discrete wavelet transform.
- h) Reduce the intensity value of third level horizontal coefficient of input image and low frequency part of second level of secrete information to half; since it is used as a watermark keys while extraction of secrete information.
- Add the updated part of low frequency component of secrete information into the high frequency component of third level of input image pixel by pixel.
- j) Perform the three level 2D inverse discrete wavelet transform (IDWT) of input image by using approximation coefficients of input image to find the invisible watermark image using addition algorithm. Gray scale invisible watermark image is obtained, which is perceptually equal to original input image.
- k) Find the mean square error (MSE), peak signal to noise ratio (PSNR) and correlation coefficient (CC) in between the original input image and invisible watermark image by using the related formulae as these are the important performance parameters.
- We can make program generalize as per the size is concern i.e. we can change the size of input image and secrete information by changing the size parameters in program. But only essential condition is that both images should be square images.

4.2 Secrete Information Extraction Algorithm

- a) Consider invisible watermark image as input image or input image having size 512 X 512.
- b) Decompose the invisible watermark image by using 2D discrete wavelet transform. Then we will get the first level approximation coefficients i.e. InverseLL₁, horizontal coefficient InverseLH₁, vertical coefficient InverseHL₁, diagonal coefficient InverseHH₁ as first level watermark key coefficients of invisible watermark image.
- c) Approximation coefficient of first level is InverseLL₁ which is further decomposed into new coefficients i.e. InverseLL₂, horizontal coefficient InverseLH₂, vertical coefficient InverseHH₂ as second level watermark key coefficients of invisible watermark image.
- d) Approximation coefficient of second level is InverseLL₂ which is further decomposed into new coefficients i.e. InverseLL₃, horizontal coefficient InverseLH₃, vertical coefficient InverseHL₃, diagonal coefficient InverseHH₃ as third level watermark key coefficients of invisible watermark image.
- e) Consider the InverseHH₃ part of invisible watermark image, subtract the IHH₃mod from current InverseHH₂ part and multiply by the scaling factor to get NewSLL₂.
- f) Perform the two level 2D inverse discrete wavelet transform (IDWT) of secrete information by using approximation coefficients of secrete information to find the secrete information using addition algorithm. Gray scale secrete information is obtained, which is perceptually equal to secrete information.
- g) Find the mean square error (MSE), peak signal to noise ratio (PSNR) and correlation coefficient (CC) in between the original secrete information and extracted secrete information by using the related formulae as these are the important performance parameters.

5. PERFORMANCE PARAMETERS

The performance parameters used for comparing the results are Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and Correlation Coefficients (CC). The imperceptibility of a watermark is measured by the watermarked image quality in terms of Peak-Signal-to-Noise Ratio (PSNR) (in dB) [9]. The robustness performance of watermark extraction is evaluated by normalized correlation coefficient, r, of the extracted watermark A and the original watermark B.

$\gamma = X/Y$

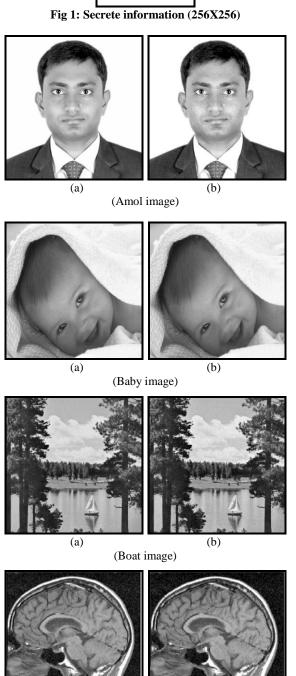
where $X = (\sum (A(m,n)-A')(B(m,n)-B')$ $Y = \sqrt{(\sum (A(m,n)-A')^{2*} \sum (B(m,n)-B')^{2}})$

A and B respectively, the normalized original and extracted watermark by subtracting its corresponding means value. The magnitude range of r is [0, 1], and the unity holds if the extracted image perfectly matches the original one. The difference between host image and watermark image or watermark logo and extracted watermark logo can be found by using the factor mean square error. It is better to have the value less as possible.

6. RESULT AND DISCUSSION

The above algorithm has been tested on the different types of host/input images. The gray scale secrete information used for experimentation purpose is as shown in figure 1. Figure 2 gives basic idea about the different input images, its respective invisible digital watermark images.

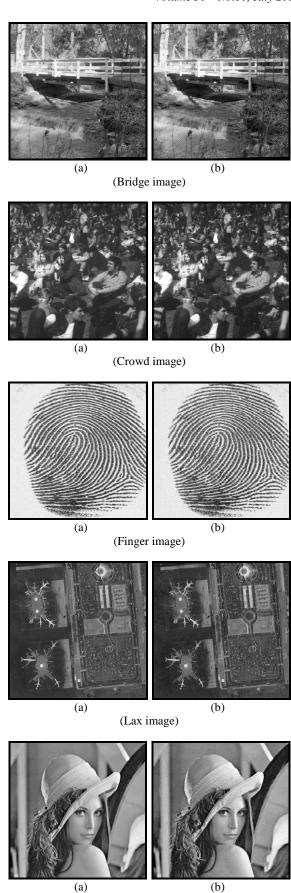




(a)

(Brain image)

(b)



(Lena image)

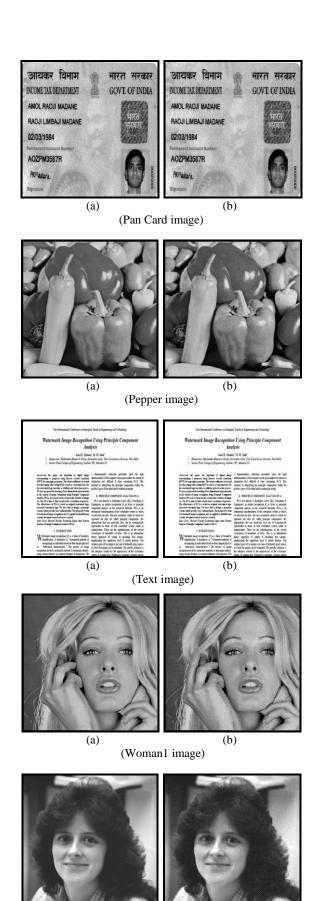


Figure 2: (a) Input Image (512X512), (b) Invisible Digital Watermark Image (512X512)

(Woman2 image)

(b)

(a)

As a next step, we have calculated the performance parameters to check the robustness of our algorithm. Table 1 shows the values of peak signal to noise ratio, mean square error, correlation coefficient between original image and the invisible watermark image. If we compare the image input image with the invisible watermark image, both the image looks like as same image. The secrete information is perceptually invisible in watermark image i.e. invisible watermark image.

Table 1. Performance parameters for original image and invisible watermark image

Input Image	Watermark Image		
	PSNR	MSE	CC
Amol	78.2167	9.7275e-004	0.9972
Baby	78.2508	9.7275e-004	0.9954
Boat	78.0090	9.7275e-004	0.9924
Brain	78.2508	9.7275e-004	0.9910
Bridge	78.2508	9.7275e-004	0.9901
Crowd	78.2508	9.7275e-004	0.9878
Finger	78.2508	9.7275e-004	0.9747
Lax	77.6880	9.7275e-004	0.9787
Lena	78.2508	9.7275e-004	0.9902
Pancard	78.2508	9.7275e-004	0.9875
Peppers	77.2405	9.7275e-004	0.9920
Text	78.2167	9.7275e-004	0.9921
Woman1	76.1839	9.7275e-004	0.9868
Woman2	78.2167	9.7275e-004	0.9951

Then, the secrete information extracted from invisible watermark image with the help of extraction algorithm. Table 2 gives the values of performance parameters of secrete information and the extracted secrete information.

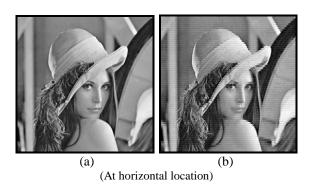
Table 2. Performance parameters for secrete information and the extracted secrete information

Input Image	Extracted Secrete Information			
	PSNR	MSE	CC	
Amol	72.2302	0.0031	0. 9412	
Baby	72.2302	0.0035	0.9945	
Boat	72.2302	0.0037	0.9967	
Brain	72.2302	0.0045	0.9754	
Bridge	72.2302	0.0039	0.9948	
Crowd	72.2302	0.0043	0.9864	
Finger	72.2302	0.0039	0.9968	
Lax	72.2302	0.0022	0.9967	
Lena	72.2302	0.0021	0. 9959	
Pancard	72.2302	0.0039	0. 9880	
Peppers	72.2302	0.0039	0.9961	
Text	72.2302	0.0049	0.6887	
Woman1	72.2302	0.0039	0.9904	
Woman2	72.2302	0.0032	0.9949	

Table 3. Performance parameters for original image and invisible watermark image after adding at different locations

Added the	Watermark Image (Lena Image)			
Secrete	PSNR	MSE	CC	
Information in				
Horizontal (H3)	78.2508	9.7275e-004	0.9861	
Diagonal (D3)	78.2508	9.7275e-004	0.9902	
Vertical (V3)	78.2508	9.7275e-004	0.9721	

If we compare the values of performance parameters from table 1 and table 2, Lena image gives better results in both the cases (watermark image and secrete information). So, we have chosen Lena image for future work this algorithm.





(a) (b) (At vertical location)

Figure 3: (a) Input Image (512X512), (b) Invisible Digital Watermark Image (512X512)

Table 4. Performance parameters for secrete information and the extracted secrete information found out from different locations

Added the	Secrete Information (Lena Image			
Secrete Information in	PSNR	MSE	CC	
Horizontal (H3)	78.2508	9.7275e-004	0.9861	
Diagonal (D3)	78.2508	9.7275e-004	0.9902	
Vertical (V3)	78.2508	9.7275e-004	0.9721	

As a next steps, we have added the secrete information at different levels of third level discrete wavelet transform image i.e. in horizontal component, diagonal component, vertical component. We are getting the best performance at diagonal level. That's why, we have chosen the diagonal place to add the secrete information. The main reason is the diagonal

components are the high frequency component which carries low information.

7. CONCLUSION

We have designed the system for digital image watermarking with a given secrete information into discrete wavelet transform as tool. The system provides for a MSE, PSNR and normalized correlation coefficient that determine the robustness of the secrete information in digital image. This is necessary in the case of fragile watermarks as they can be easily removed by basic image transformations. In such a case the imperceptibility of the watermark helps protect it from malicious attacks and provides the copyright protection. The robust secrete information is embedded in the wavelet coefficients of third level diagonal band of host image to strengthen the information and against various attacks such filtering, data compressing, and other malicious modification etc. The developed application also detects and extracts an embedded secrete information from a digital image.

8. REFERENCES

- [1] Barni Mauro, Bartolini Franco, Piva Alessandro 2001, "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking", IEEE Transaction on Image Processing, pp. 783-791, Vol. 10, No. 5, May 2001.
- [2] Premaratne Prashan, DeSilva Liyanage and Burnett Ian 2006, "Low Frequency Component-Based Watermarking Scheme Using 2D Datamatrix", International Journal of Information Technology, pp. 1-12, Vol. 12, No. 7, November 2006.
- [3] Sharkas Maha, ElShafie Dahlia and Hamdy Nadder 2007, "A Dual Digital-Image Watermarking Technique", Journal of World Academy of Science, Engineering and Technology, pp. 136-139, Vol. 5, No. 1, May 2007.
- [4] Essaouabi A., Ibnelhaj E. and Regragui F. 2009, "Digital Image Watermarking for Arbitrarily Shaped Objects Based on SA-DWT", International Journal of Computer Science Issues, pp. 1-8, Vol. 5, No. 1, October 2009.
- [5] Hajjara Suhad, Abdallah Moussa and Hudaib Amjad 2009, "Digital Image Watermarking Using Localized Biorthogonal Wavelets", European Journal of Scientific Research, pp. 594-608, Vol. 26, No. 4, February 2009.
- [6] Tripathi Shikha, Ramesh Nishanth, Bernito and Neeraj K J 2010, "A DWT based Dual Image Watermarking Technique for Authenticity and Watermark Protection", International Journal of Signal and Image Processing, pp. 33-45, Vol. 1, No. 2, December 2010.
- [7] Singh Akhil Pratap and Mishra Agya 2010, "Wavelet Based Watermarking on Digital Image", Indian Journal of Computer Science and Engineering, pp. 86-91, Vol. 1, No. 2, August-September 2010.
- [8] Kumar Amitesh and Santhi V. 2011, "A Review on Geometric Invariant Digital Image Watermarking Techniques", International Journal of Computer Applications, pp. 0975–8887, Vol. 12, No. 9, January 2011.
- [9] Zhang Fan and Zhang Hongbin 2004. "Image Digital Watermarking Capacity and Reliability Analysis in Wavelet Domain", IEEE Proceedings of 47th Midwest symposium on Circuits and Systems, pp. 101-104, Jul 2004.