ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Invisible Image Watermarking using DWT

Anshuja Wandile, Amit V. Kulkarni

M.E. Student, Department of Electronics (VLSI and Embedded), MIT Academy of Engineering, Pune, Maharashtra, India[1]

Assistant Professor, Department of Electronics, MIT Academy of Engineering, Pune, Maharashtra, India[2]

ABSTRACT: This paper introduces an algorithm of digital watermarking based on Discrete Wavelet Transform (DWT). A lossless data hiding scheme is presented based on quantized coefficients of discrete wavelet transform (DWT) in the frequency domain to insert undisclosed message. We had developed watermarking schema which uses DWT algorithm to embed the watermark and to extract watermark we have use DWT and thresholding. The results show that this system is make watermark invisible and has good robustness for various attacks such as sharpening attack, various noise attacks, histogram attack etc**.** The various statistical parameters are also calculated to check robustness of algorithm such as PSNR, MSE, FOR (Fitness of recovery).

KEYWORDS: Fitness of Recovery (FOR), Discrete Wavelet Transform (DWT).

I. INTRODUCTION

In recent years, almost everyone uses digital multimedia technologies for storing and sharing videos, images and information in many more forms. Owing to this concern of security of the content becomes very vital in these days. We have to shield these computerized information from unapproved replication of information. Authentication and copyright protection, information hiding, content identification and proof ownership have also become vital issues. Watermarking is the key solution for these issues. In digital watermarking a perceptually transparent design is introduced in an image using an inserting method. It is just like signature to provide authentication or proof of ownership to the digital Content or information. It can be video, image or audio. Generically watermark message may be plain text, cipher text, logo image or any other images. Any watermarking algorithm consists of embedding algorithm and detection (extraction) algorithm.

Digital image watermarking techniques are classified into two broad categories Spatial Domain Watermarking and Frequency Domain Watermarking. In spatial domain, the watermark image is added by manipulating pixel values of original image. Least Significant Bit insertion is example of spatial domain watermarking. But such algorithms have very less information hiding capacity, they can be easily discovered and quality of watermarked image and extracted watermark is not satisfactory as pixel intensities are directly changed in these algorithms [1]. In Frequency domain the watermark is inserted into transformed coefficients of image giving more information hiding capacity and more robustness against watermarking attacks [2].

Spatial domain based watermarking techniques are rarely preferred over transform domain based watermarking techniques because the watermark placed by them can be easily destroyed and modified by the attackers [3]. Watermarking in frequency domain is highly robust than watermarking in spatial domain because information can be spread out to whole image. For frequency transform, we are having different options like: Fourier Transform (FT), and Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Combination of DCT and DWT. However, DWT has been used in digital image watermarking more frequently due to its excellent spatial localization and multi-resolution uniqueness, which are similar to the hypothetical models of the human illustration system. Further performance improvements in DWT-based digital image watermarking algorithms could be obtained by increasing the level of DWT [4].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

II. Related work

Many watermarking methods have been proposed in the literature. Schyndel Tirkel, and Osborne [5] generated a watermark using a m-sequence generator. They embedded the watermark to the least significant bit of the original image to produce the watermarked image. They extracted the watermark from a suspected image by taking the least significant bits at the proper locations. Detection had been performed by a cross-correlation of the original and extracted watermark. Schyndel et al. showed with simple extraction procedures that the resulting image contain an invisible watermark. For the additive noise, the watermark was not robust. Cox et al. [6] noted that, watermark should be placed in perceptually significant areas of the image for a watermark to be robust to attack. The watermark had 1000 random samples of N (0, 1) distribution. These samples were added to the 1000 largest DCT coefficients of the original image, and the inverse DCT retrieved the watermarked image. In detection, the watermark was extracted from the DCT of a suspected image. They performed the extraction on the basis of knowledge of the original signal and the exact frequency locations of the watermark. They calculated the correlation coefficient and set to a threshold. The watermark was detected only if the correlation was large enough. The method was robust to image rescanning, scaling, JPEG coding, dithering, and cropping.

Xia, Boncelet, and Arce [7] proposed a watermarking scheme based on the Discrete Wavelet Transform (DWT). They added the watermark to the middle and high frequency bands of the image as Gaussian noise. In decoding process, the DWT of a potentially marked image had been taken. They extracted the watermark sections and then correlated that sections with the original watermark sections.

Bartolini*et al.* [8] first generated a watermarked image from DCT coefficients. On the new image, spatial masking was performed to hide the watermark. Kundur and Hatzinakos [9] embedded the watermark in the wavelet domain. The watermark strength was determined by the contrast sensitivity of the original image. In both techniques, the resistance to common signal processing operations had been shown. Delaigle*et al.* [10] proposed a unique watermarking scheme based on the Human Visual System. They generated the Binary m-sequences and then modulated it on a random carrier. This image was served as the watermark, and then it masked based upon the contrast between the original signal and the modulated image. To form the watermarked image, the masked watermark was added to the original image. This technique was robust to rescanning, JPEG coding, and additive noise.

Craver *et al* [11] noted that certain watermarking techniques were susceptible to counterfeit attacks. They showed that, by creating a fake original image and fake watermark that is indistinguishable from the true original image and watermark, the method proposed by Cox et al. can be attacked. For the prevention of this scenario, they modified the Cox *et al.* algorithm and made the watermark dependent on the original image. This scheme was less susceptible to counterfeiting and still maintained robustness.

III. Proposed algorithm

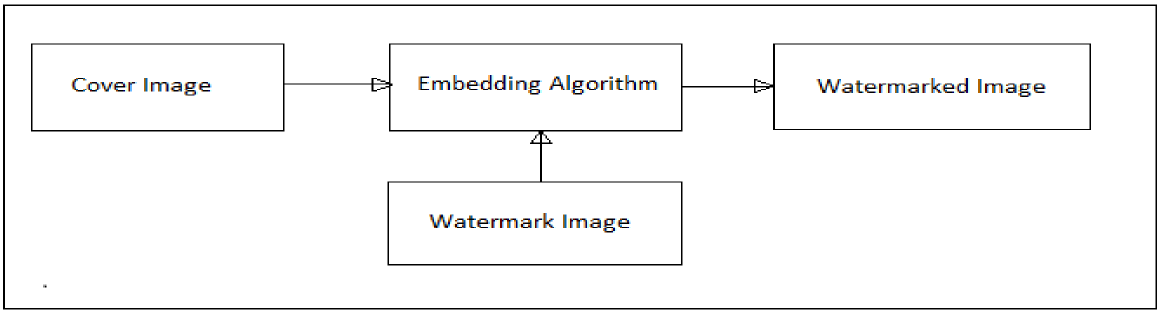

Fig. 1. Basic Watermarking Process.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

The most robust watermarking scheme is that which sustains in various attacks such as image compression, noise attack, and histogram equalization, sharpening attack, blur attack, fragile attacks.

We have proposed DWT based watermarking technique which provides good imperceptibility and high robustness against various kinds processing attacks.

The proposed watermarking technique is shown in fig.1 proposed method embeds secret message into DWT coefficients in medium high frequency components and restores the original image coefficients after the secret messages have been extracted. Wavelet transform is used to converts an image from time or spatial domain to frequency domain. Decomposition of digital image will be pair of waveform with high frequency corresponds to detailed parts of an image & low frequency to smooth parts of image.

A. *Embedding Algorithm:*

1: Set the size of image block for Embedding.
2: Read & display cover image.
3: Determine row & column size of cover image.
4: Read & display Watermark image.
5: Determine row & column size of Watermark image &resize the image.
6: Apply discrete wavelet transform to cover image. Dwt transform divide cover image into four sub bands.
7: Apply discrete wavelet transform to watermark image. Dwt transform divide cover image into four sub bands.
8: Embed the watermark image into cover image with the help of multiplication factor.
9: Apply IDWT to the embedded image.
10: Watermarked image convert into unsigned 8-bit integer.
11: Write watermarked image to file.
12: Show the watermarked image.

B. *Extracting Algorithm:*

1: Read & display watermarked image.
2: Determine row & column size of watermarked image.
3: Read & display cover image.
4: Apply discrete wavelet transform to cover image. Dwt transform divide cover image into four sub bands.
5: Apply discrete wavelet transform to watermark image. Dwt transform divide cover image into four sub bands.
6: Extract the watermark image into cover image with the help of Division factor and thresholding.
7: Apply IDWT to the Extracted image.
8: Extracted image convert into unsigned 8-bit integer.
9: Write Extracted image to file.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

IV. SIMULATION RESULTS

I. Salt and paper noise

a) b)

Figure: a) salt-n-pepper noise attacked image b) watermark extraction

Since the LL sub band gives better extraction, it is used for calculation of above parameters. The higher values of PSNR, shows that inserted watermark has very less effect on visibility, and for input and output watermark and good value of Fitness of recovery ensures better extraction of watermark.

	MSE	PSNR	PSNR in dB
For cover and watermarked image	0.001831,	35791394.133333	151.075572
For input and extracted watermark	2.882935	22732.392429	87.132903
FOR	99.287593		

Table: Proposed Result with Salt-n-Pepper Noise Attack.

The PSNR value is 151dB for cover and watermarked image and we got 99% Fitness of Recovery for the same.

II. Gaussian noise

a) b)

Figure: a) Gaussian noise attacked image b) Watermark extraction

The watermark shows good Fitness of recovery and PSNR values. Thus a good extraction of watermark, even Gaussian attack is feasible.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

	MSE	PSNR	PSNR in dB
For cover and watermarked image	0.011536	5681173.671958	135.088761
For input and extracted watermark	2.882935	22732.392429	87.132903
FOR	95.469991		

Table: Proposed Result with Gaussian Noise Attack

From above table, it can be seen that for cover and watermarked image, value of peak signal to noise ratio is 135.088 dB.

III. Image Sharpening Attack

a) b)

Figure: a) Image Sharpening attacked image b) Watermark extraction

It can been seen form above figure, that HH sub band gives better watermark extraction compared to other sub band. The same is used for parameter calculation.

	MSE	PSNR	PSNR in dB
For cover and watermarked image	0.095520	686097.012141	116.727711
For input and extracted watermark	2.882935	22732.392429	87.132903
FOR	66.766563		

Table: Proposed Result with Sharpening Attack

Above table for Sharpening Attack gives 116.727711 dB PSNR value for cover and watermarked image. The fitness of recovery is 66.76 %.

V. CONCLUSION

In this paper, discrete wavelet transform based invisible image watermarking algorithm has been designed. In this algorithm different attacks has been introduced on watermark image. The Paper Describe the Effects of different attacks on watermark image in terms of PSNR. The proposed algorithm provide the robustness in the form Fitness of recovery.

REFERENCES

1. Baisa L. Gunjal, R.R. Manthalkar, **"**An overview of transform domain robust digital image watermarking algorithms", Journal of Emerging Trends in Computing and Information Sciences, Volume 2 No. 1 ISSN 2079-8407, 2011.
2. Saied Amirgholipour Kasmani, Ahmadreza Naghsh-Nilchi, "A New Robust Digital Image Watermarking Technique Based on Joint DWT-DCT Transformation", Convergence and Hybrid Information Technology, Volume: 2, pp: 539-544, 2008.
3. Nidhi Bisla, Prachi Chaudhary**, "**Comparative Study of DWT and DWT-SVD Image Watermarking Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.
4. Nikita Kashyap, G. R. SINHA, "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)", I. J. Modern Education and Computer Science, 3, 50-56, 2012
5. R. Schyndel, A. Tirkel, and C. Osborne, "A Digital Watermark," Proc. IEEE Int. Conf. on Image Processing, vol. II, pp. 86-90, Nov. 1994.
6. M. Swanson, B. Zhu, and A. Tewfik, "Transparent Robust Image Watermarking," Proc. IEEE Int. Conf. on Image Processing, vol. III, pp. 211-214, Sept. 1996.
7. X. Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark for Digital Images," Proc. IEEE Int. Conf. on Image Processing, vol. I, pp. 548-551, Oct. 1997.
8. F. Bartolini, M. Barni, V. Cappellini, and A. Piva, "Mask Building for Perceptually Hiding Frequency Embedded Watermarks," Proc. Int. Conf. on Image Processing, vol. I, pp. 450-454, Oct. 1998.
9. D. Kundur and D. Hatzinakos, "A Robust Digital Image Watermarking Method Using Wavelet-Based Fusion," Proc. IEEE Int. Conf. on Image Processing, vol. I, pp. 544-547, Oct. 1997.
10. J. Delaigle, C. De Vleeschouwer, and B. Macq, "Psych visual Approach to Digital Picture Watermarking," Journal of Electronic Imaging, vol. 7, no. 3, pp. 628-640, July 1998.
11. S. Craver, N. Memon, B. Yeo, and M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications," IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 573-586, May 1998.

BIOGRAPHY

Anshuja Wandile is a Master of Engineering student in the Electronics Department, MIT AOE, Savitribai Phule Pune University. She received Bachelor of Engineering (BE) degree in 2012 from RTMNU, Nagpur, Maharashtra, India. Her research interests are Computer Networks (wireless Networks), Image processing etc.

Amit V. Kulkarni is an Assistant Professor in the Electronics Department, MIT AOE, Alandi, Savitribai Phule Pune University. He has done Master of Engineering in Embedded Systems and Bachelor of Engineering in Electronics and Telecommunication. He is having 10 years of teaching experience and 1.6 years of Industrial experience. His research interest is in embedded systems.