International Journal of Electronics Engineering, 1(2), 2009, pp. 149-151

Design and Implementation of a Robust Watermarking Algorithm for Image Protection

Deepti Prit Kaur[1], Jaspreet Kaur[2], Vivek Singla[3] & Mahesh K. Yadav[4]

[1]ECE, Chitkara Institute of Engg. & Tech., Punjab, P.T.U. Jalandhar, Punjab, INDIA
[2]ECE, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, INDIA
[3]CSE, Infosys Technologies Ltd, Chandigarh, INDIA
[4]ECE, BRCM College of Engg. & Tech., Bahal, M.D.U. Rohtak, Haryana, INDIA

Abstract: This paper presents *the design and implementation of a robust watermarking algorithm for protection of digital images. The recent growth in the field of multimedia has proposed many facilities in transportation, transmission and manipulation of data. Along with this advancement of facilities there are larger threats to authentication of data, its licensed use and protection against illegal use of data. Out of many schemes available for content protection, Digital watermarking is one of the most recent proposed systems to observe the authentication of licensed user by indicating whether data is containing copyright or not. Developments in the field of watermarking though have provided new ways of protecting data yet there are many factors which need to be addressed such that the algorithm is robust enough to signal processing operations (lossy compression, filtering, D/A and A/D conversion) and common geometric transformations (cropping, scaling, translation and rotation). Moreover, the algorithm should embed as many message bits as possible into the host image while preserving the properties of imperceptibility and security. We have designed a method to meet all these challenges, in which, the concept of nested watermarking is used to increase the embedding capacity. To increase security we embed encrypted watermarks in the image. Further, the use of Gaussian noise ensures strong resilience to multi- document or collusion attacks. This method is a blind watermarking recovery method (means original image and original watermark are not needed at the time of watermark extraction process).*

Keywords: *Digital Image Watermarking, Watermark, Robustness, Nested Watermarking, Attacks, Discrete Wavelet Transform (DWT), Watermarking using Spread Spectrum, Copyright Protection.*

1. INTRODUCTION

Image security has become the most popular research topic in recent years. The reason might be the increasing development of World Wide Web (www) and all the new numerical supports such as CD, DVD, and MP3 etc. which are giving new opportunities to pirate copyrighted products. There has been a huge demand for protected data, because so many images are available on www at virtually no cost, and there is a need to protect these images. There are many solutions to solve these problems, such as Cryptography, Steganography, Watermarking [1] etc. Watermarking uses the concept of data hiding and can be considered as a signature that reveals the owner of the multimedia object [2]. Watermarking methods differ in one or more aspects out of the following three topics: Signal design, Embedding, Recovery. To insert a watermark we can use spatial domain, frequency domain, wavelet domain or spread spectrum domain.

2. PROBLEM FORMULATION

There are various requirements for a watermarking system to be ideal such as Imperceptibility, Robustness, Capacity, Payload of the watermark, Security, Specificity, Inseparability and Fragility. From the study of various traditional and recent approaches that have been implemented till now, it has been observed that Spatial Domain method is the simplest algorithm to implement but is easily defeated [2]. Spread Spectrum Methods are relatively one of the best methods. The watermarked image is visually an exact copy of the original. All the DCT based approaches take similar amount of time and the results are almost equivalent to the DWT-based methods except that watermarked data can be easily lost [3]. Thus, Existing methods suffer from one or the other short comes and it seems to be difficult to increase the security and capacity simultaneously, hence the robustness of a watermark. But it can be achieved if we combine two methods together. Spread spectrum and discrete wavelet transform method are chosen for this as these two are relatively better methods against all kinds of attacks.

3. ALGORITHM DEPLOYED

The new algorithm presented here will provide additional level of security because now the watermark itself will be encrypted and algorithm is robust enough against any attacks. While designing the scheme, following important points are taken care of:

*Corresponding Author: deepti.hunjan@gmail.com

- To increase capacity the concept of nesting [4] is used with a difference. Here we embed one watermark in other in spread spectrum domain.
- To increase security of watermark cryptography [5] is used.
- For embedding the watermarked watermark in cover image, DWT technique is used for increase in robustness.
- Before embedding watermarks at both levels we encrypt them with XOR operation. XOR has one important property: if we XOR the data twice with same key we get the original data again. This property of XOR is used for encryption and decryption.

3.1. Watermark Insertion Algorithm

1. We take Watermark1 (WM1 in the Figure 1) and encrypt it by performing XOR operation with the Encryption key EN1. Let the output of this step be WE1.
2. Embed WE1 in the second binary watermark image (WM2) using key W1. Let output image is WW.
3. Again encrypt WW using XOR with Encryption key EN2 to give the output image WE2.
4. Embed WE2 in the gray-scale Cover Image using key W2. Output image is final watermarked image (FWI). The keys are used to embed an image into the other.

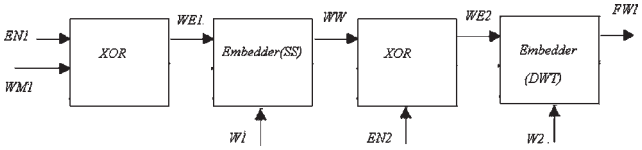

Figure 1: Watermark Insertion

3.2. Watermark Extraction Algorithm

1. Extract the encrypted watermark 2 (i.e. WE2 in Figure 2) from received watermarked image using key W2. Let the recovered image is WE2'.
2. Decrypt WE2' by performing its XOR operation with key EN2. Output of this step is called RW2.
3. Extract the encrypted watermark1 (i.e. WE1) from RW2 using key W1. Let the output be WE1'.
4. Decrypt WE1' by performing its XOR with key EN1. Output of this step is called RW1.

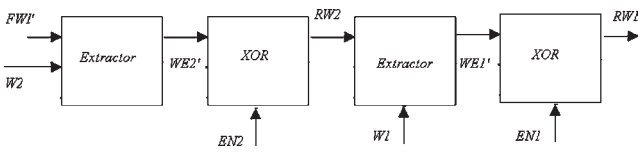

Figure 2: Watermark Extraction

4. EXPERIMENTAL RESULTS

Experimental results are given in support of the claims made in the paper. Images of different sizes have been used as cover images as shown in Figure 1-7. Simulation results for one of these are as follows:

Figure 3: Watermark 1

Figure 4: Watermark 2

Figure 5: Cover Image

Figure 6: Watermarked Image

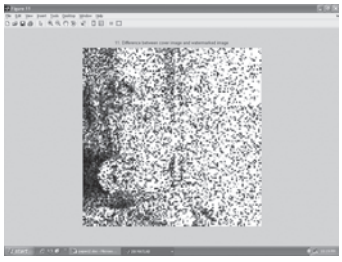

Figure 7: Difference (of cover and watermarked) Image

On application of mentioned attacks on the watermarked image, the picture quality is not degraded, that means the watermark is able to withstand various attacks. Following results are given as Figure 8-13 in support of the claims:

Figure 8: 180 Degrees Flip

Figure 9: Cropping

Figure 10: Scaling

Figure 11: Filtering

Figure 12: Transformation

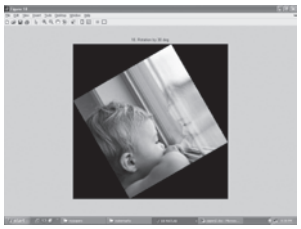

Figure 13: 30 Degree Rotation

The quality of any watermarked image is measured in terms of Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The relation between the two is given by:

$$PSNR = 10 \log_{10}((255)^2 / MSE) \text{ dB}$$

Ideally it is desirable to have infinite PSNR & Zero MSE but as it is not possible to have such results for watermarked images so large PSNR and small MSE is acceptable to verify similarity between original and watermarked images. Samples of 3 images were taken for experimental purpose and following results were obtained:

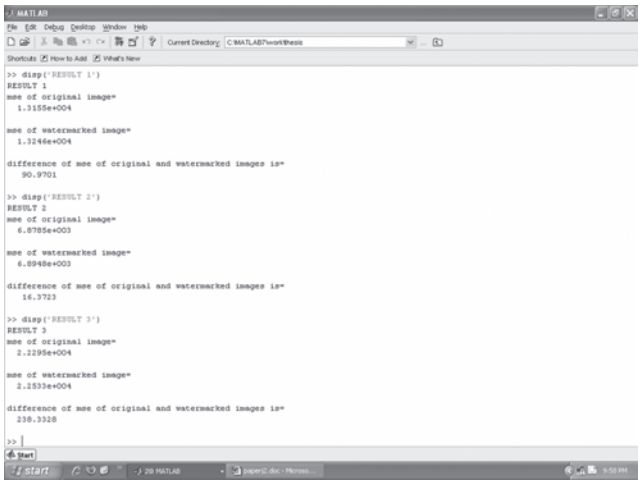

Figure 14: MSE Results for Different Cover Images

5. CONCLUSION

Based on nested watermarking in Spread Spectrum and Wavelet Domain, a Robust Watermarking scheme is designed to survive both common signal processing and geometrical attacks. There are several key elements in this scheme, which are as follows:

- Using watermark nesting we can embed more number of bits in the cover image and some metadata about watermark also.
- Because our technique uses encryption, so it increases the security of watermarks.
- It is a blind watermarking technique. So, original images as well as the original watermark are not required at the time of watermark detection process.
- Because we are using Spread Spectrum based technique for embedding watermark in watermark so this technique is providing an additional level of security against any intentional attack by the hacker.
- Because we embed final watermark in DWT domain, so this technique is robust against many unintentional attacks.

REFERENCES:

[1] Chris Shoemaker, Hidden Bits: A Survey of Techniques for Digital Watermarking, Independent Study, (2002).

[2] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, A Survey of Digital Image Watermarking Techniques, 3rd IEEE International Conference on Industrial Informatics (INDIN), (2005), 709-716.

[3] Na Li, Xiashi Zheng, Yanling Zhao, Huimin Wu, Shifeng Li, Robust Algorithm of Digital Image Watermarking based on Discrete Wavelet Transform, *IEEE International Symposium on Electronic Commerce and Security*, (2008), 942-945.

[4] Feng-Hsing Wang, Lakhmi C. Jain, Jeng-Shyang Pan, IEEE Hiding Watermark in Watermark, *IEEE*, (2005), 4-8.

[5] Jian Ren, TongTong Li, Mehrdad Nadooshan, A Cryptographic Watermark Embedding Technique, *IEEE*, (2004), 382-386.

[6] XU Duan-quan, ZHU Guang-xi, An Algorithm to Improve the Performance of Watermarking Systems, 2008 Congress on Image & Signal Processing, *IEEE*, (2008), 664-668.

[7] Deepti Prit Kaur, Jaspreet Kaur, Kamaldeep Kaur, Digital Image Watermarking: Challenges and Approach for a Robust Algorithm, *IJEE, International Journal of Electronics Engineering*, **1**(1), (2009), 95-97.