International Journal of Electronics Engineering, 1(1), 2009, pp. 95-97

Digital Image Watermarking: Challenges and Approach for a Robust Algorithm

Deepti Prit Kaur, Jaspreet Kaur & Kamal Deep

ECE, P.T.U. Jalandhar, Punjab, INDIA

Abstract: *This paper presents the challenges for a robust digital image watermarking algorithm. Need for copyright protection in digital media has led to enormous growth in the field of Digital Image Watermarking whereby researchers are striving to come up with new ways of content protection. Recent 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 of embedding/ extracting a watermark is robust enough to meet these challenges. Robustness can be defined as resilience for a watermark to remain unaffected even when digital content is passed through various processes and attacks and hence increase security, capacity, and imperceptibility of watermarked data. The paper begins with a brief introduction to cryptography and Steganography, which is the platform for a number of digital watermarking concepts. Then, requirements for watermarking systems are discussed along with methods to watermark data efficiently and their strengths and weaknesses. In conclusion there is a new method proposed which uses a concept of nested watermarks using Discrete Wavelet Transform for binary images and Cryptography using Spread Spectrum technique and is supposed to be robust enough to cater to challenges presented here.*

Keywords: *Digital Image Watermarking, Watermark, Challenges to Robustness, Robustness, Nested Watermarking, Attacks, Discrete Wavelet Transform (DWT), Watermarking using spread spectrum, copyright protection.*

1. INTRODUCTION

The advancement in digital multimedia technologies has facilitated the transmission, manipulation & reproduction of data presented in digital form. But this progress has also led to the challenges such as copyright protection, content authentication etc. 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]. The hiding process has been illustrated in Fig.1.

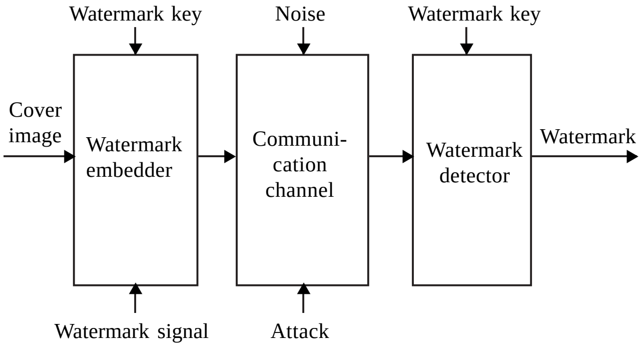

Figure 1: Generic Watermarking Scheme

Generation & Embedding of Watermark, attacks and retrieval/detection of embedded Watermark, these are the main steps of a Watermarking Algorithm. There can be two types of watermarks: visible & invisible. A Visible Watermark [3] allows the primary image to be viewed, but still marks it clearly as the property of the owning organization. An Invisible Watermark [3], on the other hand, is an image overlaid on another image which cannot be seen, but can be detected algorithmically.

1.1 Image Watermarking Techniques

Spatial Domain techniques: Spatial domain method [2] analyzes the original data in spatial domain and manipulates the least significant bit (LSB) to embed watermark. This technique is easy to embed watermark but not robust to lossy compression and filtering

Frequency based Techniques: Frequency domain method converts the original and watermark data into frequency domain and manipulates the coefficients to embed watermark into original data. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are frequently used techniques in frequency domain. DCT is very robust to data manipulation like compression and filtering. DWT is robust against noise and geometric attacks. Spread Spectrum method is an application of frequency domain methods which is much robust to filtering, Cropping, lossy compression, re sampling and other data manipulations.

*Corresponding author: deepti.hunjan@gmail.com

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, following observations have been made:

- Spatial Domain method is the simplest algorithm to implement but is easily defeated.
- Threshold based Comparison methods take a longer amount of time but seem to perform a little better.
- 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.
- DWT based methods are employed to minimize the data loss in transformations, to reduce .noise generation and to increase the robustness, but their computational complexity is more.
- DFT based techniques are rotation, scaling and translation invariant and thus robust against geometric distortions.

There are various attacks which a good watermarking algorithm should be resilient to. These can be intentional (there can be cases that a watermark is tried to be removed by specifically designed procedures), unintentional (modifications applied with a purpose other than to destroy a watermark) and geometric attacks.

Intentional Attacks

(1) *Removal attacks:* Various removal attacks include Inversion, Collusion [7], De noising attack and Compression attack using synthetic modeling. These are the attacks in which attackers try to remove a hidden watermark by manipulating a watermarked image such that the quality of the image is destroyed.

(2) *Ambiguity attacks*: Various ambiguity attacks include Copy attack, Jamming & saturation. Copy attack [7] is a protocol attack. This also estimates the watermark and can cost protocol ambiguity within a watermarking system. Jamming & Saturation attacks try not to alter the original watermark but embed further watermarks so that the original can not be extracted reliably.

Unintentional Attacks

(1) *Noise attacks:* These attacks attempt to paralyze the embedded watermark by manipulating the whole watermarked data without an attempt to remove the watermark [3]. These can attack the digital data while it is passing the communication channel.

(2) Attacks during processing of data: These include Filtering [10], A / D or D/A conversion. Watermarks must also be resilient to common analogue interference such as Additive White Gaussian Noise (AWGN).

Geometric Attacks

Geometric attacks such as Scaling (uniform or non-uniform) [10] and Rotation are also possible but most algorithms are highly robust to these methods. Rotation and Scaling of the image result in the Translation at log polar mapping of the Fourier magnitude spectrum of the image [4]. One effective geometric attack is cropping which is effective when the watermark is not present at all in whole image or this image is required during watermark detection. Pixel Permutations, Subsampling, Insertion/Removal of Pixels and Gamma Correction are various operations which can be performed on Images to modify them. There exists a tool named Stirmark [8] which is a generic tool to test the robustness of digital watermarking algorithm and has been freely available. It can also perform a default series of tests which serve as a benchmark for watermarking. It breaks many of the attacks by adding sub-perceptual distortion.

3. PROBLEM SOLUTION

As we have discussed that existing methods suffer from one or the other short comes like non robustness to geometric attacks, Image Modifications etc, hence it is worth to solve the problem such that we get a watermarking technique that will increase the security of watermark by increasing its robustness.

In the proposed method we will use concept of nested watermarks [6]. We will be embedding a watermark in watermark using an embedding technique based on cryptography in Spread spectrum domain [5]. The resultant encrypted watermark will be embedded into the Cover Image using DWT [9] .This method will provide additional level of security because now the watermark itself will be encrypted and algorithm is robust enough against any attacks. Our proposed solution will be implemented in 3 steps as is depicted by Fig. 2.

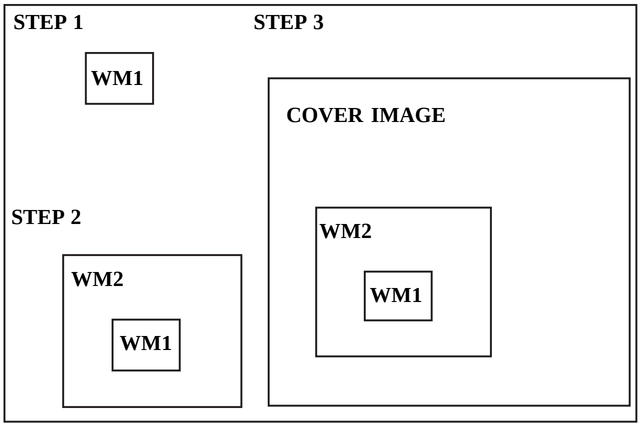

Figure 2: Proposed Solution

Table 1
Results of Measurement of Quality of Watermarked Image

Cover Image	*WM1*	*WM2*	*PSNR1*	*MSE1*	*PSNR2*	*MSE2*	*R1*	*R2*
Sample1 (400 × 400)	8 × 10	20 × 48	17.9214 dB	0.0186	39.1735 dB	8.6213	0	0
Sample2 (435 × 435)	10 × 10	20 × 50	16.9879 dB	0.0212	38.1246 dB	7.8983	0	0
ample3 (512 × 512)	12 × 12	27 × 56	17.1213 dB	0.0185	37.8571 dB	9.2123	0	0

PSNR1: PSNR after embedding WM1 in WM2.
MSE1: MSE after embedding WM1 in WM2.
R1: MSE of recovered watermark WM1 from Main watermark WM2.
R2: MSE of recovered watermarked watermark WM2 from coverimage.
PSNR2: PSNR after embedding WM2 in Cover Image.
MSE2: MSE after embedding WM2 in Cover Image.

Step 1: Watermark 1 (WM1) is the actual watermark which will help in proving authenticity of Copyright Information.

Step 2: WM1 is embedded into Watermark2 (WM2) using spread spectrum cryptographic technique which can render the watermark from being successfully recovered by unauthorized users.

Step 3: Now the encrypted watermark (WM1 embedded in WM2) is embedded into the cover image (which has to be protected) using DWT.

This method is a blind watermarking recovery method (means original image is not needed at the time of extraction). Because we will use cryptography in spread spectrum domain this method will not suffer from non robustness as is the case with spatial domain cryptography. Also DWT itself is very robust to geometric as well as noise attacks.

The quality of any watermarked image is measured in terms of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error), 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 embedded & extracted watermark. Samples of 3 images were taken for experimental purpose and results obtained are shown in table-1.

4. CONCLUSION

We have discussed various present day challenges to algorithms for Embedding/Extracting Digital Watermarks and also suggested a solution so that our algorithm meets these challenges to give us a robust digital watermarking technique. The proposed method is supposed to be very robust against all kinds of attacks as

- Embedding a watermark using DWT makes the watermarked image resistant to any geometric and noise attacks.
- Embedding a watermark using cryptography in spread spectrum domain provides additional level of security against any intentional attacks by the hacker.

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] Jung S Cho, Seung W. Shin, Won H. Lee, M Jong U. Choi, Enhancement of Robustness of Image Watermarks Image Watermark into Coloured Image, based on WT & DCT, ITCC Las Vegas, (2000).

[4] Lian Cai, Sidan Du, Robust Digital Watermarking Method against RST Attacks, *International Conference on Signal Processing & Communications*, (2004), 491–495.

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

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

[7] Chun-Shien Lu, Chao-Yung Hsu, Near-Optimal Watermark Estimation and Its Counter Measure: ANTI Disclosure Watermark for Multiple Watermark Embedding, *IEEE Transaction on Circuits and Systems for Video Technology*, **17**, (4), (2007), 454–467.

[8] Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn, Information Hiding - A Survey, *Proceedings of the IEEE Special Issue on Protection of Multimedia Content*, **87**(7), (1062) , (1999).

[9] 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.

[10] Neelu Sinha, Data Throughput and Robustness Studies in a New Digital Image Watermarking Technique Based upon Adaptive Segmentation and Space - Frequency Representation (WASSFR), *Fifth IEEE Southwest Symposium on Image Analysis and Interpretation (SSIAI'02) IEEE*, 2002.