Challenges and Approach for a Robust Image Watermarking Algorithm

Afrin Zahra Husaini¹ & M. Nizamuddin²

¹²ECE Dep’t, Al-Falah School of Engineering & Technology, Faridabad, India

Abstract: 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. Digital watermarking is one of the proposed solutions for copyright protection of multimedia data. This technique is better than Digital Signatures and other methods because it does not increase overhead. Digital watermarking is not a very old field. Researchers try to invent techniques that increase the security, capacity, and imperceptibility of watermarked images. In this paper I plan to present a new image watermarking technique that can embed more number of watermark bits in the cover image without affecting the imperceptibility and increase the security of watermarks. To increase the embedding capacity the concept of watermark in watermark is used. Means it embeds an extra watermark into the main watermark and then embeds the main watermark into the cover image. To increase security we embed encrypted watermarks in the image. This provides an additional level of security for watermarks. For instance if watermarking key is hacked still the attacker will not be able to identify the watermark because it is encrypted. In conclusion there is a new method proposed which uses a concept of nested watermarks using Discrete Wavelet Transform and Cryptography using Spread Spectrum technique and is supposed to be robust enough to cater to challenges presented here.

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

1. INTRODUCTION

Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. The signal may be audio, pictures or video, for example. If the signal is copied, then the information is also carried in the copy. It may carry several different watermarks at the same time. In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this is also a visible watermark.

In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden). The watermark may be intended for widespread use and is thus made easy to retrieve or it may be a form of Steganography, where a party communicates a secret message embedded in the digital signal.

Applications

Digital Watermarking can be used for a wide range of applications such as copy write protection, Source Tracking (Different recipients get differently watermarked content), Broadcast Monitoring (Television news often contains watermarked video from international agencies), Covert Communication Annotation of digital photographs with descriptive information is another application of invisible watermarking. The use of the word of watermarking is derived from the much older notion of placing a visible watermark on paper as shown in fig.1.

Figure.1: Visible Watermark
Watermarking Life-cycle Phases

Classification

A digital watermark is called robust with respect to transformations if the embedded information can reliably be detected from the marked signal even if degraded by any number of transformations. Typical image degradations are JPEG compression, rotation, cropping, additive noise and quantization.

Robustness: A watermark is called fragile if it fails to be detected after the slightest modification. Fragile watermarks are commonly used for tamper detection (integrity proof). Modifications to an original work that are clearly noticeable are commonly not referred to as watermarks, but as generalized barcodes.

A watermark is called semi-fragile if it resists benign transformations but fails detection after malignant transformations. A watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copy protection applications to carry copy and access control information.

Perceptibility: A watermark is called imperceptible if the original cover signal and the marked signal are (close to) perceptually indistinguishable. A watermark is called perceptible if its presence in the marked signal is noticeable, but non-intrusive.

Capacity: The length of the embedded message determines two different main classes of watermarking schemes:

- The message is conceptually zero-bit long and the system is designed in order to detect the presence or the absence of the watermark in the marked object. This kind of watermarking schemes is usually referred to as Italic zero-bit or Italic presence watermarking schemes. Sometimes, this type of watermarking scheme is called 1-bit watermark, because a 1 denotes the presence (and a 0 the absence) of a watermark.

- The message is a n-bit-long stream \( m = m_1 \ldots m_n \), \( n \in \mathbb{N} \), with \( n = |m| \) or \( M = \{0, 1\}^n \) and is modulated in the watermark. These kinds of schemes are usually referred to as multiple bit watermarking or non zero-bit watermarking schemes.

Embedding Method: A watermarking method is referred to as spread-spectrum if the marked signal is obtained by an additive modification. Spread-spectrum watermarks are known to be modestly robust, but also to have a low information capacity due to host interference. A watermarking method is referred to as amplitude modulation if the marked signal is embedded by additive modification which is similar to spread spectrum method but is particularly embedded in the spatial domain.

2. ATTACKS ON ALL WATERMARKS

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).

Spatial Domain Attacks

The Special domain attacks are shown in Fig.3 (a-f)

![Figure 3(a-f): Special Domain Attacks](image)
Challenges and Approach for a Robust Image Watermarking Algorithm

3. WHY TO SOLVE THIS PROBLEM

Watermarking is not a fully mature technology. A lot of research is going on this field, especially to increase security and capacity of watermark data. Most of researchers try to increase the watermark capacity by compromising image quality, because there is a trade off among data rate, security and imperceptibility. But with our scheme we will be able to embed more number of watermark bits without affecting the imperceptibility of the cover image. Also our watermarking technique will use cryptography. So, it will provide an additional level of security. For instance if watermarking key is hacked still the attacker will not be able to identify the watermark because it is encrypted. So, it is worth to solve this problem, because by solving it we will get a watermarking technique that will increase the robustness of watermarks.

4. IMPLEMENTATION & EXPERIMENTAL RESULTS

We are giving a new image watermarking method. This method increases the security and capacity, hence the robustness of a watermark. To increase capacity the concept of nesting is used. We embed one watermark in another, and then the final watermark is embedded into the cover image. This makes more number of watermark bits to be inserted into the original cover image, thereby increasing the capacity. To increase security of watermark cryptography is used. By doing this, we have provided additional levels of security of the system.

It is a blind watermarking method. Means original image as well as original watermark are not required at the time of watermark recovery process. For embedding first watermark we use spread spectrum domain technique, because it is less time consuming as compared to wavelet or frequency domain techniques. Moreover this method will not suffer from non robustness as is the case with spatial domain cryptography, for embedding second watermark we used technique based on DWT, which is very robust against attacks.

5. ALGORITHM USED

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.6.

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

Step 2: WM 1 is embedded into Watermark 2 (Wm2) using spread spectrum cryptographic technique which can render the watermark from being successfully recovered by unauthorized users.

Figure 4: Frequency Domain Attacks Showing Cropping

Figure 5: Wavelet Domain Attacks Showing SPIHT and IW4

Figure 6: Steps of Implementation of the Algorithm
Steps 3: Now the encrypted watermark (WM1 embedded in WM2) is embedded into the cover image (which has to be protected) using DWT.

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. For encryption we XOR the binary image with some key. For decryption the encrypted image is XORed with same key. It gives the original image.

**Watermark Embedding Algorithm**

- WM1 – binary image to be embedded in WM2
- WM2 – binary image acting as main watermark.
- Cover Image – gray scale image to be watermarked.
- EN1 – key used for encrypting WM1.
- EN2 key used for encrypting watermarked watermark (let it WW).
- W1- key used to embed encrypted binary watermark into the main watermark.
- W2- key used to embed encrypted watermarked watermark in Cover Image.

**Algorithm**

1. We take WM1 and encrypt it by performing XOR operation with the key EN1. Let the output of this steps be WE1, as shown in Fig.7.
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 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 (FW1).

**Figure.7: Watermark Insertion**

This algorithm produces one output which is final watermarked image (FW1).

**Watermarks Extraction Algorithm**

The watermark extraction algorithm is shown in Fig.8

- FW1 – It is the received watermarked image.
- SZ1- size of WM1
- SZ2- size of WM2
- EN2 – key used to decrypt Recovered watermark from cover Image.
- EN1- key used to extract encrypted watermarked watermark from main watermark.
- W2 – key used to extract encrypted watermarked watermark from Cover Image.
- W1 – key used to extract encrypted binary watermark from the main watermark.

**Algorithm**

1. Extract the encrypted watermark2 (i.e.) WE2) from received watermarked image using key W2. Let the recovered image is WE2’
2. Decrypt WE2’ by performing its XOR operation with key EN2. Let the output be 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. 8: Watermark Extraction**

This algorithm produces two outputs namely:

- RW2- main watermark recovered from the received watermarked image.
- RW1- watermark recovered from the main watermark.

6. CONCLUSIONS

This paper presents a blind watermarking technique that uses watermark nesting and encryption. Nesting means it embeds an extra watermark into the main watermark and then embeds the main watermark into the cover image. For encryption we used XOR operation. For embedding Watermark in a Watermark we used Spread Spectrum based technique. For embedding watermarked watermark in cover Image we used DWT based technique.

7. FUTURE SCOPE

Need for copyright protection in digital media has led to enormous growth in the field of digital Watermarking whereby researchers are striving to come up with new ways of content protection. Most of the research is going on in this field, especially in the field of image watermarking. The watermarking technique that is given in this paper can be further improved to increase the hiding capacity of images without affecting the imperceptibility of the images. The
other future scope is that our technique can be enhanced to embed colored nested watermark in colored image. Because in this technique we used encryption that is based on XOR operation, so, further work can be done to find some other encryption technique to increase the security of watermarks.

REFERENCES


