Digital Image Watermarking

Ajinkya Kawale, Shubham Gaidhani

Abstract—Eyssentially a watermark is a pattern, image or text that is impressed onto paper, which provides evidence of its authenticity. There are two types of watermarks: visible watermark and invisible watermark. This paper centres upon implementation of watermark in an image. The main consideration for any watermarking scheme is its robustness to various attacks. Watermarking dependency on the original image increases its robustness but at the same time it needs to be ensured that the watermark is imperceptible. In this paper, an invisible watermarking technique (least significant bit) and a visible watermarking technique is implemented. An attack is also implemented on the visible watermarked image by adding a random noise to the watermarked image. The watermarked image is then compressed and decompressed using JPEG compression. Finally noise is removed and the images are separated from the recovered watermarked image.

Index Terms— Digital Watermarking, Invisible Watermark, Image Compression, Image Decompression, JPEG picture format, Noise addition, Steganography, Visible Watermark

---- 🌢

1 INTRODUCTION

Information hiding can be mainly divided into three pro-Lesses - cryptography, stenography and watermarks. Cryptography is the process of converting information to an unintelligible form so that only the authorized person with the key can decipher it. As many advances were made in the field of communication it became rather simple to decrypt a cipher text. Hence more sophisticated methods were designed to offer better security than what cryptography could offer. This led to the discovery of stenography and watermarking. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Thus even the existence of secret information is not known to the attacker. Watermarking is closely related to stenography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication.

The history of watermark dates back to the 13th century. Watermarks were used to indicate the paper brand and the mill that produced it in Italy. By the 18th century watermarks began to be used as anti-counterfeiting measures on money and other documents and in 1995 interest in digital watermarking began to mushroom. Intense research has been carried out in this field for the past few years which has led to the discovery of various algorithms. Throughout this report some of these techniques are discussed and one such technique is implemented.

As many advances are made in the field of communication it became rather simple to decrypt a cipher text. Hence more sophisticated methods are designed to offer better security than what cryptography can offer. This led to the discovery of stenography and watermarking. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Watermarking is closely related to steganography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication. Figure explains how watermarking is derived from steganography.

2 STATEMENT OF THE PROBLEM

The main aim of this technique is implementation of watermark in an image. To prove the robustness of this proficiency, an invisible watermarking technique (least significant bit) and a visible watermarking technique is implemented. An attack is also implemented on the visible watermarked image by adding a random noise to the watermarked image. The watermarked image is then compressed and decompressed using JPEG compression. Finally noise is removed and the images are separated from the recovered watermarked image.

All tables and figures will be processed as images. You need to embed the images in the paper itself. Please don't send the images as separate files.

3 DEFINITION OF TERMS

3.1 Techniques or Schemes of Watermarking

Watermarks can be embedded within images by modifying these values, i.e. the transform domain coefficients. In case of spatial domain, simple watermarks could be embedded in the images by modifying the pixel values or the Least Significant Bit (LSB) values.

3.2 Spatial Domain Techniques

Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression.

3.3 Least Significant Bit Coding (LSB)

LSB coding is one of the earliest methods. It can be applied to any form of watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. In order to retrieve it back this sequence should be known. The watermark encoder first se-

Ajinkya Kawale is currently pursuing bachelors degree program in electronic engineering in Nagpur University, India, PH-+919763195577. E-mail: ajinkya.d.kawale@gmail.com

[•] Shubham Gaidhani is currently pursuing bachelors degree program in electronic engineering in Nagpur University, India.

lects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component.

3.4 Predictive Coding Schemes

Predictive coding scheme was proposed by Matsui and Tanaka in [8] for gray scale images. In this method the correlation between adjacent pixels are exploited. A set of pixels where the watermark has to be embedded is chosen and alternate pixels are replaced by the difference between the adjacent pixels. This can be further improved by adding a constant to all the differences. A cipher key is created which enables the retrieval of the embedded watermark at the receiver. This is much more robust when compared to LSB coding.

4 METHODOLOGY

In this paper, the LSB technique is used for visible and invisible watermarking.

4.1 Invisible Watermarking (Least significant bit Watermarking)

1. A raw bitmap image 'A' will be selected from the set of standard test images. Let this be the base image on which the watermark will be added.

2. A raw bitmap image 'B' will be selected from the set of standard test images. This will be the watermark image which will be added to the base image.

3. The most significant bit henceforth will be mentioned as MSB, of watermark image 'B' will be read and these will be written on the least significant bit, henceforth will be mentioned as LSB, of base image 'A'.

4. Thus, 'A' will be watermarked with 'B' resulting in a combined image 'C'.

5. 'C' therefore will now contain an image 'A' which has its LSBs replaced with the MSBs of 'B'.

6. The technique used will be LSB technique which is a form of spatial domain technique.

7. This technique is used to add an invisible and visible watermark in the image.

4.2 Visible Watermarking – Concatenation

1. A raw bitmap image 'A' will be selected from the set of standard test images. Let this be the base image on which the watermark will be added.

2. A raw bitmap image 'B' will be selected from the set of standard test images. This will be the watermark image which will be added to the base image.

3. Now both images 'A' and 'B' will be concatenated to get a watermarked image 'D'

4. 'D' therefore will now contain the base image 'A' and the watermark image 'B'.

5. This technique is used to add visible watermark in the image.

4.3 Visible Watermarking – Noise Addition

Now, noise is added to concatenate watermarked image 'D'. 2. The noise is a random matrix of order [512x512].

3. The resulting image after the addition of noise is displayed and stored as 'Noisy Image

4.4 Visible Watermarking – JPEG Compression

1. Once the noise is added, the program halts and waits for the JPEG compression to be done

2. Once the compression is done, the program is informed by pressing enter key that the compression is done and it can proceed by removing the noise.

3. JPEG Compression is done by running the .exe file available.

4. The watermarked image added with noise 'E' which is in bitmap format is compressed into JPEG format 'F'.

5. The size of the original image is 257KB.

6. The JPEG compressed image is 92.2KB.

4.5 Visible Watermarking – Denoising

1. The JPEG compressed image, is now denoised.

2. The program which was on hold is triggered by pressing the 'Enter Key'.

3. The program runs by reading the JPEG compressed noised and watermarked image.

4. The noise is now removed from the JPEG compressed image. The resulting image will be 'G'.

4.6 Visible Watermarking – Separating the Watermark

1. Finally the base image 'A' and the watermark image 'B' are separated from the concatenated recovered watermarked image 'G'

2. The images are in JPEG format, when compared to the original images, which were in Bitmap formats. Therefore their sizes are less.

5 RESULTS

The attacks applied to the watermarked image to test the robustness of watermark are JPEG compression, cropping, low pass filtering, medium pass filtering, rotation and modification. The extracted watermarks after applying various attacks are shown in fig. The watermarked image is compressed using lossy JPEG compression. The percentage by which the watermarked image is compressed to test robustness where less percentage represents most compression and more degraded watermarked image.

6 CONCLUSION

Using MATLAB software, waterermarking techniques are used for both visible and invisible images. Noise is added to the images as a form of attack. The images are compressed and decompressed as another form of attack. The noise is later removed and the base and watermark images are separated from the watermarked image. Finally, we are compared the original images and recovered images. The performance evaluations of original and recovered image are done based on PSNR, SSIM and SSIM map which is left.

REFERENCES

[1] G. K. Wallace, "The JPEG still picture compression standard", IEEE

IJSER © 2013 http://www.ijser.org Trans. on Consumer Electronics, Vol. 38, pp.18-34, Feb. 1992.

- [2] P. Vidyasagar, S. Han and E. Chang. "A survey of digital image watermarking techniques", 3rd IEEE International Conference on Industrial Informatics (INDIN 2005), edited by T. Dillon, X.Yu. and E. Chang, pp. 495-502, Perth, Western Australia, 2005.
- [3] Digital Image Processing- third edition by Rafael C. Gonzalez and Richard E.Woods
- [4] Bender W., Gruhl D., Morimoto N., "Techniques for data hiding", Proc. SPIE, Storage and Retrieval for Image and Video Databases III, vol. 2420, San Jose, CA, pp. 165-173, Feb. 1995.
- [5] I.J. Cox, et al, "Digital watermarking and steganography" (Second Edition), Morgan Kaufmann, 2008.

IJSER