Investigation of the Effects on Embedded Watermarks under Image Manipulations

Nilesh Moti
Dept. of Electrical and Electronic Engineering Science
University of Johannesburg
Johannesburg, South Africa
nmoti@csir.co.za

Theo G. Swart
Dept. of Electrical and Electronic Engineering Science
University of Johannesburg
Johannesburg, South Africa
tgswart@uj.ac.za

***Abstract*—In this paper, different types of image watermarking techniques, the embedding of data or copyright information into the data file, are investigated. Three image watermarking techniques are discussed, namely: least significant bit, least significant bit and discrete cosine transform combined, and discrete cosine transform and discrete wavelet transform combined. These embedded watermarking techniques are evaluated on how robust each technique is under image manipulations. Simulations are done using the three image watermarking techniques to determine the effects on how well the embedded watermarking technique resists manipulations. Different watermarking techniques resulted in high robustness in some cases but showed visible artefacts, in other cases robustness was low but image quality stayed relatively close to the original watermark.**

***Index Terms*—Digital images, robustness, watermarking**

I. Introduction

Due to advancements in technologies, the current trend in the world is that most individuals prefer to use the Internet as the primary medium to transfer data from one end to another across the world. The data transmission is made very simple, fast and accurate using the Internet. However, unauthorized sharing of information over the Internet is an issue. Therefore, it becomes essential to take data sharing into consideration and try to preserve the original creator's identity. This area of data sharing has gained more attention due to the massive increase in data sharing over the Internet and people claiming data as their own [1]. One way of ensuring identity ownership is to embed a watermark into the data, where this data can be any multimedia file, such as images, audio and video.

This paper investigates the effects of embedded watermarks in image files under manipulation. A watermark can be used to identify ownership of the images, watermarks may also be used to verify the authenticity or integrity of the owner's data or to show the identity of its owner/creator, it can be used for tracing copyright infringements as well. If a watermark distorts the owners data negatively after it has been embedded, the watermarking technique that is used is poor and can be of no use. The watermark should be statistically invisible and to prevent detection and/or removal, be robust against manipulations [2]. Watermarks are usually found on pictures, audio and video files, these watermarks are called digital watermarks and are normally incorporated in the carrier signal. The focus of this paper will be to compare a number of different watermarking techniques in images and determine the watermarking techniques robustness against manipulation.

In Section II the three watermarking techniques being considered are discussed. Section III presents the results and analysis of the extracted watermarks after different image manipulations were applied. The paper is concluded in Section IV.

The authors of this paper gratefully acknowledge the financial support received from the CSIR.

II. Watermarking Techniques

Three different types of watermarking techniques will be discussed: least significant bit (LSB) method, LSB and discrete cosine transform (DCT) combined, and DCT and discrete wavelet transform (DWT) combined. For each watermarking technique, the embedding process and extraction process will be discussed and are used in simulations. Once the watermark is embedded into the image file, manipulations are applied to the watermarked image, the watermark will be extracted using the extraction process and the recovered watermark will be compared to the original watermark and determine how much the watermark image has changed, to determine the robustness of the watermarking technique.

A. Least Significant Bit

The LSB method is the most common watermarking technique that can be easily implemented. It uses the lowest significant bit in the byte value to embed the information in the image pixel.

The concept of LSB embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being just by looking at it. The conventional LSB technique requires eight bytes of pixels to store 1 byte of information, but in some cases the LSB technique requires just four bytes of pixels and it is sufficient to hold one message. The rest of the bits in the pixels remains the same as the original [3].

From Fig. 1 the watermark byte, which is highlighted in grey, is distributed to the pixels' last bits in order to embed the watermark, the rest of the pixel bits stay the same. By doing this a watermark can be embedded into an image without

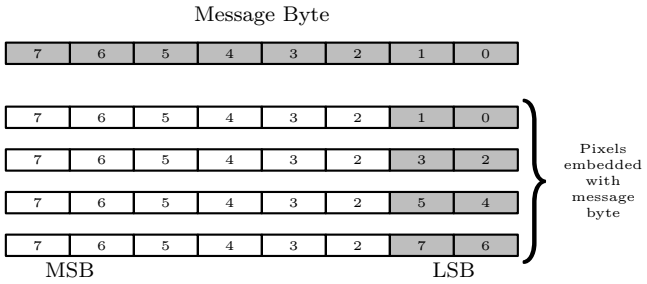


Fig. 1. Example of least significant bit method

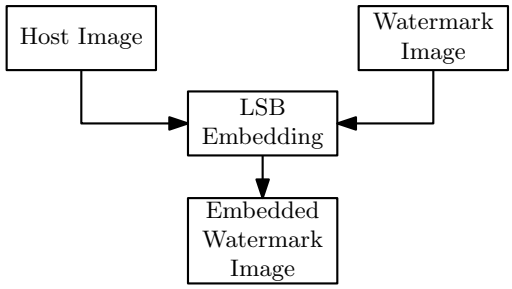


Fig. 2. LSB embedding process

it being distinguishable by human vision. With regards to the hiding capacity, the size of the information to be hidden relatively depends on the size of the cover image and therefore the size of the cover image must always be smaller than the image [4].

The LSB embedding process that was followed is shown in Fig. 2: where the watermark image is embedded into the host image using the LSB method. The final output image is the embedded watermark image.

Once the watermark is embedded, the extraction process is the reverse of Fig. 2. In the embedding process, the watermark image was embedded in the 7-th and 8-th bits, the 7-th and 8-th bits are the least significant bits, for the extraction process only the 7-th and 8-th bits get extracted, the rest of the bits are ignored and this will produce the original watermark image.

B. LSB and DCT Combined

The second watermarking technique to be evaluated is to combine the LSB method and the DCT. When an image is processed by DCT, we obtain the direct current (DC) coefficients and the alternating current (AC) coefficients. The DC coefficient is the first coefficient after the image transforming which indicates the average brightness of an image. The AC coefficients are the remaining coefficients which include the high frequency coefficients, the intermediate frequency coefficients and the low frequency coefficients [5]. Fig. 3 shows the frequency distribution of DC and AC coefficients.

The embedding process is shown in Fig. 4, the first step is to perform the DCT on the host image. Now, the LSB method is used to embed the watermark bits into the coefficients of the DCT-transformed host image by replacing the least significant bits. Lastly inverse discrete cosine transform (IDCT) is

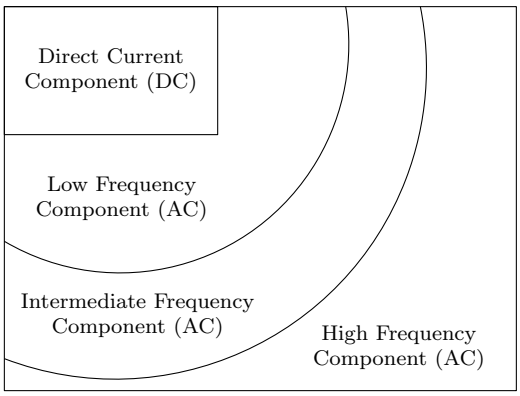


Fig. 3. Frequency distribution of DCT coefficients

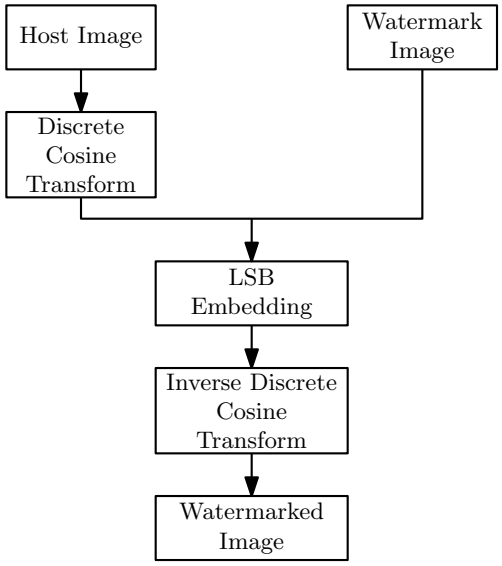


Fig. 4. Embedding structure

performed on the embedded watermarked image to produce the original image with the watermark embedded.

For image extraction the reverse of the embedding procedure must be applied. In the extraction process, the DCT is performed on the watermarked image. Once that is done, LSB extraction is performed on the least significant bits of the transformed watermarked image, this then removes the watermark image from the host image [5].

C. DCT and DWT combined

The third image watermarking technique that is evaluated is the technique that is based on DCT and discrete wavelet transform (DWT). In the DWT the image is differentiated multiple times and decomposed into a sub-image of different spatial domains and independent frequency regions. Once the original image is DWT transformed, the image is decomposed into four frequency regions, one low frequency region (LL) and three high frequency regions (LH, HL, HH). L represents a low-pass filter and H represents a high pass filter. If the

information of the low frequency region is DWT transformed, the sub-level frequency region information will be obtained.

A 2D image is shown in Fig. 5 after it has been decomposed three times using DWT. The original image can be decomposed into frequency regions HL_1, LH_1 and HH_1. The low frequency region information can be further decomposed into sub-level frequency regions of HL_2, LH_2 and HH_2. The low frequency region's image closely resembles the original image, as most of the signal information lies in the low frequency region. The frequency regions of LH, HL and HH respectively represents the level of detail, the upright detail and the diagonal detail of the original image [6].

Fig. 6 shows the watermark embedding process and how the watermark image gets embedded into the host image. The watermark image is first transformed using DCT, as the DCT transform contains the low frequency information of the watermarking image, then the renewed watermark image can be recovered quite well as long as a lot of information is not lost during manipulation. The host image is decomposed through the DWT and a wavelet modulus is chosen in the high frequency level in which the watermarking image is embedded into.

Now to embed the watermark, the wavelet coefficient values C_k is amended to the chosen streak blocks, the embedding formula is

$$C'_k = C_k + av_k, \quad k = 1, 2, \ldots, PQ, \tag{1}$$

where C_k is the former wavelet coefficient value of the streak

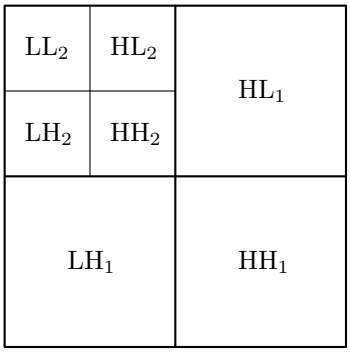


Fig. 5. Discrete wavelet transform regions

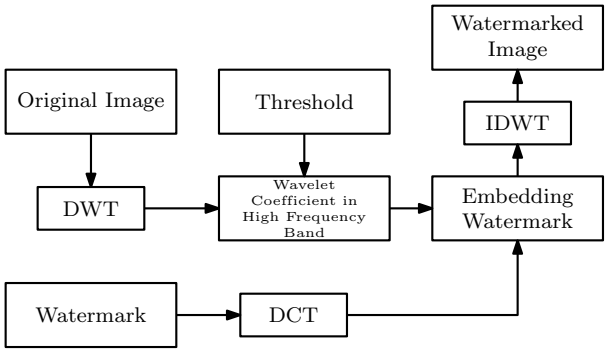


Fig. 6. Embedding block diagram

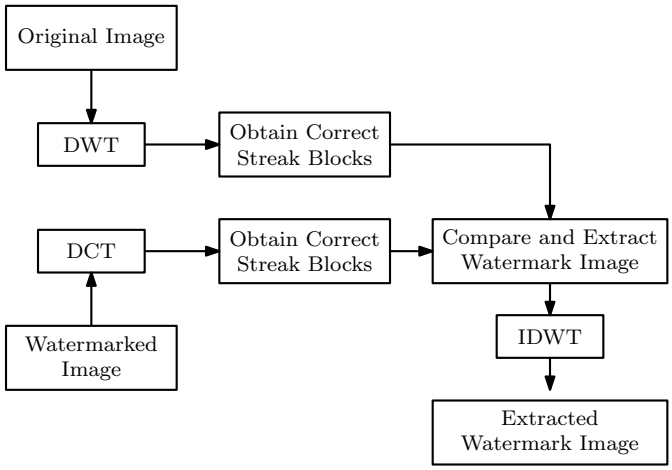


Fig. 7. Extraction block diagram

sub-block, V_k represents the k-th component weight of one dimensional digital watermarking sequence V, C'_k represents the new wavelet coefficient value of the streak sub-block U_k and a represents the embedding depth for digital watermarking. Once the watermark signal is embedded, the information of the lowest frequency band and the high frequency band is bonded. The wavelet transform of the image is inversed and the watermarked image is obtained.

The extraction process is shown in Fig. 7, where the DWT is applied to the original image and the watermarked image. Once the DWT is done, the information of the low frequency band and high frequency band are obtained. The streak block is obtained from the high frequency band of the original image after being DWT transformed. For extracting the watermark signal, entropies $H(U_k)$ and $H(U'_k)$, which correspond to the streak block U_k and U'_k, and the result of $H(U_k) - H(U'_k)$ is obtained. The DCT of the disordered watermarking image is inversed and the image is obtained [7].

III. Results and Analysis

The three mentioned image watermarking techniques were simulated in Matlab and various manipulations were applied to the watermarked image, thereafter the embedded watermark was extracted and analyzed to determine how robust the watermarking technique was against the manipulation. The manipulations that were applied are blurring, cropping, adding of noise, rotating and sharpening of the image.

The BER and PSNR was used to compare the extracted watermark image and the embedded watermark image with no manipulation, to give a quantitative value as to how much the manipulation affected the original watermark image [8].

The bit error rate (BER) is

$$BER = \frac{\text{Number of errors}}{\text{Total number of bits sent}}. \tag{2}$$

If the two images are identical the BER would be zero, if the reference image and an image with errors are compared, the BER that is closer to zero represents an image with very

(a) (b)

Fig. 8. Simulation images used: (a) host image, and (b) watermark image

little errors. Matlab has the BER function built in which can be utilized. The peak signal to noise ratio (PSNR) is a metric used to compare image quality. The PSNR is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed or reconstructed image [9], [10]. Matlab has an inbuilt function to calculate the PSNR of images, where:

$$PSNR = 10\log_{10}\frac{A^2}{\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}[f(i,j)-f'(i,j)]^2}. \quad (3)$$

The host image used in the simulations is a 512×512 grey scale image of a woman shown in Fig. 8(a), while the watermark image used is a 512×512 black and white image of a baboon that is shown in Fig. 8(b). For purposes of documentation, the images are scaled down in order to be presented correctly.

In the following subsections, the results of the simulations that were done on the three above mentioned image watermarking techniques are shown.

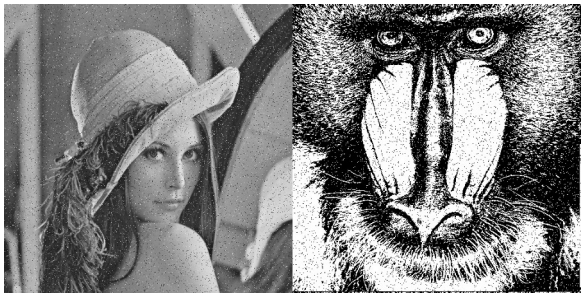
A. Least Significant Bit Results

By using the LSB technique, the mentioned manipulations were performed on the watermarked image and the results are shown in Fig. 9. Each figure compromises of the manipulated watermarked image which is shown on the left and the extracted watermark shown on the right. From Fig. 9(d) rotation around the center was applied and even though the angle of rotation was small only the middle area of the watermark was partially recovered. Fig. 9(a) blurring of the image, the pixel takes the value of the surrounding pixel values which causes a smoothing or blurring of the image, an increase in the amount of blurring results in the altering of the embedded image also which effects the embedded watermark image negatively as seen in the recovered watermark.

Analysis is done on the results obtained. The BER and PSNR results were calculated for each manipulation and is presented in Table I. We can see that this watermarking technique did well when the watermarked image was cropped and noise was added. The PSNR was used to measure the imperceptibility of the watermark image embedded into the original image and for this watermarking technique the measured PSNR value is 51.1407, which is acceptable and the embedded watermark could not be seen.

(a) blurring

(b) cropping



(c) adding of noise

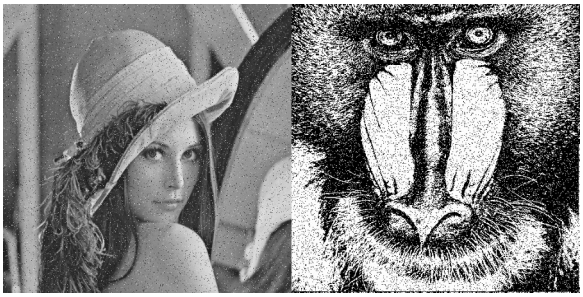
(d) rotating by 0.1°

(e) sharpening

Fig. 9. Extracted watermark image for LSB after the respective manipulations were applied

(a) blurring

(b) cropping



(c) adding of noise

(d) rotating by $0.1°$

(e) sharpening

Fig. 10. Extracted watermark image for LSB/DCT after the respective manipulations were applied

(a) blurring

(b) cropping

(c) adding of noise

(d) rotating by $0.1°$

(e) sharpening

Fig. 11. Extracted watermark image for DCT/DWT after the respective manipulations were applied

TABLE I
ANALYSIS OF RESULTS FOR DIFFERENT WATERMARKING TECHNIQUES

	LSB		LSB/DCT		DCT/DWT	
Manipulation	PSNR	BER	PSNR	BER	PSNR	BER
Blurring	3.859	0.411	6.759	0.211	∞	0
Cropping	6.062	0.248	6.145	0.243	3.210	0.478
Adding of noise	6.415	0.228	6.039	0.249	15.832	0.026
Rotating	3.205	0.478	2.916	0.511	3.242	0.474
Sharpening	4.613	0.346	5.108	0.309	4.965	0.319

B. LSB and DCT Combined Results

The simulation results of the LSB and DCT combined image watermarking technique are shown in Fig. 10. Again, each figure compromises of the manipulated watermarked image shown on the left and the extracted watermark shown on the right. From Fig. 10(d), by rotating the image slightly resulted in a completely noisy or indistinguishable image, with the addition of noise in Fig. 10(c) the watermark technique did well to recover the watermark but with an increase in noise which results in a degraded watermarked image.

The BER and PSNR results were calculated for each manipulation and are also presented in Table I, showing that this watermarking technique did well against blurring, cropping and adding of noise. The PSNR was also used to measure the imperceptibility of the watermark image embedded into the original image, and the PSNR value is 18.2544, which is the lowest of the three watermarking techniques, however the watermark could not be seen.

C. DCT and DWT Combined Results

The simulation results of the image watermarking based on DCT and DWT are shown in Fig. 11. As before, each figure compromises of the manipulated watermarked image shown on the left and the extracted watermark shown on the right. From Fig. 11(e), with the addition of the sharpening filter this resulted in the watermark image becoming lighter and with further increases in the sharpening filter resulted in a complete white image. In Fig. 11(c), with the addition of noise the watermark image was recovered, but larger increases in noise level resulted in a white image.

As before, the BER and PSNR results were calculated and are presented in Table I, showing that this watermarking technique produces the exact watermark image when the blur filter was applied, however it did not do very well against cropping and rotation of the image. Cropping of the image resulted in a blank image. The PSNR was used to measure the imperceptibility of the watermark image embedded into the original image, the measured PSNR value is 44.5302, which is acceptable and the watermark could not be seen.

IV. CONCLUSION

Three image watermarking techniques were discussed and simulated in Matlab in this paper. Analysis of the simulation results shows that all three watermarking techniques suffered badly when the watermarked image was rotated, the LSB method was able to recover a small amount of data, however that is not sufficient. The image watermarking technique based on DCT and DWT did not fair very well when cropping or rotation manipulation was applied but did very well against adding of noise and blurring of the image. The LSB and LSB/DCT combined watermarking techniques showed consistent results when evaluating its BER and PSNR values.

The types of manipulations that were applied are very common manipulations that most image processing software can do. So from the simulation results obtained, future developments can be made to develop a more robust image watermarking technique.

REFERENCES

[1] P. K. Sharma and Rajni, "Information security through image watermarking using least significant bit algorithm," in *Proc. Int. Conf. Comput. Sci. Eng. Applic.*, Delhi, India, May 26–27, 2012, pp. 61–67.

[2] L. Boney, A. H. Tewfik and K. N. Hamdy, "Digital watermarks for audio signals," in *Proc. IEEE Int. Conf. Multimedia Comput. Syst.*, Hiroshima, Japan, Jun. 17–23, 1996, pp. 473–480.

[3] B. S. Champakamala, K. Padmini and D. K. Radhika, "Least significant bit algorithm for image steganography," *Int. J. Advanced Comput. Technol.*, vol. 3, no. 4, pp. 34–38, Aug. 2014.

[4] G. M. Kamau, "An enhanced least significant bit steganographic method for information hiding," Masters dissertation, Jomo Kenyatta University of Agriculture and Technology, Kenya, 2013.

[5] Z. Fu-an, "A robust watermarking scheme based on least significant bit and discrete cosine transform," *Int. J. Security Applic.*, vol. 9, no. 4, pp. 175–184, 2015.

[6] P. M. Pithiya and H. L. Desai, "DWT based digital image watermarking, de-watermarking & authentication," *Int. J. Eng. Research Develop.*, vol. 7, no. 5, pp. 104–109, Jun. 2013.

[7] M. Jiansheng, L. Sukang, and T. Xiaomei, "A digital watermarking algorithm based on DCT and DWT," *Proc. Int. Symp. Web Information Syst. Applic.*, Nanchang, China, May 22–24, 2009, pp. 104–107.

[8] V. Licks, F. Ourique, R. Jordan and F. Perez-Gonzalez, "The effect of the random jitter attack on the bit error rate performance of spatial domain image watermarking," in *Proc. Int. Conf. Image Process.*, Barcelona, Spain, Sep. 14–17, 2003, pp. 455–458.

[9] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 6, no. 3, pp. 243–250, Jun. 1996.

[10] M. Antonini, M. Barlaud, P. Mathieu and I. Daubechies, "Image coding using wavelet transform," *IEEE Trans. Image Process.*, vol. 1, no. 2, pp. 205–220, Apr. 1992.