Title: Copyright protection of Digital Images using Biometric Watermarking

Ms. Nidhi Upreti

nidhiupreti23@gmail.com

Abstract:

The advancement in Computer Science technology and available tools has put the images at the risk of being copied without your permission. One deterrent to scare people away from stealing your images is to place a watermark on your image. It can also provide information that would benefit the people you want to share your image with. A watermark is an obvious text or logo that has been superimposed on an image. The information hiding process could be done either in spatial domain or in frequency domain. In this paper, simple arithmetic operations have been performed for inserting a speech signal as watermark on image. The quality of the watermarked image and extracted watermark is measured using peak signal to noise ratio (PSNR) and normalized correlation (NC) respectively. Robustness of proposed algorithm is tested against addition of salt and pepper noise and Gaussian filters attacks and cropping .The proposed algorithm is robust against the aforesaid attacks.

1. INTRODUCTION

With advancing technology, we need a better system to ameliorate the security of data being transmitted. The images being transmitted are at high risk of being forged, thus it is necessary to add a copyright mark to the image to protect its true ownership. [8] This is the reason that digital watermarking has become a hotspot of research in recent years. Watermarking is the process of hiding digital information in a carrier signal.

Digital watermarks are used to verify the authenticity or integrity of the carrier signal or to show the identity of its owner. [7] The main characteristics of Digital watermark are *Robustness, Imperceptibilityand Security.* Robustness implies that the watermark should be able to withstandnormal signal processing operations such as cropping, transformation, compression,etc.

*Imperceptibility means t*he watermarked image should look like same as theoriginal image to the normal eye. The viewer should not be able to detect theembedded watermark.

Security implies that an unauthorized person cannot detect,retrieve or modify the embedded watermark.

While going through the various watermarking techniques used in “Robust watermarking of fingerprint images.”[2] and “Fusion of LSB and DWT biometric watermarking for offline handwritten signature”[10] gives us the algorithm of using biometric fingerprint and signature as the watermark. The algorithm presented in these papers is complex and difficult to be used for pragmatic purposes. Also, it is not very convenient to embed a fingerprint or a signature watermark to protect the copyright of image.

We propose a new idea for watermarking of digital images, which uses human voice as the original watermark which is embedded on the image. Other watermarks that are generally used are fingerprint, handwritten signature, etc. [3] But voice watermark has an intrinsic advantage over others watermarks. The phonetic parameters help us distinguish different human voices; hence it serves as an efficient watermark. [1], [4]

Section 2 gives the proposed algorithm of the embedding of the watermark onto the three different images taken. It further explains the extraction of watermark which is the voice signal to obtain the original copyright image. Section 3 analyses the performance of the proposed algorithm by calculating the value of PSNR to see the difference between the original and the extracted watermark on addition of various attacks like Salt and Pepper Noise, Gaussian Low pass filter and Cropping attack. [9]

2. Proposed Algorithm

In this section, the proposed watermarking algorithm is elaborated in detail. During the embedding process the biometric watermark of the owner of an image is inserted in to an image in spatial domain. Similarly during reconstruction process the inserted watermark is extracted and used for ownership verification.

Watermark Embedding Process

In watermark embedding process, the biometric data is considered as watermark and inserted in an image to protect ownership of it. During this process the strength of watermark is adjusted in order to make the underlying cover data not to be distorted much. In this proposal biometric data such as voice signal is considered as watermark.

This is obtained from the output of the microphone. The voice of the copyright holder is taken from the microphone and is converted into a digital signal hence obtaining a single dimensional array Y which is called watermark.

The obtained voice signal in digital form is converted into binary bits. Thus, these bits are then used in the insertion algorithm to generate watermark. Since the watermark is being added to an image, hence it should be scaled down through scaling parameter; otherwise it could distort the image quality. The watermark embedding process is carried out in spatial domain by modifying the intensity values of images to be protected. In this proposal instead of taking 2D biometric data, 1D voice signal is taken as watermark. The block diagram for inserting a watermark into an image is shown in Figure 1.

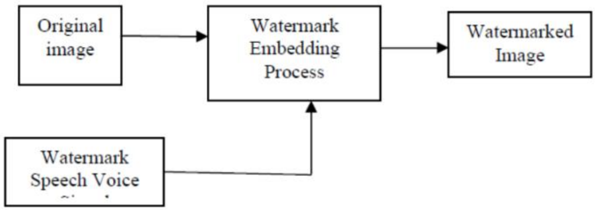


Fig 1. Watermark Embedding Process

The algorithm for embedding a biometric watermark is given below.

Watermark Insertion (I, W)

Input: Image I, Watermark W

Output: Watermarked Image I’

Read Input Image I

Obtain voice signal from microphone in 1- D form, W

Digitize the obtained voice signal using sampling and quantization technique

Insert the biometric watermark obtaining an Image I’

Watermark Extraction Process

Similarly whenever any dispute arises about the ownership of copyrighted images, the inserted biometric watermark would be extracted to prove the ownership. Thus in order to authenticate the image, the watermark needs to be extracted without hampering the image quality. As the watermark is inserted in spatial domain it would be very easy to remove the watermark form the cover image provided the original image content was available with the owner. Thus retaining original image provides next level of security; hence this kind of watermarking algorithm could be classified as non- blind watermarking algorithm. The block diagram for watermark extraction process is shown in the Figure 2.

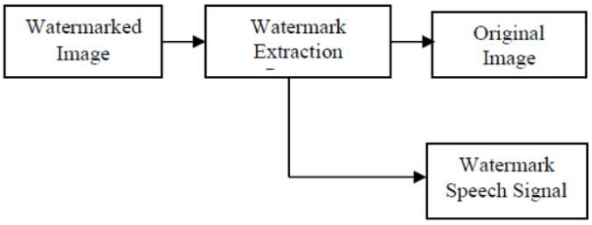


Fig 2. Watermark Extraction Process

Watermark Extraction (I’,I)

Input: Watermarked Image I, Original Image I

Output: Reconstructed Image and Watermark

1. Read original and watermarked Images Iand I’

2. Extract the Inserted biometric watermark from an image I’ using original image I

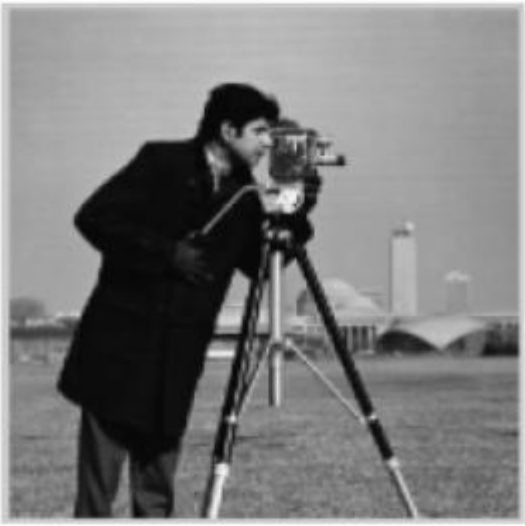
3. Calculate the similarity of the extracted watermark with the original watermark

4. Compare the quality of the reconstructed image with the original cover image.

Performance Analysis

The performance of the proposed watermarking algorithm is carried out in this section. To test the performance of the proposed algorithm the following test images are shown in Figure 3. Similarly the watermark speech signal is shown in Figure 4.

The watermarked images are shown in Figure 5.



(a) Cameraman

Fig 3. Test Image

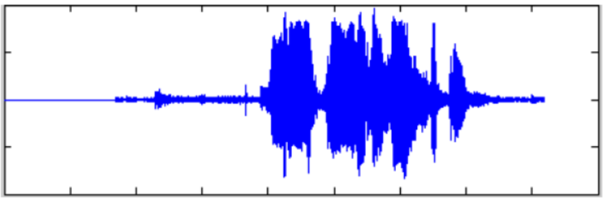


Fig 4. Original Watermark

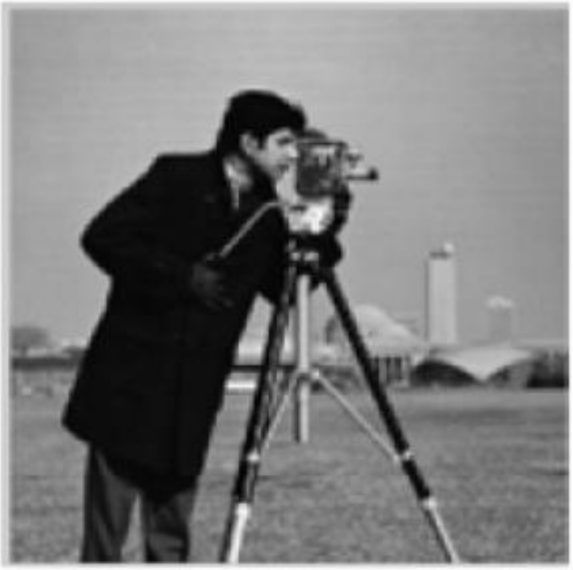


Fig 5. Watermarked Image

The performance of the proposed algorithm is analyzed through subjective and objective measurements. The subjective measures show that the inserted watermark has not distorted the quality of the cover images. The Peak Signal to Noise Ratio

(PSNR) and Normalized Correlation Coefficient (NCC) are the objective criteria used to measure the quality of the watermarked image and extracted watermark. The equations for measuring PSNR are shown in (3) and (4) respectively. [5]

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(f(i,j) - f'(i,j)\right)^2 \qquad (1)$$

$$PSNR = 10\ \log_{10}\left(\frac{255^2}{MSE}\right) \qquad (2)$$

Where f(i,j) and f’(i,j)represent the pixel values of original image and the watermarked image respectively and parameters m,n specifies the row and column size of images respectively. The quality of the watermarked image is measured through the normalized correlations coefficient (NCC) using (3), which is used to measure the similarity between original watermark and extracted watermark.

$$NC = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} W(i,j) * w_e(i,j)}{\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{m} w(i,j)^2}\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{m} w_e(i,j)^2}} \qquad (3)$$

Where Wand $W_0$are the original and extracted watermark.

The robustness of the watermarking algorithm is tested against various attacks such as addition of salt and pepper noise, Gaussian filters and cropping. The watermarked images after attacks are shown in Figure 6, Figure 7 and Figure 8.

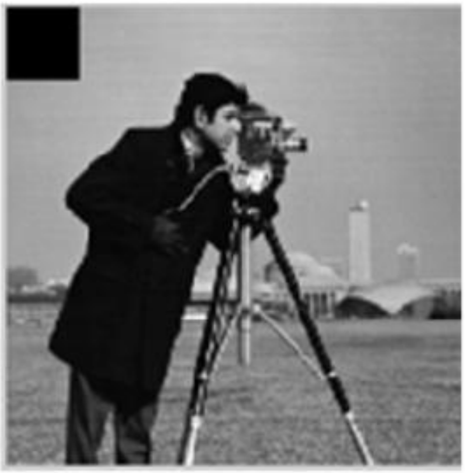


Fig 6. Watermarked Image after cropping

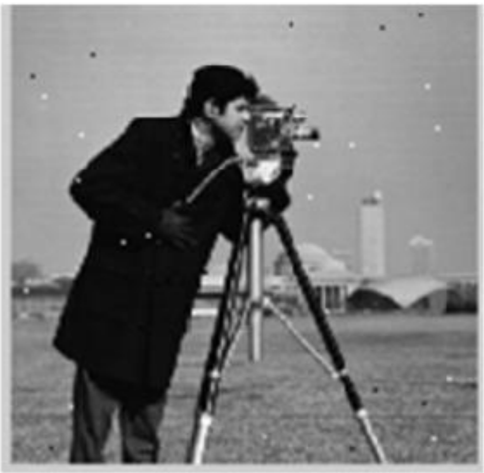


Fig 7. Watermarked image after salt and peeper attack

Fig 8. Watermarked image after Gaussian low paas filter attack

The calculated values of various attacks on images have been shown in the tables. Table 1 show the salt and pepper attack. Table 2 demonstrates Gaussian Low pass filter and Table 3 shows the cropping effect.

Table 1. Calculated NCC and PSNR values after Salt and Pepper noise attack

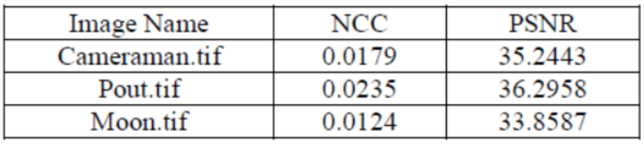


Image Name	NCC	PSNR
Cameraman.tif	0.0179	35.2443
Pout.tif	0.0235	36.2958
Moon.tif	0.0124	33.8587

Table 2. Calculated NCC and PSNR values after Gaussian Filter attack

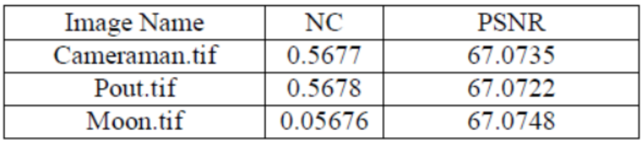


Image Name	NC	PSNR
Cameraman.tif	0.5677	67.0735
Pout.tif	0.5678	67.0722
Moon.tif	0.05676	67.0748

Table 3. Calculated NCC and PSNR values after cropping

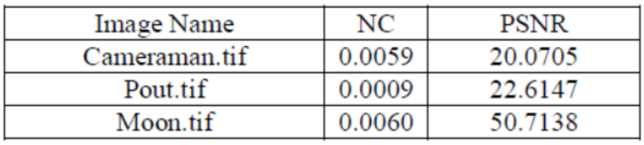
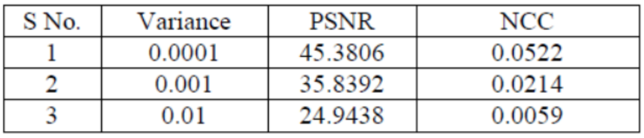


Image Name	NC	PSNR
Cameraman.tif	0.0059	20.0705
Pout.tif	0.0009	22.6147
Moon.tif	0.0060	50.7138

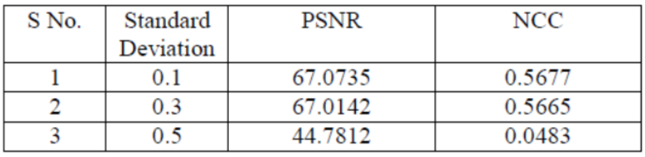
In order to check the intensity of attack, we change the value of variance and standard deviation for salt and pepper noise and Gaussian low pass filter on ‘cameraman.tif’ respectively. The calculated values are shown in Table 4 and Table 5.

Table 4. Salt and Pepper noise for different values of variance



S No.	Variance	PSNR	NCC
1	0.0001	45.3806	0.0522
2	0.001	35.8392	0.0214
3	0.01	24.9438	0.0059

Table 5. Gaussian Low Pass filter for different values of Standard deviation



S No.	Standard Deviation	PSNR	NCC
1	0.1	67.0735	0.5677
2	0.3	67.0142	0.5665
3	0.5	44.7812	0.0483

6. CONCLUSION

In this paper a digital watermarking technique using speech signal for copyright protection of digital images is proposed. The speech signal of the content owner is digitized and embedded in the cover image. The proposed algorithm is tested with three test images and results are analysed. As per the obtained results the inserted watermark has not distorted the quality of the cover image. The scaling factor used to insert watermark is selected empirically on trail and error basis. The inserted speech signal is extracted after implementing attacks and recognized by hearing it. Thus the inserted watermark is recognizable after attacks and it could be used to prove ownership of coverimages.

REFERENCES

[1] Gunsel, B., Sener, S., &Yaslan, Y. (2003).An adaptive encoder for audio watermarking. *WSEAS Transactions on Computer*, *4*(2), 1044-1048.

[2] Gunsel, B., Uludag, U., & Murat Tekalp, A. (2002). Robust watermarking of fingerprint images. *Pattern Recognition*, *35*(12), 2739-2747.

[3] Hartung, F., &Kutter, M. (1999). Multimedia watermarkingtechniques.*Proceedings of the IEEE*, *87*(7), 1079-1107.

[4] Andrews, H., & Patterson, C. (1976). Singular value decompositions and digital image processing. *Acoustics, Speech and Signal Processing, IEEE Transactionson*, *24*(1), 26-53.

[5] Santhi, V., & Thangavelu, D. A. (2009). DWT-SVD combined full band robust watermarking technique for color images in YUV color space. *InternationalJournal of Computer Theory and Engineering*, *1*(4), 424-429.

[6] Quan, L., &Qingsong, A. I. (2004). A combination of DCT-based and SVDbased watermarking scheme.In *Signal Processing,2004.Proceedings.ICSP'04.2004 7th International Conference on* (Vol. 1, pp.873-876).IEEE.

[7] Jain, A. K., Uludag, U., & Hsu, R. L. (2002). Hiding a face in a fingerprintimage.In *Pattern Recognition, 2002.Proceedings.16th International Conference on* (Vol. 3, pp. 756-759).IEEE.

[8] Cox, I. J., Kilian, J., Leighton, F. T., &Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *Image Processing, IEEE Transactionson*, *6*(12), 1673-1687.

[9] Jain, A. K., Ross, A., &Prabhakar, S. (2004). An introduction to biometric recognition. *Circuits and Systems for Video Technology, IEEE Transactionson*, *14*(1), 4-20.

[10] Low, C. Y., Teoh, A. B. J., & Tee, C. (2008, May). Fusion of LSB and DWT biometric watermarking for offline handwritten signature, In *Image and SignalProcessing, 2008. CISP'08.Congress on* (Vol. 5, pp. 702-708).IEEE.