Digital Watermarking for Data Security

AVI KHANDELWAL

Roll no: 204102301

Abstract

The project implements Digital Watermarking based technique for digital content copyright protection. In this project with Discrete Cosine Transform method, the watermark is located within low frequency DCT coefficients of the original image because of their resistance to most attacks and with the combination of the DCT and Principal Component Analysis technique, the watermark appears invisible while the quality of the cover image is unaltered which is later confirmed with wide range of attacks.

1 Introduction

With Internet rapidly developing, illegal copy of digital content poses a serious problem since it can be conveniently reproduced and modified by anyone with minimal technical skills. Most vulnerable to such attacks are the digital images published on websites. Digital Watermarking can be used as a means for discovering unauthorized content usage and also for copyright protection. It is basically a technique of embedding some unique identification mark also called as watermark into the digital image by its owner. After embedding, watermarked data is generated. A good Watermarking technique must have certain qualities such as robustness and imperceptibility. In the proposed method a watermark is hidden using a secret key in digital image which only the owners of that content can extract using the unique watermarking extraction algorithm.

1.1 Background

The characteristics of the watermarking system are determined mainly by 2 important factors which are robustness and invisibility. These Watermarking techniques further can be categorized into spatial domain and frequency domain. Although experience has shown that spatial domain techniques need less hardware and have shorter execution time, but they are not much resistant against malicious attacks, while there are many techniques in frequency domains like DCT and DWT which prove to be more robust.

1.2 Terminologies

PART A: DISCRETE COSINE TRANSFORM

The two dimensional Discrete cosine transform (DCT) of an MxN function f(i,j) is defined as

$$F(u,v) = \frac{2C(u)C(v)}{\sqrt{MN}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{cos(2i+1)u\pi}{2M} \frac{cos(2j+1)v\pi}{2N} f(i,j)$$

and inverse DCT is defined as

$$f(i,j) = \frac{2C(u)C(v)}{\sqrt{MN}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{cos(2i+1)u\pi}{2M} \frac{cos(2j+1)v\pi}{2N} F(i,j)$$

where u = 0,1,...M-1 and v = 0,1,....N-1 and

$$C(x) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{if } x = 0 \\ 1, & \text{otherwise} \end{cases}$$

PART B: PRINCIPAL COMPONENT ANALYSIS

Principal component analysis (PCA) is a technique for removing co-relation among the dimensions of the feature vector. Assuming matrix X of size N × M, PCA transform is defined as-

$$\mathbf{Y = AX}$$

where

$$\vec{X} = [\vec{X}_1, \vec{X}_2, ..., \vec{X}_k, ...\vec{X}_N]^T$$

$$\vec{X}_k = [\vec{x_1}, \vec{x_2}, ...\vec{x_M}]^T (k = l, ..N; \vec{X}_k \in R^m$$

The matrix **A** contains the eigenvectors, $\vec{a_i}$, which can be described as

$$\vec{A} = [\vec{a_1}, \vec{a_2}, ..., \vec{a_M}]$$

1.3 Organization

This project consists of five parts. First part consists of image pre-processing. The second and third part revolves around the DCT and PCA application in watermarking. In fourth part, the proposed scheme is applied. Finally in part five, evaluation and performance metrics against various image processing attacks are discussed.

2 Dataset used

Following 2 images have been used as a part of the data set for the project.

2.1 Evaluation Metrics

1. Peak Signal to Noise Ratio (PSNR)

$$mse = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - I'(i,j)]^2$$

PSNR is the means for evaluation of image quality after watermarking or in other words invisibility of a watermark in the image can be described by PSNR. It is targeted to 40 dB.

$$PSNR = 10 \log_{10}(\frac{\max_{\forall(i,j)}(I(i,j))^2}{mse})$$

2. Normalized Correlation (NC)

$$NC = \frac{\sum_{i=1}^{M} W_i \times W_i'}{\sqrt{\sum_{i=1}^{M} W_i^2 \times \sum_{i=1}^{M} W_i'^2}}$$

Normalized Correlation (NC) is the method used for comparison between original watermark and the extracted watermark quality. It reflects to a robustness of watermarking scheme. Ideally NC should be close to 1.0

3 Literature

[1], [2], [2], [3], [4], [5].

3.1 Previous methods

Some of the previous methods had the watermark placed in areas of the image that are important for human visual system (HVS) so by the DCT method, middle frequency band is used generally because of it's relative advantage compared to other bands as the high-frequency band is quite fragile against most attacks and the lowfrequency band is bad in terms of invisibility of the watermark and the quality of the watermarked image.

3.2 Research gaps or loopholes in the previous methods

While middle frequency band has it's advantages but on contrary low frequency band is more resistant against some attacks (low-pass filtering and JPEG compression) but since hiding watermark in low-frequency DCT coefficients doesn't really make watermark completely invisible, hence this technique is generally avoided.

3.3 Proposed Method

In this project, in order to use the lowfrequency band a new method is proposed based on a combination of the DCT and PCA technique. PCA is dimension reduction technique but more importantly it makes dimensions linearly independent such that when watermark is hidden in these independent dimensions it becomes completely invisible whereas earlier since these dimensions were highly correlated, so hiding watermark in these correlated dimensions would not really make watermark invisible. So with this proposed scheme, the watermark is rendered invisible while the quality of the cover image is maintained.

4 Methodology

In this project, the original image due to the fact that nearby pixels have a high correlation together, is divided into non-overlapping blocks with the size of 8×8 and then DCT will be applied to each block separately, after that, the low-frequency band coefficients of every block are placed in a vector. By doing this process for all other blocks, the data matrix X will be formed, then the PCA transform will be applied to the data matrix X. The first component of the PCA has the maximum energy concentration, in other words, it consists of maximum amount of information of cover image than any other the DCT coefficients which are located in the low frequency band of a block. So the watermark is placed within it. The mechanism of the proposed scheme is divided into two parts, watermark embedding and watermark detection.

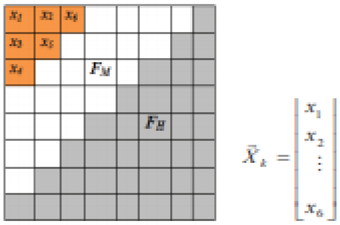

x_1
x_2
x_6
x_3
x_5
x_4
F_M
F_H
$\vec{X}_k = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_6 \end{bmatrix}$

Fig. 3. The DCT region is used to embed watermark.

4.1 Algorithm

A. Watermark Embedding Algorithm:

The algorithm which for embedding a watermark on an image is given below:

1. Original image is divided into non-overlapping blocks of 8×8.

2. DCT will be applied on each block.

3. The low-frequency band coefficients will be placed in $\vec{X_k}$, then data matrix **X** will be formed as $\vec{X} = [\vec{X_1}, \vec{X_2}, ..., \vec{X_k}, ...\vec{X_N}]^T$

4. PCA will be applied on the matrix **X**, so matrix **Y** will be formed as $\vec{Y} = [\vec{Y_1}, \vec{Y_2}, ..., \vec{Y_k}, ...\vec{Y_N}]^T$

5. Converting the binary watermark logo into vector W as W = $\{w_1, w_2, ..., w_N\}$

B. Watermark Detection Algorithm

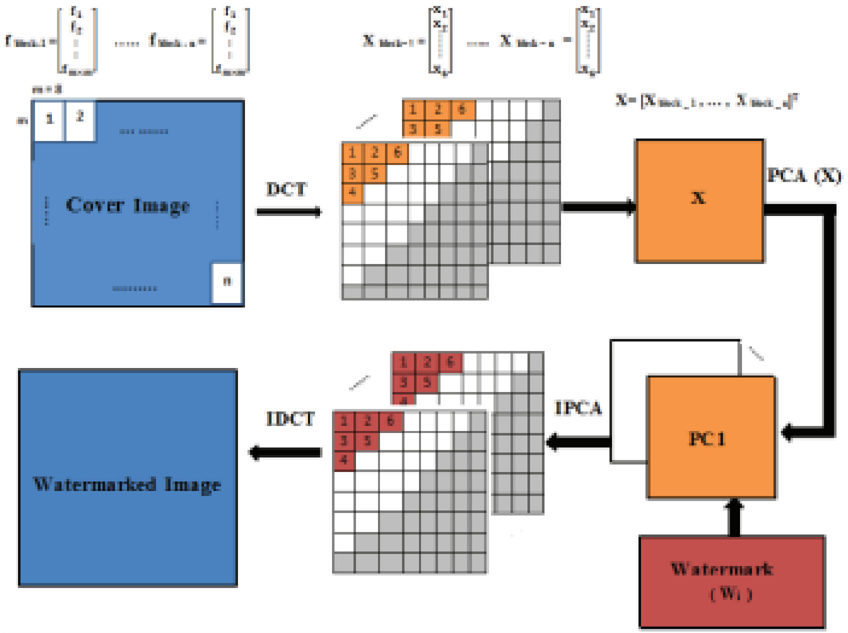
The algorithm used for detection of the watermark is given below:

1. From the original image and the watermarked image, data matrix, X and X' will be formed separately.
X= matrix data of cover image
X'= matrix data of watermarked image

2. The PCA will be applied to matrix X and matrix X' so matrix Y and matrix Y' are obtained.

3. The watermark bits are extracted from the first component of the PCA with the formula $W_i = \frac{Y_i' - Y_i}{\alpha}$

4.2 Block Diagram



Above block diagram shows the working of our watermarking scheme.

1. Apply DCT on non-overlapping blocks of size 8x8.

2. Take the 6 low-frequency DCT coefficients of every block as a vector in data matrix X.

3. Apply PCA.

4. Watermark in first dimension of transformed matrix.

5. Take inverse PCA.

6. Apply IDCT and construct the watermarked image.

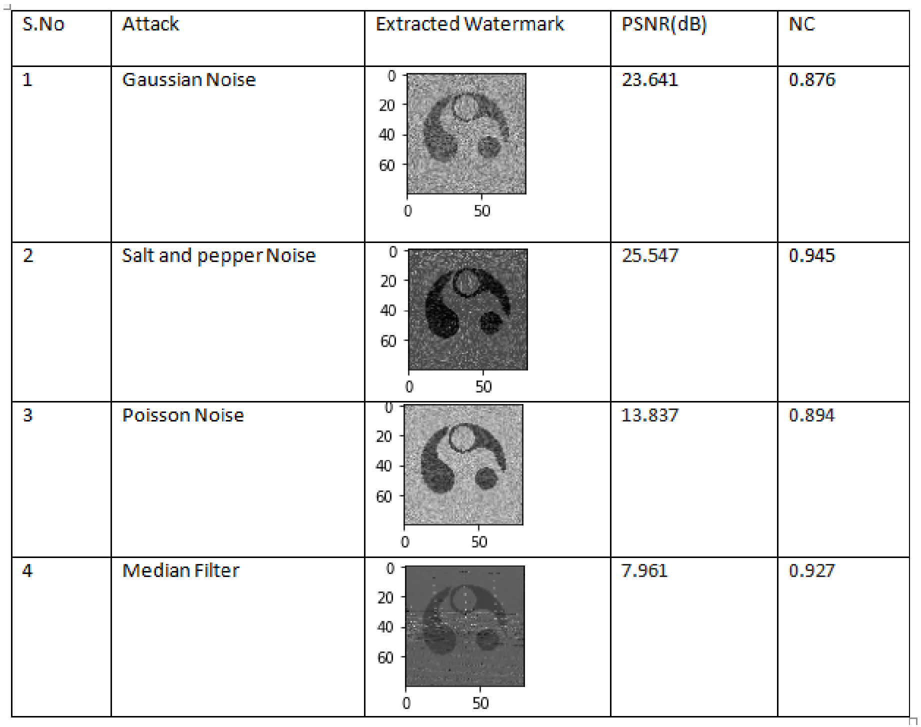
7. Image processing attack happens.

8. Repeat the above mentioned steps to extract the watermark.

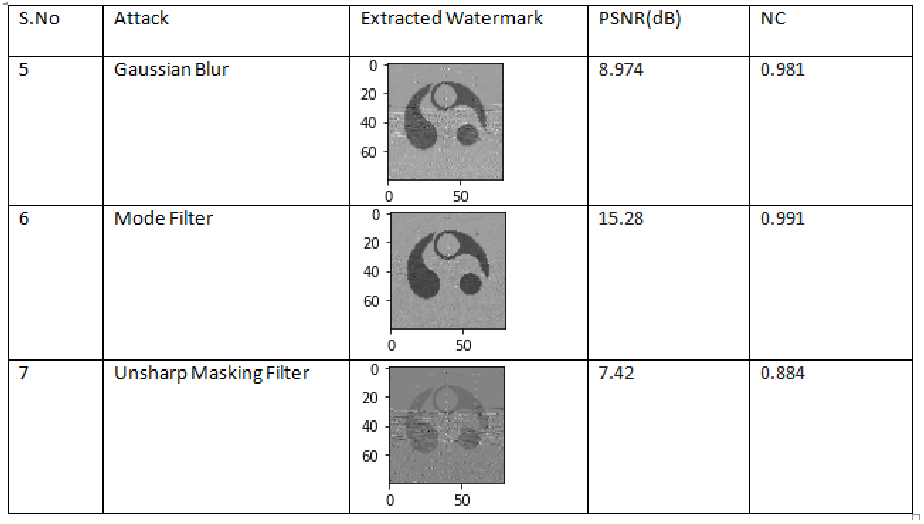
9. Observe how close it is to original watermark, more close would mean that our scheme has been successful against protecting the image and less close would otherwise mean that it was not able to protect the image against that attack.

4.3 Plots tables and outputs

Below table describes the evaluation metrics of the proposed scheme.



S.No	Attack	Extracted Watermark	PSNR(dB)	NC
1	Gaussian Noise		23.641	0.876
2	Salt and pepper Noise		25.547	0.945
3	Poisson Noise		13.837	0.894
4	Median Filter		7.961	0.927



S.No	Attack	Extracted Watermark	PSNR(dB)	NC
5	Gaussian Blur		8.974	0.981
6	Mode Filter		15.28	0.991
7	Unsharp Masking Filter		7.42	0.884

5 Conclusions

After the proposed watermarking scheme is implemented and subjected to various image processing attacks, it can be confirmed that the scheme works well enough for extracted watermark to be identified well enough for content owner to know if their images are being copied by someone. There is still further scope of improvement like making this algorithm resistant against complex attacks like JPEG compression but as of now this algorithm is quite resistant to some commonly encountered attacks, making the digital content on internet a little more secure for usage.

References

[1] S. H. Arash Saboori, "A new method for digital watermarking based on combination of DCT and PCA," *2014 22nd Telecommunications Forum Telfor (TELFOR)*, 25-27 Nov. 2014.

[2] J. Abraham, "Digital image watermarking: An overview," *Modern Trends in Electronic Communication Signal Processing*, February 2011.

[3] M. A. Suhail, "Digital watermarking-based dct and jpeg model," *IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 52*, OCTOBER 2003.

[4] p. G. Ken Cabeen, "Image compression and discrete cosine transform," *International Journal of Computer Science Engineering Survey*, 10.5121/ijcses.2014.5204.

[5] W.-S. W. Chih-Chin Lai, "Digital image watermarking using dct and z-score transform," *Proceedings of the Ninth International Conference on Machine Learning and Cybernetics, Qingdao*, 11-14 July 2010.