International Journal of Electronics Communication and Computer Engineering
Volume 5, Issue (4) July, Technovision-2014, ISSN 2249–071X

Technovision-2014: 1st International Conference at SITS, Narhe, Pune on April 5-6, 2014

Digital Watermarking Technique for Image Authentication and Recovery

Rasika Jadhav
Department of E & TC
Rajarshi Shahu College of Engineering, Maharashtra, India
Email: rasika.rscoe@gmail.com

Akanksha Pawar
Department of E & TC
Rajarshi Shahu College of Engineering, Maharashtra, India
Email: akanp012@gmail.com

Prof. B. D. Jadhav
Department of E & TC
Rajarshi Shahu College of Engineering, Maharashtra, India
Email: bhagavat2@rediffmail.com

Abstract **– Digital media has become a large source of information exchange. Digital images constituting the most basic form of data shared. However along with simplicity, digitization poses to be a never-ending threat to the ownership of data. In this paper we propose a reliable Watermarking technique that protects the copyrights of the owner. This is achieved by decomposing the cover image as well as the watermark logo up to three levels of DWT. Analysis of the different attacks performed on the watermarked image is studied. The watermark logo is recovered and performance parameters, comparing the original and recovered images, such as mean square error (MSE), peak signal to noise ratio (PSNR) and normalized correlation (NC) are measured. A Graphic User Interface (GUI) is implemented in MATLAB to make the application user friendly.**

Keywords **– Watermarking, DWT, MSE, PSNR, NC, GUI.**

I. INTRODUCTION

The Internet with its availability of digital information has brought revolution in human life. Exchange of data between two distant places has not only become possible but also instant. Digital data is today's most popular and cheapest form of mass communication. However this has brought insecurity along with it. The data available on the Internet can easily be copied, shared and also edited. This causes an obstruction to the owner, as his copyrights are no longer protected. This is a major problem for the data on the web.

Different techniques were invented over the years to protect the digital material. Some of these techniques include cryptography and steganography. In cryptography a secret code or a hidden message is encrypted in the digital data. Encryption is done using a special type of key. However if this key is known, anybody can easily lay hands on the secret information. Steganography on the other hands deals with hiding the image, to be protected, in some another image. Steganography too uses a key for the encryption. But in steganography, if the cover image is tampered with or made any changes, the hidden image is likely to vanish and thus get lost. Another interesting technique existing for data authentication is Digital Watermarking.

Watermarking has proved to be an excellent tool in the field of authentication since ages. In ancient times, important documents were protected by watermarking them. Back then, watermarking meant creating patterns in paper by varying their thicknesses. Digital Watermarking follows the same idea. An image, most commonly known as watermark logo, is hidden in the image to be protected. This means that the watermark logo protects the cover image, making it a noble technique.

As the purpose of steganography is to have a covert communication between two parties i.e. existence of the communication is unknown to a possible attacker, and a successful attack shall detect its existence.

Watermarking, as opposed to steganography, makes a system to be robust against possible attacks and identify the ownership copyrights.

Digital Watermarking secures the original information from unauthorized manipulations and authenticates multimedia content and provides copyright protection [1].

A Digital Watermarking technique hides a signal which is imperceptible to the Human Visual Systems (HVS), and is statistically undetectable, resistant to lossy compression and common signal processing operations.

Digital Watermarking can be Fragile or Robust type. In fragile watermarking, if the Watermarked image is tampered with, the watermark logo vanishes. Such a watermarking technique finds its application in Tamper detection. In robust watermarking, no matter how many times the watermark is tampered, the watermark logo does not vanish. Such a watermarking technique finds its application in Content authentication. In this paper, we propose a Robust Watermarking Scheme.

Digital Watermarking can be accomplished by using different transforms like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [2].

DCT is not preferred because DCT coefficients are likely to be changed in case of any attacks which simultaneously change the further pixel values [3].

II. PROPOSED METHODOLOGY

Proposed watermarking technique exploits the characteristics of the Human Visual System (HVS). It is possible to hide watermarks with more energy in an image. This makes the watermarked image more robust. Bearing this in mind, the Discrete Wavelet Transform

(DWT) is chosen for watermarking. The DWT is an interesting transform, because it can be used as a computationally efficient version of the frequency models for the HVS. For instance, the human eye is less sensitive to noise in high resolution DWT bands. DWT decomposition can be exploited to make a real-time watermark application.

Thus the Discrete Wavelet Transform method is opted for this project to implement the Robust and Invisible Watermarking.

A. Watermark Embedding

The embedding process is implemented in the steps given below.

i. Select the original or the cover image, I
ii. Select the watermark logo, J
iii. Convert both the images into their respective grey scales.
iv. Apply DWT to both the images and decompose them into four sub bands, LL1, LH1, HL1 and HH1 for the cover image and L_L1, L_H1, H_L1, H_H1 for the watermark logo. The size of each sub band is exactly half.
v. Select the LL1 and the L_L1 band from the cover image and watermark logo and decompose it into further four bands, LL2, LH2, HL2, HH2 and L_L2, L_H2, H_L2, H_H2 respectively. This is the second level DWT.
vi. Now select the LL2 and the L_L2 bands and perform third level DWT forming the bands , LL3, LH3, HL3, HH3 and L_L3, L_H3, H_L3, H_H3

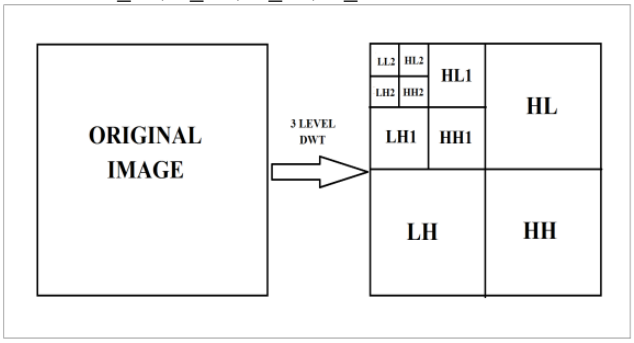


Fig.1. 3-Level DWT decomposition

vii. Now perform the embedding procedure W1= LL3+(L_L3*α)
viii. Apply inverse DWT to W1, LH3, HL3 and HH3 and obtain the image W2.
ix. Now apply second level inverse DWT to W2, LH, HL and HH2 and obtain image W3.
x. Perform third level DWT to W3, LH1, HL1 and HH1 to obtain final watermarked image W.
xi. Save the Watermarked Image.

B. Watermark Extracting

i. Select the watermarked image, W.
ii. Perform DWT and decompose the watermarked image W and the cover image I into four sub bands, W_LL1, W_LH1, W_HL1 and W_HH1 and LL1, LH1, HL1 and HH1.
iii. Further perform second level DWT on the sub bands W_LL1 and LL1, and third level on the sub bands W_LL2 and LL2 to obtain images W_LL3 and LL3.
iv. Perform watermark extraction, W1' = α*(W_LL3-LL3)
v. Perform inverse DWT to W1', W_LH1, W_HL1 and W_HH1 and obtain W1'.
vi. Then perform second level inverse DWT to W2', W_LH2, W_HL2 and W_HH2 and third level inverse DWT to W3', W_LH3, W_HL3 and W_HH3 and obtain W'.
vii. Save the extracted watermark W'.

III. Analysis of Attacks

To attain prominent watermark embedding and error free recovery, the watermarking process should to be robust to most of the attacks and modifications. The aim of attacks is not only to get rid of or destroy the embedded watermark but to prevent it from getting discovered. There always exists a risk that such attacks may harm the system performance [5].

A watermarked object may be altered either intentionally or accidentally. However in both the situations the watermarking technique should be able to detect and extract the watermark successfully after the attacks. Well known watermarking attacks, which may be intentional or unintentional, depending on the application, are:

A. Effect of different noises

Sometimes a random signal consisting of some noises like Gaussian, Poisson, or Salt and Pepper noise may get added to the image accidentally. In certain applications such additive noises may originate from converters or simply as transmission errors. However, error can also be introduced deliberately. These noises are defined below.

i. Salt and Pepper Noise:

The malfunctioning pixels added through the camera or the dust and light during the image acquisition produce the Salt and Pepper noise. The bit errors generated during the transmission of data or due to the D/A and A/D convertors also give rise to the salt and pepper noise. This is the most basic form of noise and can be eliminated by using simple median filters.

ii. Gaussian Noise :

The Gaussian noise is basically caused due to the fluctuations occurring randomly in the signal. The thermal noise can also be a reason for the Gaussian noise. Other sources are amplifier noises and reset noises produced by capacitors.

iii. Poisson Noise:

Poisson Noise is most commonly known as Shot Noise or Photon Noise. The Poisson noise is a kind of electronic noise and is caused due to the non-uniform characteristics of electric charge. Another source for this noise is the uneven fluctuations in the number of photons in optical devices.

B. Effect of Compression

Compression can be said to be more of accidental changes than deliberate attacks. These attacks are mostly encountered during sharing of images. The Internet allows compression of images during distribution. To avoid degradation, Robust watermarking techniques should be applied. The JPEG2000 compression is the primary compression attack. The DWT-domain watermarking is robust to JPEG2000 compression [5].

C. Effect of Resizing

Similar to Compression, resizing is another unintentional attack. The resizing effect can also be termed as Scaling attack. There are chances that the image gets resized by a scalar or resized to some specific dimensions while being shared over the Internet. The proposed watermarking technique is robust to this attack [5].

IV. Analysis of Parameters

To test the potency of the proposed watermarking technique different performance measuring entities are calculated. These parameters give a clear picture of effects of different noises on the extracted watermark logo.

A. Mean Square Error

For two MxN images, the Mean Square Error (MSE) simply measures the difference between them. The MSE calculates each different pixel value by comparing both the images. The value for MSE should be as small as possible to obtain a minimum error image.

If W is the original watermark logo of size MxN and RW is the extracted watermark logo also of size MxN, then MSE can be calculated by the following formula.

$$MSE = \frac{1}{M * N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left(|W(i,j) - RW(i,j)| \right)^2$$

B. Peak Signal to Noise Ratio

For two MxN images, Peak Signal to Noise Ratio (PSNR) measures the quality of the reconstructed image. It determines the ratio of the maximum signal power to the maximum power of the error signal. It is measured in decibels. The PSNR can be defined as:

$$PSNR = 10 \log_{10} \left(\frac{[\max(MSE)]}{MSE} \right)$$

C. Normalized Correlation

The measure of similarity between the original watermark logo and the recovered watermark logo is given by Normalized Correlation (NC). The value of NC ranges from 0 to 1. Zero value of NC indicates that the recovered image is very poor. As the value approaches 1 the recovered image gets more similar to the original image. For original watermark W and recovered watermark RW, NC can be defined as stated below [4].

$$NC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} W(i,j) * RW(i,j)}{\sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} [W(i,j)]^2 * \sum_{i=1}^{M} \sum_{j=1}^{N} [RW(i,j)]^2}}$$

D. Accuracy Rate

Accuracy Rate defines the degree of difference between the original and recovered watermark logo. The accuracy rate is expressed in percentage. It is the ratio of the number of similar pixels in both original and recovered watermark to the total number of pixel elements in an image [4].

$$AR = \frac{\text{No. of Correct Pixels}}{\text{Total No. of Pixels}} * 100$$

V. Graphic User Interface

A GUI has been implemented to make the relation between the user and the application more friendly and interactive. This GUI also makes it easy to analyze the robustness of the watermarked image. The GUI has been designed to provide a simple to use interface that allows easy comparisons of images.

The user first chooses a cover image and then the watermarking logo. The user can introduce desired of the three attacks like different types of noises, cropping and compression, in the watermarked image and observe its effect on the watermark. The provided GUI also helps the user to calculate and compare different performance or image quality parameters. To test the robustness of the frequency domain watermarking technique the GUI allows the user to find parameters like MSE, PSNR, NC and AR of the images [7].

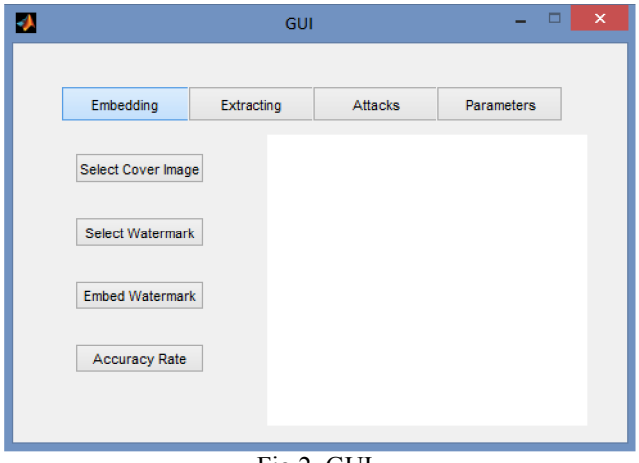


Fig.2. GUI

VI. Experimental Results

Original Images

(a) Lenna

(b) Capsicum

(c) Dogs

Watermark Logo

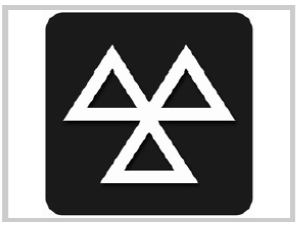
Watermarked Image:

(a) Lenna

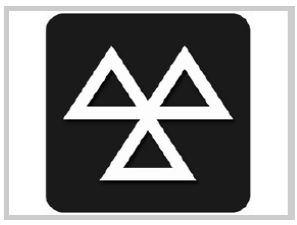
(b) Capsicum

(c) Dogs

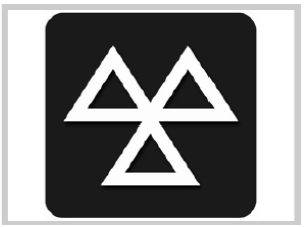
Extracted Watermarks:



(a) From Lenna



(b) From Capsicum



(c) From Dogs

Extracted Original Images:

(a) Lenna

(b) Capcicum

(c) Dogs

Following table shows the comparison of MSE, PSNR and NC for the three different images.

Table 1: Comparison of different parameters

Images compared w.r.t. Original Images	Parameters Calculated		
	MSE	PSNR	NC
Extracted Watermark	1.9952	9.9826	1
Extracted Image Lenna	1.9946	10.2425	1
Extracted Image Capsicum	1.9878	10.1189	1
Extracted Image Dogs	1.9803	10.1951	1

VII. CONCLUSION

In this paper we can conclude that a reliable digital image watermarking technique has been developed. The images in the Experimental Results show that the watermark logo can be successfully embedded in and completely extracted from any cover image. The watermark logo is imperceptible to the naked eye and can be viewed only after extraction. Table 1 shows the different values of MSE and PSNR compared for different images. The values of NC for all images is 1, this shows that the embedded watermark and the extracted watermark are similar to each other. The values of MSE and PSNR are also nearly constant.

Another conclusion that can be drawn is, if the extracted watermark is unharmed the image has not been tampered with, but if the watermark is blur or harmed, then tamper can be detected. Study of different attacks on the watermarked image show that the watermark is robust. The implemented GUI makes it easy and simple to use the application.

REFERENCES

[1] L. Tong, Q. Zheng-ding, "*The Survey of Digital Watermarking-based Image Authentication Techniques"* , 6th International Conference on Signal Processing, 2002, ICSP proceedings, vol.2,pp.1556-1559,Aug.2002

[2] V. M. Potdar, S. Han, E. Chang,"*A survey of Digital image watermarking techniques"*,3rd IEEE International conference on Industrial Informatics,INDIN'05,pp.709-716,Aug2005

[3] Mauro Barni, Franco Bartolini, Alessandro Piva, 2001, "*Improved Wavelet-Based Watermarking Through Pixel-Wise Masking"* IEEE Trans., Image Processing,vol.10,pp.783-791.

[4] Keshav S Rawat, Dheerendra S Tomar,2009,"*Digital Watermarking Schemes for Authorization against copying or Piracy of Color Images*", Indian Journal of Computer Science and Engineering,vol.1,no4,pp.295-300.

[5] Priyanka Mitra, Reena Gunjan, 2013, "A Statistical Property based Image Watermarking using Permutation and CT-QR",IEEE conference.

[6] Nidhi Divecha and Dr. N Jani, 2013, "*Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images"* IEEE Conference, Intelligent Systems and Signal Processing,pp.204-208.

[7] Karnpriya Vyas, Kirti Sethiya, Sonu Jain,2012,"*Implementation of Digital Watermarking using MATLAB software*",Compusoft International Journal of Advanced Computer Technology,vol.1,issue1.

[8] Makarand L Mali, Nitin N Patil and J B Patil , 2013, "*Implementation of Text Watermarking Technique Using Natural Language Watermarks"* IEEE Conference, Communication Systems and Network Technologies,pp.482-486.

[9] Shivani Garg, Ranjith Singh,2012,"*An efficient method for Digital Image Watermarking based on PN seuences*",IJCSE,vol4,no9,pp.0975-3397

[10] Ibrahim Kamel, Waheeb Yaqub and Kareem Kamel, 2013,"*An Empirical Study on the Robustness of a Fragile Watermark for Relational Databases"* IEEE Conference, Innovations in Information Technology,pp.227-232.