Different Types of Attack in Image Watermarking including 2D, 3D Images

Dr. Sanyam Agarwal1,Priyanka2,Usha Pal3
Department of ECE
BIT MEERUT,
U.P., INDIA
1)sanyamagarwal@hotmail.com
2)choudhary_priyanka@rediffmail.com
3) pal.usha@yahoo.co.in

Abstract—Digital Watermarking is a method through which we can authenticate images, texts and videos. Watermarking functions are not only authentication purpose, but also protection for such documents against malicious intentions to change such documents or even claim the rights of such documents. The aim of Watermarking is adding "ownership" information in multimedia contents to prove the authenticity.In this paper, we used DCT technique and different types of attack for digitally watermarked 2D and 3D images .Common attacks to watermark usually aim to destroy the embedded watermark or to impair its detection.

Keywords- Attack, Discrete Cosine Transform(DCT),Peak Signal to Noise Ratio(PSNR),Mean Square Error (MSE).

I.

II. INTRODUCTION *(DIGITAL WATERMARKING)*

Within the field of Watermarking, image watermarking particularly has attracted lot of attention in the research community. Most of the research work is dedicated to image watermarking as compared to audio and video. There may be 3 reasons for it. Firstly, because of ready availability of the test images, secondly because it carries enough redundant information to provide an opportunity to embed watermarks easily, and lastly, it may be assumed that any successful image watermarking algorithm may be upgraded for the video also. Images are represented/stored in spatial domain as well as in transform domain. The transform domain image is represented in terms of its frequencies; whereas, in spatial domain it is represented by pixels. In simple terms, transform domain means the image is segmented into multiple frequency bands. To transfer an image to its frequency representation, we can use several reversible transforms like or Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT).

Digital watermarking technology is drawing the attention as a new method of protecting copyrights for digital images. It is realized by embedding data that is insensible for the human visual system. The embedded information data is called watermark. So watermarking in digital images is the process by which a discrete data stream is hidden within an image imposing imperceptible changes of the image.

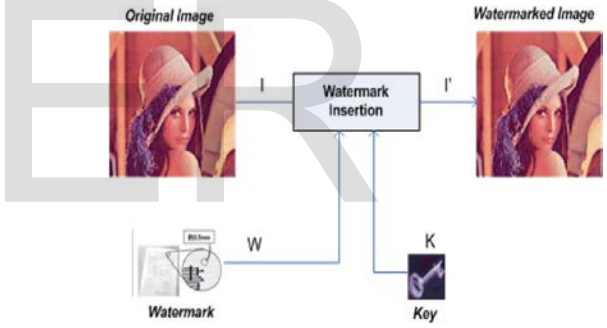

Fig: 1 Watermark Embedding Process

The general process involved in Watermarking System as illustrated in fig.1.The process can be divided into three parts: Embedding, Transmission and Extraction.

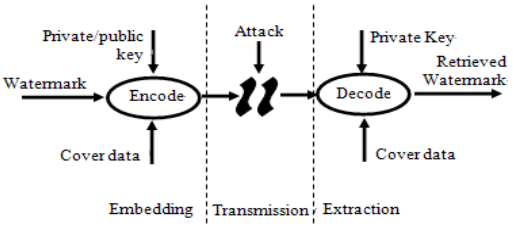

Fig: 2 Watermarking System

In the embedding process, the watermark signal may be encoded into the cover data using a specific key. This key is used to encrypt the watermark as an additional protection

level. The output of the embedding process, the watermarked image, is then transmitted to the receiver. During this transmission process, the watermarked image can be damage or corrupt due to noise or some attacks. Therefore, there is no guarantee that the watermarked image received by the receiver is exactly the same data as that sent by the transmitter. After finding the watermarked image we apply Extraction process. Extraction process, compare the watermarked image with original image. Similar watermark will prove the authenticity.

II.PROPERTIES OF WATERMARK

The important properties that arise in the study of digital watermarking techniques are :

A. Invisibility

The digital watermark embedded into the image data should be invisible to the human observer.

B. Robustness

The robust watermarking aims to embed information into a file which cannot be easily destroyed.

C. Fragile

Fragile watermarking involves embedding information into a file which is destroyed if the file is modified. This method is suitable for verification or authenticity of original content.

D. Semi-fragile

Semi-fragile watermark are robust to incidental modification, but fragile to another modification. It is sensitive to some degree of the changed to a watermarked image.

E. Imperceptible

The watermark should be imperceptible to human observe while the host image is embedded with secret data and illegal removal watermark must be impossible.

IV. WATERMARKING ATTACKS

Watermark attacks, classified into four main groups:

- Simple attacks are conceptually simple attacks that attempt to damage the embedded watermark by modifications of the whole image without any effort to identify and isolate the watermark. Examples include frequency based compression, addition of noise, cropping and correction.

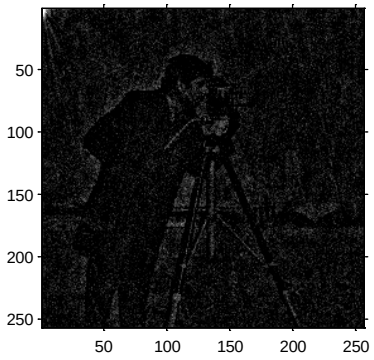

Fig: 3 Addition of Noise

- Detection-disabling attacks attempt to break correlation and to make detection of the watermark impossible. Mostly, they make some geometric distortion like zooming, shift in spatial or (in case of video) temporal direction, rotation, cropping or pixel permutation, removal or insertion. The watermark in fact remains in the cover content and can be recovered with increased intelligence of the watermark detector.
- Ambiguity attacks attempt to confuse the detector by producing fake watermarked data to discredit the authority of the watermark by embedding several additional watermarks so that it is not obvious which the first was, authoritative watermark.
- Removal attacks attempt to analyse or estimate (from more differently watermarked copies) the watermark, separate it out and discard only the watermark. Examples are collusion attack, denoising or exploiting conceptual cryptographic weakness of the watermark scheme (e.g. knowledge of positions of single watermark elements).

V. GOALS OF WATERMARKING ATTACKS

x: original (cover image), size N=M.M ,
n: noise-like watermark,
y: stego-image, with
$y=x+n$
y': attacked stego-image.

Main goals of attacks on watermarks:

- preserve image quality:
  $y'=x$
- render watermark undetectable/undecodable.

Our goal is to use prior knowledge:
- Watermark and image probability distributions
- The watermarking method used

VI. QUALITY MEASUREMENT

Two commonly measurements that are used to quantify the error between images are namely, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) [7]. Their equations are as follows:

- Peak Signal to Noise Ratio(PSNR)

  PSNR = 10 × log10 ((255×255) ÷ MSE

- Mean Square Error(MSE)

  D = abs (True Image – Inverse Image) ^2

  MSE = sum (D (:)) /numel (True Image)

Increasing PSNR represents increasing the quality of image. In general when the PSNR is 35 dB or larger, then the two images are virtually indistinguishable by human observers. Image Quality depends upon attacks, watermark length and size of image

VII. ATTACKS ON GRAY SCALE IMAGE

1) Blurred Image using DCT

Fig 4: Blurred Image

ALPHA	MSE	PSNR
1) 0.01	538.66	20.81
2) 0.1	2.635e^003	13.92
3) 0.2	9.035e^003	8.571
4) 0.5	5.394e^004	0.811

Table 1: Blurred Image using DCT with different values of Alpha, MSE , PSNR

2) Cutting part of Image

Fig 5: Blurred Image

VIII. ATTACKS ON COLOUR SCALE IMAGE

1) Blurred Image using DCT (RGB to Gray Image)

Fig 6: Blurred Image

2) Cutting part of Image (RGB to Gray Image)

Fig 7: Cutting part of Image

IX. ATTACKS ON 3-D IMAGE

1) Uniform Noise

Fig 8: Adding Uniform Noise in 3D image

2) Crop Image

Fig 9: Cutting part of 3D image

3) Filtered Image

Fig 10: Adding Filter in 3D image

X. CONCLUSION

In Watermarking scheme, image is considered as a communication channel to transmit messages. In this paper, we presented the different types of attack that affected the quality of 2-D, 3-D watermarked images.

REFERENCES

[1] RIDZOŇ, R.; LEVICKÝ, D.: Usage of different color models in robust digital watermarking,978-1-4244-3538-8/09/$25.00©2009 IEEE.
[2] RIDZOŇ, R.; LEVICKÝ, D.: Robust digital watermarking based on the log-polar mapping. In: *Radio engineering*. vol. 16, no. 4 (2007), p. 76-81.
[3] Avani Bhatia, Mrs. Raj Kumari U.I.E.T, Punjab University: "Digital Watermarking Techniques", white paper.
[4] Chunlin Song, Sud Sudirman, Madjid Merabti ,School of Computing and Mathematical Sciences Liverpool John Moores University,UK : "Recent Advances and Classification of Watermarking Techniques in Digital Images", ISBN: 97-1-902560-22-9 © 2009PGNet.
[5] Mauro Barni, Franco Bartolini, Vito Cappellini,: "A DCT-domain system for robust image watermarking", M. Barni et al. / Signal Processing 66 (1998) 357-372.
[6] Chunlin Song, Sud Sudirman, Madjid Merabti School of Computing and Mathematical Sciences Liverpool John Moores University, UK," Recent Advances and Classification of Watermarking Techniques in Digital Images", ISBN: 978-1-902560-22-9 © 2009 PGNet.
[7] Wen Yuan Chen and Shih Yuan Huang, Department of Electronic Engineering National Chin-Yi Institute of Technology: "Digital Watermarking Using DCT Transformation", white paper.
[8] R.Gonzalez and R.Woods, "Digital Image Processing", 1998, Pearson Edition.
[9] Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T.: Digital Watermarking and Steganography, 2Nd Ed. ISBN: 978-0123725851.
[10] Liy, Anthony Dicky, Chunhua Sheny, Anton van den Hengely, Hanzi Wang, 2012. Incremental Learning of 3D-DCT Compact Representations for Robust Visual Tracking,18 July 2012, *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE*, pp. 1-21.
[11] Www.advancesourcecode.com
[12] Www.codeforge.com/libs/highlight/stles/sunburst.css