DWT Based Robust Technique of Watermarking Applied on Digital Images

Chirag Sharma, Deepak Prashar

Abstract:- Digital Watermarking is a process of embedding unnoticeable signal in an image in the form of text and image in such a way that intruder is no able to trace the signal to enhance Copyright Protection. This Paper presents an efficient Watermarking Technique for Digital Media Content Protection and Copyright Protection. Watermarking is a technique to embed hidden and unnoticeable signal into digital media in such a way that if an intruder wants to copy it, he can be caught on the basis of Copyright protection and Ownership Identification. There are many Techniques that are available to watermark the data, proposal we are discussing DWT Technique which is most robust to attacks rather than LSB for the protection of Digital Images. We are going to find the Quality loss after the addition of watermark after applying various attacks on Watermarked Image, the more the quality loss will be there lesser will be the efficiency of Watermarking. There will be many factors that can effect the quality of the Images after the addition of Watermarking that are discussed in Later Section. The Creating on GUI and Implementation of our purposed Algorithm is realized using MATLAB.

Keywords: - Discrete Wavelet Transform (DWT), Image Watermarking, Information Hiding,, Invisible Watermarking, PSNR, Visible Watermarking.

I. INTRODUCTION

Digital Data is available in World Wide Web in the form of Images, Audio and video in large amount. It is very easy to copy, distribute, modify, manipulate and destroy by the intruders, So there is a great need to protect the integrity of the digital data, The technique that is useful to avoid unauthorized copying or tempering of digital data is Watermarking. Digital watermarking is used for protection of digital images. Digital Watermark is a visible or invisible identification code that is permanently embedded in the host media. Watermark of the media aims at discouraging unauthorized copying [2].

When Watermark is added to digital data such as images even if any intruder tries to damage or manipulate it, he can be caught after the retrieval of watermark on the basis of Copyright Protection. There are many features of Watermarking [8]. Watermark should be Imperceptible, transparent, secure, robust so as to enhance its application in Copyright Protection, Video Authentication, Fingerprinting, Copy Control. There are many techniques of Watermarking that are described in Figure1 [6]. The most popular technique is the least significant bit (LSB) method.

Manuscript received on April 26, 2012.

Chirag Sharma, Computer Science Department, Lovely Professional University, Jalandhar , India, +919464014927. (email : ch.savachi@gmail.com).

Deepak Prashar, Computer Science Department, Lovely Professional University, Jalandhar, India,+919815688883
(e-mail: Deepak.prashar@lpu.co.in).

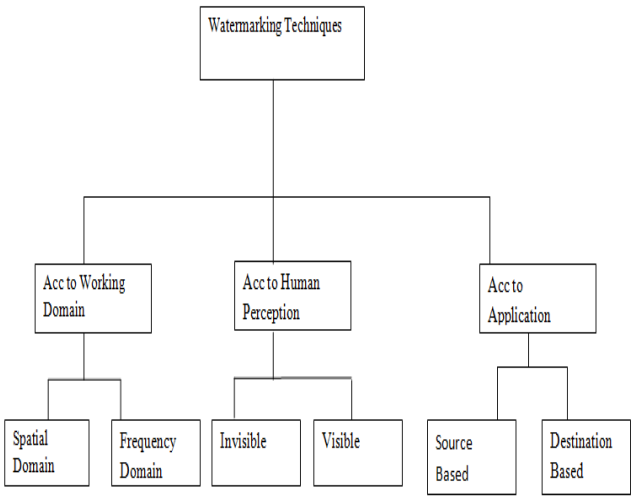

Figure1: Techniques of Watermarking [6]

In transform domain the watermark is embedded by modifying the frequency coefficients of the transformed image. The common methods in the transform domain are Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), etc [1]. The main procedure of Watermarking is followed in 2 parts: Watermark addition and embedding and Watermark Retrieval and extraction. Our main concern is that the output watermarked image should not lose much of a quality after the addition of Watermark. We have designed a Graphical User Interface for the addition of Watermark and retrieval of Watermark. Embedding can be done in an image in the form of Text or Image and can be done in many formats. Watermark Extraction can be done to recover the watermark used for copyright protection. In this paper, we are going to use DWT technique for Watermarking. The DWT decomposes input image into four components namely LL, HL, LH and HH where the first letter corresponds to applying either a low pass frequency operation or high pass frequency operation to the rows, and the second letter refers to the filter applied to the columns. The lowest resolution level LL consists of the approximation part of the original image [8].The remaining three resolution levels consist of the detail parts and give the vertical high (LH), horizontal high (HL) and high (HH) frequencies. In the proposed algorithm, watermark is embedded into the host image by modifying the coefficients of high-frequency bands i.e.HH subband described in figure 2 [8].

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

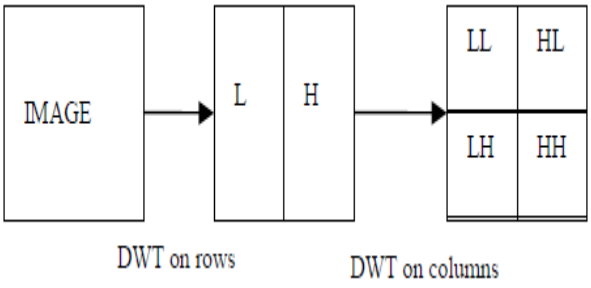

Figure 2: DWT Decomposition [8]

II. PURPOSED SCHEME

The purposed algorithm is based on DWT Technique and is divided into 2 phases

A. Watermark Embedding
B. Watermark Retrieval
C. Efficiency of Watermarking(Calculating PSNR)

A. Watermark Embedding

1. Select a Source Image
2. Separate Image into 4 Bands using DWT : LL, HL,LH, HH(Diagonal).
3. Select HH Band For Embedding of Watermark.
4. Watermark Embedding can be done by the following Figure 2 [9]

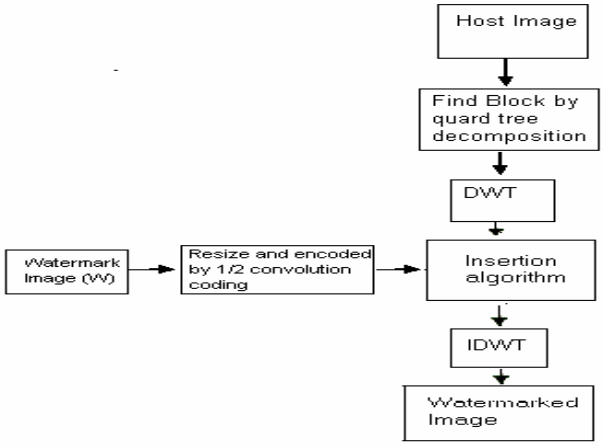

Figure3: Embedding of Watermark in an image [9]

5. So hence our values can be calculated as :
$$S \times W + K(optional) \rightarrow Y \quad (1)$$
Here S= Source Image W=Watermark K=Key that is an optional field and Y is a Watermarked Output image
6. Key is added to provide Encryption
7. Thus Values of HH Band are modified and Now Apply Inverse Transformation
8. Thus After applying Inverse Transformation we get
$$Y \leftarrow S \times W + K \quad (2)$$
9. Inverse DWT can be applied after modifying the sub band values of HH band

B. Watermark Retrieval or Watermark Extraction

1. Perform DWT on Watermarked Image.
2. Perform DWT on HH band of the image.
3. Extraction of Watermark Can be done using formula
$$W = (Y - K)/S \quad (3)$$
4. Perform Inverse Transformation on Watermarked Image and put the right Value of key if inserted to extract the watermark.

C. Efficiency of Watermarking

After the addition of Watermark we have to determine the efficiency of our purposed technique. This can be done by following factors

1. *Deblurring or Additional noise*: This is a parameter that determines how much disturbance or noise is contained in the image after the addition of Watermark. It can be determined by a Formula. G=HF+N, G=Watermarked Image H=Source image F=disturbance N= additional noise.
2. *Salt and Pepper Attack:* This attack is applied to watermarked image and it results in additional noise of the image.It is given in Figure no. 7
3. *Number of Colors reduced*: The more the numbers Colors reduced lesser the quality of Watermarked image.
4. *Hue Value (hsv)* : Hue is defined as the strength and saturation. The more the hue value better will be the quality of watermarked image
5. *Cropping*: Here attacker is interested in small portion of the watermarked object, such as parts of certain picture or frames of video sequence. This attack will enable the intruder to crop any part of the multimedia he wants to use [2] . This will no degrade the quality due to loss of frames but also there is a loss of important information. This attack tests the efficiency of watermarking such that how watermarked can be removed from an image such that no quality is lost. Her if the watermarked is removed easily that means the technique is not robust. It is given by following example

Figure4: Attack of Cropping on Watermarking

6. *Rotation and Scaling*: It is mostly done in Still Images. When it is being performed Correlation based detection and extraction fails considerably. It would be possible to search on different angles and scaling factors until correlation peak is found that will be very complex [7].
7. *JPEG Compression*: This is generally an unintentional attack which appears in multimedia applications. Mostly the multimedia in Internet are distributed in compressed form because it is not easy to transmit original source data. DCT domain Watermarking is more robust to JPEG compression than Spatial domain [4]. This is one of the most dangerous attacks

since attacker sometimes use those tools that can compress the original video without loss of much quality and frames and the multimedia distributed through internet is pretended as from original source but it is not exactly so.

8. *Number of Frequency Components lost*: They determine the quality of Watermarked image after the addition of Watermark, Lesser the number of these components lost more will be quality of Watermark.

PSNR Values and Accuracy Rate: The visual quality of watermarked and attacked images is measured using the Peak Signal to Noise Ratio. It is given by equation 5

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (4)$$

Here MSE= Mean Squared Error between Original and Distorted Images. It is given by equation 6 [8]

$$MSE = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left(\frac{[OI(i,j) - DI(i,j)]^2}{MxN} \right) \quad (5)$$

Accuracy Rate Can be determined by the Equation

$$A = D/O \quad (6)$$

where D= No. Of Distorted pixels and O= Total No of Pixels in an image

III. DESIGNED GUI FOR THIS TECHNIQUE USING MATLAB

Following Figures indicate the Graphical User Interface designed for insertion and extraction of watermark from the images. Realization of GUI is shown in Figure No.5

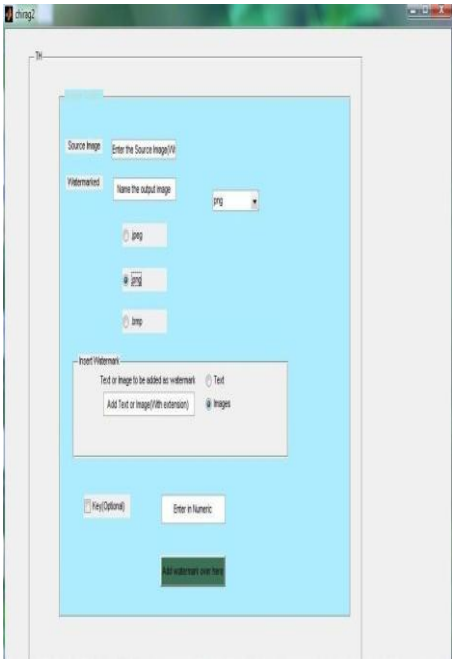

Figure5: Insertion of Watermark in an image

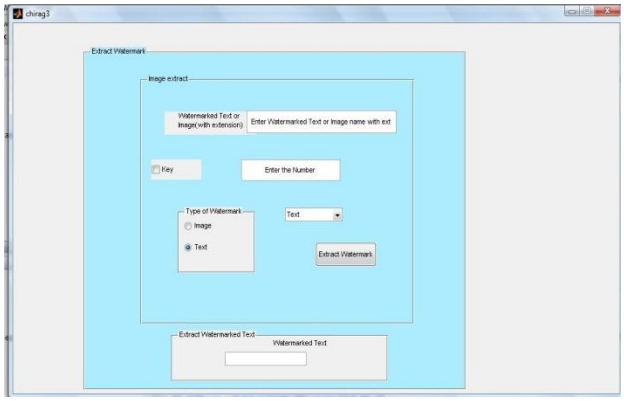

Figure 6: Extraction of Watermark from an image

IV. RESULTS AND CALCULATIONS

After the series of Experiments performed on Images in MATLAB, we have realized the above factors determine the Quality of Watermarked Object. Our purposed Technique is better than LSB technique to Watermarking because it is more robust to Cropping, Rotation and Scaling, Salt and Pepper attack, Gaussian Noise in case of Invisible Watermarking and there are less number of Frequency components lost in the watermarked image. To measure the effectiveness of the method, the performance metrics is measured. The quality of a watermarked video is measured by the peak signal-to noise ratio (PSNR). The quality of extracted watermark can be measured by: PSNR (Peak Signal-to-Noise Ratio) and AR (Accuracy rate). PSNR is provided only to give us a rough approximation of the quality of the visible watermark. The Results show the high value of PSNR ranging from 30-35 db (decibel). It shows that the purposed technique is efficient enough to handle such attacks. Using equation in figure 5 we have calculated PSNR values after applying following attacks seems to be: PSNR Value can be calculated as given in Table1:
PSNR is measured in db. The higher value of PSNR indicates more efficiency of the purposed scheme

Table1 : Calculation of PSNR values by applying various attacks on purposed scheme of Watermarking

S No.	Attack	PSNR value(db)	Actual Image	Watermarked Image
a.	Salt and Pepper Attack	35.123		
b.	Gaussian Noise	34.327		

c.	Cropping	32.713		
d.	Rotation and Scaling	32.284		
e.	Deblurring	34.410		

Resulting PSNR values are higher that indicates higher efficiency of Purposed Watermarking Scheme

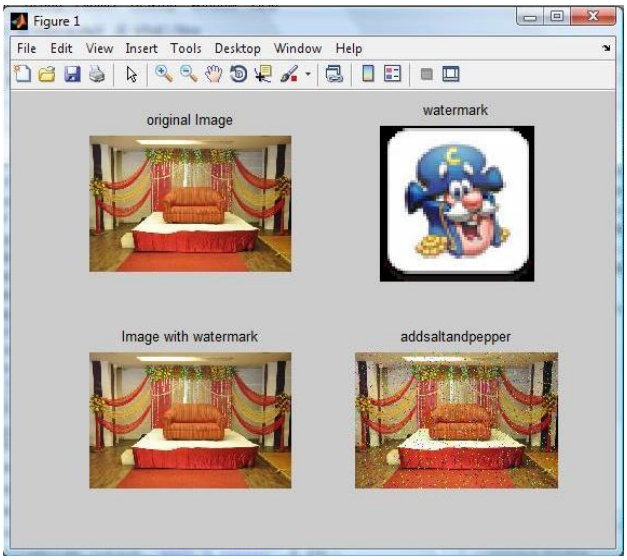

Figure 7: Addition of watermark inside the image and performing the salt and pepper attack on the watermarked image to find the difference of 2 images.

V. CONCLUSION

In the growing field of multimedia technology the area of watermarking has significant importance but still there is a need to protect digital data because intruder are finding different measures to trace data and use it illegally. Our Purposed technique is useful in insertion of watermark in such a way such that intruder cannot trace it easily and there is less quality of loss after the insertion of watermark inside the images. Watermarking in videos is one of the major issues throughout the internet. People are adding their owner watermarks over the original watermark hence to hinder copyright protection and owner ship identification. A number of techniques have been proposed of watermarking, However our purposed technique is more robust than LSB Technique thus provide better results in case of Copyright Protection and Ownership Identification, The performance of Our purposed watermarking scheme is evaluated with common image processing attacks such as additive noises, filtering, intensity adjustment, histogram equalization, JPEG compression, Scaling and rotation. Experimental results demonstrate this watermarking technique is robust against those attacks. Additional Security has been provided after the addition of key that is used for encryption. Implementation and comprehensive analysis of multimedia objects have been performed successfully.

REFERENCES

1. Kamble Sushila, Maheshkar Vikas, Agarwal Suneeta, K Srivastava Vinay, "DWT-SVD Based Secured Image Watermarking For Copyright Protection using Visual Cryptography", CS & IT-CSCP 2012, ITCS, SIP, JSE-2012, CS & IT 04, pp. 143–150, 2012.
2. Chandra Munesh, Pandey Shikha," A DWT Domain Visible Watermarking Techniques for Digital Images" International Conference on Electronics and Information Engineering (ICEIE 2010),V2,Pp-421-427.
3. Saraswathi.M,"Lossless Visible Watermarking for Video",IJCSIT,V2(3),Pp-1109-1103,2011.
4. Subbarayan Sadasivam, Ramanathan S.Karthick," EffectiveWatermarking of Digital Audio and Image using Matlab Technique" Second International Conference on Machine Vision, Pp-317-319,2009.
5. A. Sangeetha , Gomathy.B , K.Anusudha,"A Watermarking Approach to Compact Geometric Attacks"International Conference on Image Processing,Pp-381-385,2009.
6. Li Xin, Shoshan Yonatan, Fish Aleander, Jullien Graham, Yadid-Pecht Orly (2008)"Hardware Implementation of Video Watermarking" Pp-9-15.
7. Jayamalar T, Radha V (2010) "Survey on Digital Video Watermarking Techniques and attacks on Watermarks", International Journal of Engineering and Technology, Vol. 2(12), Pp 6963-6967,2010.
8. Sathik M. Mohammed and Sujatha S.S,"An Improved Invisible Watermarking Technique for Image Authentication",International Journal of Advanceed Science and Technology,Vol-24,Pp-61-74,2010.
9. Phadilkar Amit, Verma Bhupendra,Jain Sanjeev"A New Color Image Watermarking Scheme, INFOCOMP Journal of Computer Science",International Conference,2006.

AUTHORS PROFILE

Chirag Sharma was born in Jalandhar on 15th October. He received his B.TECH Degree from Punjab.Technical.University and M.TECH Degree from Lovely Professional University in 2010 and 2012 respectively. His Research Interests include Image Processing, Software Engineering and Software Quality Assurance, Data Warehousing etc.

Deepak Prashar was born in Himachal Pradesh. He received his M.TECH Degree from Punjab Engineering College Chandigarh. He is GATE qualified. His Research Interests include Image Processing, Neural Networks, Software Quality Assurance, Data Warehouse etc.