Efficient Watermarking Technique for Digital Media (Images and Videos)

Chirag Sharma

Department of Computer Science and Engineering Lovely Professional University Jalandhar 144001, India

Deepak Prashar

Department of Computer Science and Engineering Lovely Professional University Jalandhar 144001, India

Abstract— In This Paper we are going to purpose 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, In our purposal we are discussing DWT Technique which is most robust to attacks rather than LSB for the protection of Digital Images. We will try 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 will be 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].

- 1. *Imperceptibility* It should be perceptually invisible so that data quality is not degraded and attackers are prevented from finding and deleting it. A watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, un watermarked content [8].
 - 2. Readily Extractable The data owner or an independent control authority should easily extract it[8].
 - 3. Unambiguous The watermark retrieval should unambiguously identify the data owner[8].
- 4. *Robustness* It should tolerate some of the common image processing attacks. A watermark is called robust if it resists a designated class of transformations [8].

There are many techniques of Watermarking that are described in Figure 1 [6]

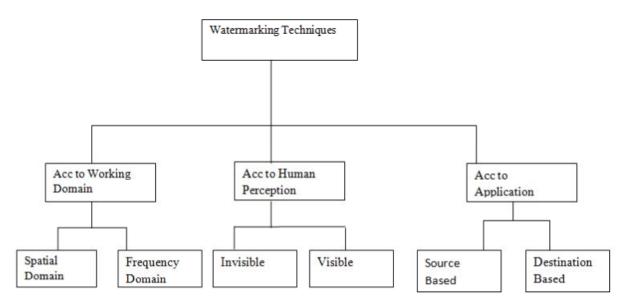


Figure 1: Techniques of Watermarking [6]

The most popular technique is the least significant bit (LSB) method. 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 Watermark Embedding by applying DWT Technique and Watermark 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 sub band [8].

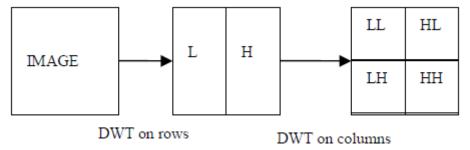
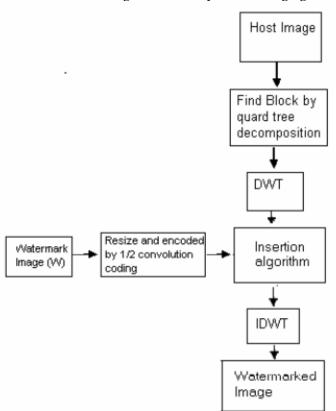


Figure 2. DWT Decomposition [8].

II. PURPOSED SCHEME

The purposed algorithm is divided into 3 phases

- A. Watermark Embedding
- B. Watermark Retrieval or Extraction
- C. Quality loss parameters
- A. Watermark Embedding [10]
- 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]

Figure 3: Embedding of Watermark in an image [9]

- 5. Hence the equation becomes $S \times W + Key(optional) \rightarrow S_{Wm}$ (1) Here S= Source Image W=Watermark k=Key that is an optional field and S_{Wm} is a Watermarked Output image.
- 6. Key is added to provide Encryption.
- 7. 2 types of Watermarked Images are produced
 - a. Watermarked Image without key.
 - b. Watermarked Image with Key (It provides more Security).
- 8. Values of HH Band are modified and now Apply Inverse Transformation.
- 9. After applying Inverse Transformation we get $S_{Wm} \leftarrow S \times W + K(optional)$ (2)
- 10. Inverse DWT can be applied after modifying the sub band values of HH band
- B. Watermark Retrieval or Watermark Extraction [10]
- 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 = (S V)/(S V)

 $W = (S_{Wm} - K)/S \tag{3}$ 1. Parform Inverse Transformation on Wetermarked Image and put the right Value

- 4. Perform Inverse Transformation on Watermarked Image and put the right Value of key if inserted to extract the watermark.
- C. Quality Loss Parameters

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

- 1. *De blurring 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. Screen Depth: Screen Depth is defined as the number of bit maps in an image
- 3. *Number of Colours reduced*: The more the numbers Colours 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 [10].
- 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



Figure 4: Attack of Cropping on Visible Watermarking

- 6. *Intensity*: If the watermarked image loses its intensity that means the quality of the image is degraded after the addition of Watermark. It is estimated that image intensity should vary from 0.4-1[1].
- 7. *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].
- 8. *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.
- 9. *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 [10].

PSNR Values and Accuracy Rate: PSNR is a Peak Signal to Noise Ratio. It is used to determine the Efficiency of Watermarking by calculating the noise. The more noise will give rise to less quality of image. The visual quality of watermarked and attacked images is measured using the Peak Signal to Noise Ratio. It is given by equation 4 [8]

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

Here MSE= Mean Squared Error between Original and Distorted Images. It is given by equation 5 [8]

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

Here OI(i,j), DI(i,j) are 2 monochromatic Images whose co ordinates are i,j

Accuracy Rate Can be determined by the Equation

A=D/O where D= No. Of Distorted pixels and O= Total No of pixels in an image (6)

III. DESIGNED GUI FOR THIS TECHNIQUE USING MATLAB

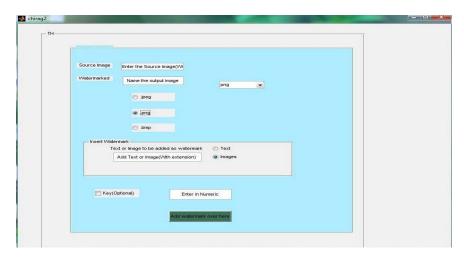


Figure5: Insertion of Watermark in an Image

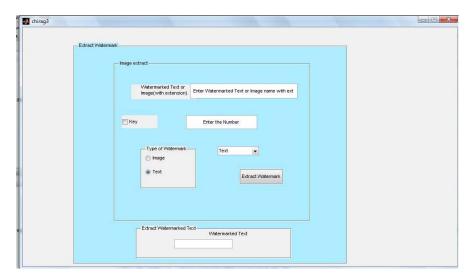


Figure6: Extraction of Watermark from an Image

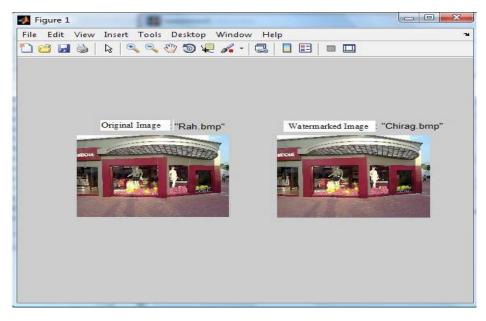


Figure7: Comparison of Actual and Watermarked Images

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 in case of Visible Watermarking, 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 [2]. It is estimated that the PSNR values after applying following attacks seems to be: PSNR Value can be calculated by equation in figure 5. Table 1 gives all the PSNR values of different attacks.

Attack **PSNR** Actual Image Watermarked Image Value Type Gaussia 30.15 Rotation 29.12 and Scaling Croppin 26.12 g

Table 1. Calculation of PSNR values by applying various attacks on Watermarking

V. CONCLUSION

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. This purposed Scheme can work on Images and Videos But yields better results in Images. Future Work can be done on robust technique applied on videos to increase efficiency of watermarking.

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.
- 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.
- Saraswathi.M,"Lossless Visible Watermarking for Video",IJCSIT,V2(3),Pp-1109-1103,2011.
 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.
- [10] Sharma Chirag, Prashar Deepak,"DWT Based Robust Technique of Watermarking applied on Digital Images", IJSCE, Vol. 2(2), Pp-399-402.

AUTHORS PROFILE

Chirag Sharma was born in Jalandhar on 15th October. He is an Assistant Professor in L.P.U. 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 etc.



Deepak Prashar was born in Himachal Pradesh. He received his M.TECH degree from Punjab Engineering College. He is GATE qualified He woks as an Assistant Professor in LPU. His Research Interests include Image Processing, Neural Networks, Software Quality Assurance, Data Warehouse etc

