Robust Watermarking Scheme for Quality Loss of Data

#1Chirag Sharma, #2Anshu Sharma, #3Shilpa Sharma
Department of Computer Science and Technology
1Ch.savachi@gmail.com,
2Asharma106@yahoo.com,
3Shilpa_sharma_86@yahoo.com
Lovely Professional University, Punjab, India

Abstract

Watermarking is a technique of embedding hidden and unnoticeable signal into an image in the form of text and image so that even if unauthorized person tries to access and use it illegally, he could be caught on the basis of Copyright Protection and Ownership Identification. There are 2 methods that can be followed to embed a watermark in an image: Visible Watermarking and Invisible Watermarking. Visible Watermarking is used to display the watermark inside the image so that intruder can’t use it unless he has copyrights for that image. Invisible Watermarking hides watermark from the intruder so that he can be caught on the basis of Copyright Protection. Quality loss is the major issue in Watermarking. Embedding watermark inside the image can degrade the quality of watermarked image. In this paper we are going to present a technique that can reduce less amount of quality after the insertion of watermark in both visible and invisible watermarking methods. The implementation of Visible and Invisible Watermarking methods is realized with the help of MATLAB. Results are taken by calculation of PSNR values of Watermarked images after applying various attacks on Watermarked image to check the efficiency of Watermarking.

Keywords: Discrete Wavelet Transformation (DWT), Invisible Watermarking, Visible Watermarking, Information Hiding, Copyright Protection, Quality loss.

1. Introduction

There is a large amount of digital and multimedia data available in the form of images, audios and videos in World Wide Web (www). 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 and providing different means to secure it. Digital Watermark is a visible or invisible identification code that is permanently embedded in the host media in the form of text and image to host media to protect copyrights for that media. Watermark of the media aims at discouraging unauthorized copying and providing ownership identification [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. Watermark should be imperceptible, transparent, secure and robust so as to achieve good and better results in the application areas such as Copyright Protection, Video Authentication, Fingerprinting, Copy Control, and Broadcast Monitoring etc. This paper presents a technique that achieves good results in the field of copyright protection. There are many techniques that can be applied to embed a watermark inside the image. These techniques are given in following Figure No. 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 [10]. 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 and after applying various attacks on watermarks. 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. After applying the attacks like Cropping, Resizing etc we are going to apply attacks to test the efficiency of watermarking. In this paper, we are going to use DWT technique for Watermarking. There is a decomposition applied by DWT to 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 [11].

2. Purposed Scheme

Our Purposed Scheme is based on both Invisible and Visible Watermarking methods. For Invisible Watermarking we will follow DWT Based Robust Method for Insertion and Extraction of Watermark from the image. This is realized by designing a Graphical User Interface for Insertion and Extraction of Watermark. Purposed Algorithm for Invisible Watermarking is divided into 2 phases.

2.1 Watermark Embedding [10]

Watermark Embedding follows various steps
1. Source Image is selected.
2. Source Image is separated into 4 Bands using DWT : LL, HL, LH, HH (Diagonal).
3. Select HH Band For Embedding of Watermark.
4. Watermark Embedding and purposed scheme algorithm is given by the following Figure 3

Figure 3: Embedding of Watermark in an image

5. So hence our values can be calculated as :
   \[ S \times W_m + K \text{ (optional)} \rightarrow F \]  \hspace{1cm} (1)
   Here S= Source Image Wm=Watermark K=Key that is an optional field and F 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. After applying Inverse Transformation \[ F \leftarrow S \times W_m + K \]  \hspace{1cm} (2)
9. Inverse DWT can be applied after modifying the sub band values of HH band

2.2 Watermark Extraction [10]

1. DWT is applied on Watermarked Image.
2. DWT is applied on HH band of the image.
3. Extraction of Watermark Can be done using formula
   \[ W_m = (F - K)/S \]  \hspace{1cm} (3)
4. Inverse Transformation is applied on Watermarked Image and put the right Value of key if inserted to extract the watermark.

In Visible Watermarking same method is used but the difference is the watermark is visible to the intruder.

3. Parameters affecting the quality loss of the Watermarked Image

There are many factors that can affect the quality loss of the watermarked image. After the insertion of watermark inside the image in the form of text...
and image. Watermarked image is found but we don’t know how efficient it is? So to test the efficiency of watermarking following attacks are applied. If we get high PSNR value it means the technique proposed is a robust one. The attacks applied on watermarked image are as follows:

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 [10].

2. **Salt and Pepper Attack**: This attack is applied to watermarked image and it results in additional noise of the image. It can affect the quality of watermarked image if its value is higher.

3. **Hue Value (hsv)**: Hue is defined as the strength and saturation. The more the hue value better will be the quality of watermarked image. The more the number of colours inside the image more will be the hue value [10].

4. **Luminance and Chrominance Effect**: These Effects determine the colour images used for watermarking. Higher value of \( Y \) (Luminance) and \( C_b, C_r \) (2 Chrominance Components) of the watermarked Image will lead good results in PSNR.

5. **Cropping**: This is a very dangerous attack because intruder can crop out the watermark from the image and use it for his own purposes. In this attack, 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 not 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 [10]. If the watermarked is removed easily that means the technique is not robust. It is given by following example. In the given example watermark has been removed. If this watermark is replaced by other watermark the efficiency of the watermarking is less.

6. **Rotation and Scaling**: It is mostly done in Still Images. When it is being performed Correlation based detection and extraction fails considerably. By applying this attack, original dimensions of the images are lost. 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 is 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 [10].

9. **Gaussian Noise**: It is an additional noise that can hamper the quality of the watermarked image hence affecting the efficiency of the proposed scheme. This attack is demonstrated by Figure no. 5.

**PSNR Values**: PSNR is a quality metric to determine the efficiency of watermarking. It is the ratio between maximum power of a signal and power of corrupting noise that affects quality of a image [3]. It is expressed in logarithmic decibels (db). The visual quality of watermarked and attacked images is measured using the Peak Signal to Noise Ratio. It is given by equation 4

\[
\text{PSNR} = 10 \log_{10} \left( \frac{255^2}{MSE} \right)
\]  

(4)

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

\[
MSE = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{(I(x, y) - D(x, y))^2}{MN}
\]

(5)

I, D= Monochromatic Images
Pixels are represented using 8 bits per sample.

4. **Results and Calculations**

After successful realization of our proposed scheme for invisible and visible watermarking
methods in MATLAB and after applying above mentioned attacks on watermarked image we have concluded that PSNR value of Invisible Watermarking methods yield higher PSNR Value as compared to Visible Watermarking method. Efficiency of the purposed scheme is measured by applying Cropping, Rotation and Scaling, Gaussian Noise, Salt and Pepper attack on output watermarked image. If the output watermarked image yields high PSNR value after applying various attacks then it is an efficient scheme. The results show that PSNR value of Invisible Watermarking methods yield PSNR Value from 30-35 decibels (db) and PSNR value of Visible Watermarking method yields PSNR value from 25-35 db after applying various attacks on watermarked image. So the Quality loss is determined by accuracy rate and PSNR value. The higher the value of PSNR and Accuracy Rate more will be Watermarking Efficiency. PSNR is measured in db. The higher value of PSNR indicates more efficiency of the purposed scheme. 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 is less number of Frequency components lost in the watermarked image as compared to Least Significant Bit Modification (LSB). PSNR Value can be calculated as given in Table 1:

Table 1: Calculation of PSNR values by applying various attacks on purposed scheme of Invisible Watermarking.

<table>
<thead>
<tr>
<th>S N o.</th>
<th>Attack</th>
<th>PSNR value (db)</th>
<th>Actual Image</th>
<th>Watermarked Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Salt and Pepper Attack</td>
<td>34.123</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b.</td>
<td>Gaussian Noise</td>
<td>35.727</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c.</td>
<td>Cropping</td>
<td>31.412</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

d. Rotation and Scaling 33.284
e. JPEG Compression 33.780

Table 2: Calculation of PSNR values by applying various attacks on purposed scheme of Visible Watermarking

<table>
<thead>
<tr>
<th>S N o.</th>
<th>Type of Attack</th>
<th>Original Image</th>
<th>Watermarked Image</th>
<th>PSNR value (db)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Salt and Pepper Attack</td>
<td></td>
<td></td>
<td>26.724</td>
</tr>
<tr>
<td>b.</td>
<td>Gaussian Noise</td>
<td></td>
<td></td>
<td>27.746</td>
</tr>
<tr>
<td>c.</td>
<td>Cropping</td>
<td></td>
<td></td>
<td>31.123</td>
</tr>
<tr>
<td>d.</td>
<td>Rotation and Scaling</td>
<td></td>
<td></td>
<td>30.640</td>
</tr>
<tr>
<td>e.</td>
<td>JPEG Compression</td>
<td></td>
<td></td>
<td>31.123</td>
</tr>
</tbody>
</table>

Resulting PSNR values are higher that indicates higher efficiency of Purposed Watermarking Scheme. Invisible Watermarking yields higher PSNR Values after applying different attacks on Watermarked Image.

Figure 5: Addition of watermark inside the image and performing the Gaussian Noise attack on the watermarked image to find the difference of 2 images.
5. Conclusion and Future Scope

In the growing field of multimedia technology the area of watermarking has significant importance but still there is a need to protect digital data and provide ownership identification because intruder are finding different measures to trace data and use it illegally. Our Proposed 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. Visible watermarks are added in images to identify the owner of the images. Watermarking in videos is one of the major issues throughout the internet. People are adding their own watermarks over the original watermark hence to hinder copyright protection and ownership identification. A number of techniques have been proposed of watermarking. However our proposed technique for visible and invisible watermarking is more robust than LSB Technique thus provide better results in case of Copyright Protection and Ownership Identification. Invisible Watermarking is giving better results than visible watermarking. The performance of the given proposed scheme for invisible and visible watermarking methods 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. The results clearly indicate that proposed scheme is giving high PSNR value as compared to other schemes. More efficiency will give good results in Copyright Protection and Ownership Identification. 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. Our proposed scheme is meant for images but it is difficult to use this technique in videos as videos comprise of different frames. It is tough to apply this scheme in higher size videos on regular basis. More work can be done by applying this scheme in videos in near future.

6. References


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. He is an Assistant Professor in LPU. His Research Interests include Image Processing, Software Engineering and Software Quality Assurance, Data Warehousing etc.
Anshu Sharma was born in Jalandhar City. She received her B.TECH degree from Punjab Technical University in 2009. She is currently doing M.TECH from Punjab Technical University. She has 3 years of teaching experience. Her Research Interests include Software Engineering, Expert Systems, Real Time Systems etc.

Shilpa Sharma was born in Jalandhar. She has done BTECH from PTU and currently perusing her MTECH from PTU. She works as a Lecturer in Lovely Professional University. She has 3 years of Experience as a Lecturer. Her Research Interests Include Software Engineering, Expert Systems and Neural networks Etc.