A ROBUST AND SECURE VISIBLE WATERMARKING SCHEME BASED ON MULTI WAVELET TECHNIQUE WITH MODIFIED FAST HAAR TRANSFORM [MFHWT]

Shefaly Sharma¹, Jagpreet Kaur²

¹(Computer science and engg., Lovely Professional University, Jalandhar, India)
²(Computer science and engg., Lovely Professional University, Jalandhar, India)

ABSTRACT

Internet has rapidly become popular worldwide and we can see that people are sharing huge amount of data [photos, videos, audio files and other crucial information] through Internet. So security of data is becoming a crucial issue. In this paper, we are providing a robust image watermarking technique. We are going to apply watermarking using multi wavelet transformation with modified fast Haar wavelet transformation [MFHWT]. Watermarking is a technique by which user can get copyright protection of the data so that no other person is able to use it without the permission of its owner.

Keywords: Visible Watermarking, MFHWT, Multi Wavelets, PSNR, MSE.

I. INTRODUCTION

There are a lot of changes being made in the field of internet and multimedia. Now days, it has become possible to create, manipulate, and transmit data at much higher rates due to the advancements being made. Protection of multimedia content has become challenging due to the threats of data authentication, and protection against illegal use of data are being increased so security has become one of the most significant and challenging problems. Watermarking is one of the popular techniques of image processing. It is used to observe authentication of licensed user over e-commerce applications and finds its use in illegal applications like copying multimedia data. A Watermark system consists of key (public key and private key). The use of key provides security i.e. prevents unauthorized use of data.[7]
1. Technologies used for Security of Multimedia

1.1 Fingerprinting
It is a technique which is used to protect data from unauthorized redistribution. It is used for embedding a unique ID called fingerprint into each user’s copy for representing anti-collision code [ACC], which can help to identify the criminal when an unauthorized link is found[5].

1.2 Cryptography
It is a technique used for secure communication. It converts data into such a form that it can only be read by the receiver. No other person is able to detect it. So for secure communication it uses public and private keys. These keys are only known to sender and receiver. If other person wants to read the data than he first needs to know the key value, and detecting this key value is not an easy task.[3].

1.3 Steganography
It is a method of hiding message such that only the sender and receiver are able to read the message. It replaces the bits of useless data in regular files with bits of different, invisible information. The hidden information can be image or text.[7]

1.4 Watermarking
It is used to provide copyright protection and also provides robustness against various attacks. Watermarking is one of the popular techniques of image processing. It is used to observe authentication of licensed user over e-commerce applications and finds its use in illegal applications like copying multimedia data. A Watermark system consists of key (public key and private key). The use of key provides security i.e. prevents unauthorized use of data.[3]

2. Visible Watermarking
Visible Watermarking is a process by which we embed data into digital and analog content in order to identify its owner. And then watermark becomes a permanent part of the content, even it is distributed to others. These are similar to watermarks used on paper. Visible watermark change the signal such that it is different from the actual signal. Watermark act as a seal which is placed on an image to provide copyright protection. For e.g. if a photography company shares its photographs on internet and wants copyright protection for its data then they can add a watermark to their data so that no other person can use it with a watermark on it without their permission. Visible watermark is also used to indicate ownership originals to monitor and track how his image is being use.[7]

3. Types of Watermark

3.1 Visible Watermarking
It is visible semi-transparent text or image overlapped on the original image. In this we are able to look at the original image but it also provide copyright protection. These watermarks are more robust against transformation of image. Thus they are preferred for strong copyright protection digital form.[7]
3.2 Invisible watermark
It is invisible text or image overlapped on original image. In this we cannot see the image. Only electronic devices can extract the hidden information to identify the copyright owner. Invisible watermarks are used to provide authentication.[7]

3.2.1 Robust
In this case, watermark is embedded in such a way that if any changes are done to the pixel value in the image then it will be unnoticeable and can on it be recovered using decoding mechanism [7]

3.2.2 Fragile
In this case, watermark is embedded in such a way that if any changes are done in the watermarked image then the image would either alter or will destroy the watermark.[7]

Figure 1: Types of Watermark

4. Characteristics of Watermark
There are three characteristics of watermarking. If we will increase any one feature then others get decreased. So we should apply it according to our needs
4.1 Maximal Capacity
This is a watermarking technique in which the size of watermark to be applied should be such that it should not degrade the quality of the image.[4][7]

4.2 Robustness
This is a watermarking technique in which watermarked image should stand against image compression, noise and cropping effects. [4][7]

4.3 Imperceptibility
Human eye should not be able to make any difference between the original image and the image to which watermark has been applied.[4][7]

4.4 Security
Our watermark should be able to provide security against unauthorized access to the watermark.[4][7].

5. Wavelet Transformation
Wavelet transformations are used to solve difficult problems of physics, computers, and mathematics. It provides various applications like compression, image processing, signal processing, etc. It allows difficult problems to be decomposed into elementary form and then reconstructed with high precision.[6][7]

6. Haar Transform
Haar transformation performs average and differentiation functions for deleting data, sorting coefficients, reconstructing the matrix such that final matrix is similar to initial matrix.[7]

7. Modified Fast Haar Wavelet Transform
MFHWT is used for 1D approach. It is faster than fast Haar transformation (FHT). By applying this method we get improved values of approximation and coefficients that fast haar transformation (FHT) and Haar transformation (HT) because in MFHWT we need to store half of the original data and hence memory used in this case is also less.[1]

II. PROPOSED SCHEME

In this paper, to overcome the limitations of DWT with modified Haar wavelet transform and wavelet packet transform we will design an algorithm which is robust enough that it can withstand different transmission parameters e.g. Compression filters, Reform attack .

STEP 1: Take an image
STEP 2: Apply multi wavelet packets.
STEP 3: Input text into decomposed sub bands.
STEP 4: Inverse of transformation.
STEP 5: Obtain image
III. EXPERIMENTAL RESULTS

Figure 2: GUI Interface for Visible Watermarking

Figure 3: Watermark applies to the top left of original image
Figure 4: Watermark applied at the Right top of the original Image

Figure 5: Watermark applied at the Center of original Image
IV. RESULTS AND CALCULATIONS

After the experiments performed on registered Images in MATLAB, we have realized that above factors determine the quality of watermarked image. Our technique is better than those of other techniques of digital watermarking, because this technique provides high quality of information. The quality of image is measured by PSNR.

<table>
<thead>
<tr>
<th>Position of Watermark</th>
<th>Left Top</th>
<th>Right Top</th>
<th>Left Bottom</th>
<th>Right Bottom</th>
<th>Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watermark Images</td>
<td><img src="image1" alt="Image" /></td>
<td><img src="image2" alt="Image" /></td>
<td><img src="image3" alt="Image" /></td>
<td><img src="image4" alt="Image" /></td>
<td><img src="image5" alt="Image" /></td>
</tr>
<tr>
<td>PSNR Values</td>
<td>47.2473</td>
<td>45.2146</td>
<td>45.8974</td>
<td>45.31</td>
<td>46.2579</td>
</tr>
</tbody>
</table>

Table 1: Visible Image Watermarking

<table>
<thead>
<tr>
<th>Text Watermark Images</th>
<th><img src="image6" alt="Image" /></th>
</tr>
</thead>
<tbody>
<tr>
<td>PSNR Values</td>
<td>26.3609</td>
</tr>
</tbody>
</table>

Table 2: Text Watermarking

V. CONCLUSION

A number of techniques have been proposed for watermarking; however our proposed technique is better than other techniques as this technique provide better quality of image after applying watermark on the original image.
VI. REFERENCES


