Edge Based Reliable Digital Watermarking Scheme for Authorized Ownership

Dr. Marlapalli Krishna1, V Devi Satya Sri2, Bandlamudi S B P Rani3, G. Satyanarayana4

1 Department of CSE, Sir C R Reddy College of Engg, Eluru-534007, India
marlapallikrishna@gmail.com, 2vdevisatyasri@gmail.com, 3bsbprani.425@gmail.com, 4snarayana.5813@gmail.com

Abstract—Images coin dominant of multimedia content. Advances in technology created threat to copy write protection and authorized ownership. For instance images can be modified, copied and distributed easily. In order to overcome these issues, digital Image watermarking is potentially good tool and it’s a process that can employ for authenticity verification or for the copyright protection of digital data. In this paper a new digital image watermarking technique is proposed based on the edge detection in order to balance between the invisibility and robustness and also improve the ability of opposing to geometric attacks of the digital image watermark. We used a well-known quality measure functions for images, such as PSNR (peak-signal-to-noise-ratio) and Jaccard function for finding the quality of the extracted watermark image and efficiency of algorithm. The results show the watermark has good invisibility of inserted watermark image, as well as less distortions of the extracted image with robustness to resisting geometric attacks.

Keywords—Multimedia, Watermarking, Digital Image, Edge detection, geometric attacks.

1. INTRODUCTION

Present-day. Sharing of Images becomes very fast and simple, the increase amount of digitized content due to technological advancement, e.g. digital photographs, electronic books, Video on Demand, downloadable music. The advances in computer networking technologies created new channels for content distribution in huge quantity and quick manner. The sophistication of software functionalities enables end user to manipulate digital contents easily. So many effective tools are existed in Image processing[1]. So, protection and security of images becomes necessary. Digital Image Watermarking[2] is one of such effective tool, to take care of protection of confidential or personal Images. The digital image watermarking is a method in which we can insert the data or image within another image so that there will not be any noticed visible variation in the original host image. Digital Image watermarking can be defined as invisible and visible[14]. To save the visual appearance of images, we point on invisible watermarks there is a concurrence between watermarking, information hidings, steganography. Information hiding involves the secretion of information so that an observer does not know of its existence. Steganography generally means “covered writing” in which communication is carried out in secret. Watermark is the enclosure of content-dependent information. A hierarchical method can be made to relate these fields i.e. information hiding covers the steganography and watermarking. Invisible digital image watermarks are more secure than visible image watermarks. According to image processing at specific applications, the image watermarking techniques are generally grouped into three types: semi fragile, fragile and robust approaches Semi fragile watermarks are good at content authentication because they can differentiate minor image enhancements from major manipulations. While fragile image watermarking are designed and adopted to discover any illegal alteration. Robust Image watermarking is well used to copyright protection to assert rightful ownership because they stay intact with the image under various manipulations. In this paper, we concentration on the robust image watermarking scheme to attain our goal.

Technology point a view, Digital Image watermarking to be categorized mainly into two ways: spatial and transform domain watermarking. In the spatial domain, differential PCM is used to detect the edge regions of the image so that data can be hidden on those pixels of the image when the differential signal is larger than a certain threshold level. The method is based on the visual masking phenomenon at large intensity transitions in the neighborhood of the pixel. In the frequency domain, DCT coefficients with significant variance are chosen and modulated using the private key sequence. Both spatial and DCT schemes are evaluated in terms of the peak signal-to-noise ratio (PSNR)[6]. This type of approaches has the benefits of easy implementation and low complexity but suffers frail battle in contradiction of malicious attacks. Cross-domain transformation requires an extra computation. For this method. Transform domain methods are widespread because of their ability to abusing human visual perception and signal characteristics in digital image watermarking

2. LITERATURE SURVEY
2.1 Invisible watermarking

Invisible watermarking (LSB) [3][9][24] A variety of invisible watermarking schemes have been reported in the recent years. A few are being discussed here. The watermark is capable of carrying such information as authentication or authorisation codes, or a legend essential for image interpretation protection, and controlled access. Several methods of implementation are proposed among those two are discussed. The first is based on bit plane manipulation of the LSB [30], it specifies easy and rapid decoding. The another one uses linear addition of the water mark to the image data, and also more difficult to decode, offering inherent security. This linearity property also allows some image processing, such as averaging, to take place on the image, without corrupting the water mark beyond recovery. Either method is potentially compatible with JPEG Joint Photographic Experts Group and MPEG Moving Picture Experts Group processing [14].

2.2 Edge detection

In the watermarking schemes, Just Noticeable Distortion (JND) model provides an efficient method to keep the balance between watermark’s imperceptibility and robustness. Traditional JND (Just Noticeable Distortion) models are not as perfect as they should be. Edge detection, which extracts content features well, improves the performance of JND models. In this paper we explore the reasons and simulate JND models based on edge detection either in spatial domain or in DCT domain. The experiment results show that JND models based on edge detection in DCT domain have better performance than those in spatial domain.

3. EXISTING METHOD

The current systems use just watermarking and steganographic techniques which are prone to several attacks like Scrambling Attacks, Pathological Distortions, Copy Attacks and Ambiguity Attacks. A scrambling attack is a system-level attack in which the samples of a Work are scrambled prior to presentation to a watermark detector and then subsequently descrambled. A copy attack occurs when an adversary copies a watermark from one Work to another. As such, it is a form of unauthorized embedding. The copy attack attempts to the effectiveness of such systems by estimating the watermark given in an originally watermarked piece of media, and then adding that watermark to an un-watermarked piece. Ambiguity attacks create the appearance that a watermark has been embedded in a work when in fact no such embedding has taken place. An adversary can use this attack to claim ownership of a distributed work. He or she may even be able to make an ownership claim on the original work. As such, ambiguity attacks can be considered a form of unauthorized embedding. However, they are usually considered system attacks. To get rid of these attacks we propose a new watermarking techniques which can withstand against such attacks. Edge based reliable digital watermarking scheme for authorized ownership.

3.1 Existing Algorithm & Results

3.1a. Encryption Algorithm

1. Read Image from Face book through R tool named as Original.
2. Read another image and named as logo.
3. Convert every images pixel into binary format.
4. for each pixel in image m do
5. Mask last two bits of image pixel in steg;
6. Hide first two bits of the image pixel;
7. Go to next pixel in the image;
8. Now convert the binary values of the resulting image to decimal.
9. After decimal conversion result could be in column matrix and so it has to be converted to the size of the image Original.
10. Convert the matrix into Image. The Stego-image is obtained.

Note: This algorithm stores the logo image into the last bit of the Face book image along the Column pixels.

3.2 Decryption Algorithm

1. Read the Stego-Image and named as Original.
2. Convert Original image into a matrix form and each pixel into binary values.
3. Read last two bits of image pixel column wise, and append these bits depending on the depth of the logo image to form pixels of the logo image.
4. Convert these binary values into Decimal values.

5. Convert the column matrix into the size of the logo image.

Note: Step 5 can be done successfully only by the prior knowledge of the size of the logo image.

The brief comparisons between the existing method and proposed methods are tabulated as follows. Table-1

<table>
<thead>
<tr>
<th>Description</th>
<th>LSB Method</th>
<th>Proposed Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method type</td>
<td>Non-blind</td>
<td>Non-blind</td>
</tr>
<tr>
<td>Size of Original Image</td>
<td>Variable</td>
<td>Variable</td>
</tr>
<tr>
<td>Size of logo or watermark image</td>
<td>Variable</td>
<td>Variable</td>
</tr>
<tr>
<td>Embedded method</td>
<td>LSB</td>
<td>Edge positions</td>
</tr>
<tr>
<td>False positive error</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Scaling factor</td>
<td>Single</td>
<td>Multiple</td>
</tr>
</tbody>
</table>

Table-1: comparisons between the existing method and proposed methods

4. PROPOSED METHOD

The proposed watermarking algorithm mainly contains three levels: decomposing original image, embedding and extraction processes. In, embedding process, we are using binary watermark image approach[12][9]. Compare to existing techniques, this approach is very easier and also difficult to guess the key to extracting the logo images from the encrypted images.

4.1 Process of Watermark embedding:

1. Read a color Image and named as Original.
2. Read the logo image and named as logo.
3. Identify the edge positions in Original image.
4. Convert each image into 2-dimensional matrix.
5. Convert logo image pixels and Edge position pixels of Original image into binary format.
6. Split each pixel binary value into four parts with each of 2-bits and now take the 2 bit of a pixel from logo and store it in the two LSB bits of Original image edges byte. Repeat it to 8 bits of logo image pixel in four edge pixels of Original image.
7. Now convert the binary values of the resulting image (Embedded) to decimal.
8. After decimal conversion result could be in column matrix and so it has to be converted to the size of the Image Original.
9. Convert the matrix into Image. The embedded image is obtained.

Note: This algorithm stores the logo image into the last 2-bits of the edge pixels of Original Image.

The process of placing logo image into Original Image is shown in figure-1.
Fig-1. The process of placing logo image into Original Image

Extraction of the watermark logo image from the inserted image, we required the original host image. The extraction method is performed as shown in figure-2.

Fig-2. The process of extraction method

5. RESULTS AND DISCUSSIONS

We analyze the performance of the edge based watermarking technique with robustness and invisibility. To compare the equality of watermark embedded image with original image and extracted watermark logo image with original logo image using PSNR, Jaccard and Normalized cross correlation.

PSNR is one of the image qualities metric. Here we use the PSNR to measure the robustness of a watermark and invisibility of a watermark is measured as the detection rate of the watermark, which is measured as the ratio between the number of correctly matched local regions of watermarked image and number of original reasons of watermarked image. The PSNR value can be determined as:

\[
PSNR = 10 \cdot \log_{10} \left( \frac{MAX^2}{MSE} \right) = 20 \cdot \log_{10} \left( \frac{MAX^2}{\sqrt{MSE}} \right)
\]

Where MAX, is the maximum gray levels of the image and MSE is the root mean square error.

\[
MSE = \frac{1}{N \times M} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [X(i,j) - Y(i,j)]^2
\]

Where \( X(i,j) \) is the logo image and \( Y(i,j) \) is the embedded image.

When dealing with data objects that have binary attributes, it is more effective to calculate similarity using a Jaccard Coefficient.

The equation to find the Jaccard Coefficient is as follows:

\[
jacc(x, y) = \frac{|x \cap y|}{|x| + |y| - |x \cap y|}
\]

5.1 Result of Existing Method

The Fig. shows that, three original images are watermarked with a logo images and also the resultant Steg-image.
The result also shows that the resultant of the extracted image from the steg-image. The Encrypted and Decrypted Output Images of Existing Method are shown in figure-3 and The detailed comparisons of the Three Images with Jaccard and PSNR values are as shown in Table-2

<table>
<thead>
<tr>
<th>IMAGE</th>
<th>JACCARD</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image1</td>
<td>20.687763</td>
<td>72.91945</td>
</tr>
<tr>
<td>Image2</td>
<td>7.499785</td>
<td>43.3096</td>
</tr>
<tr>
<td>Image3</td>
<td>17.551466</td>
<td>72.58854</td>
</tr>
</tbody>
</table>

Table-2: The Jaccard and PSNR values of the Existing System

5.2 Results of the proposed work
In this proposed work, we taken three Face book profile pictures named image1, image2 and image3 of a person are extracted from Face book and used in this proposed work. The size of the original images is variable image1 is with dimensions 600 X 600, Image2 is with the dimensions of 800 X 600, Image3 is with dimensions of 437 X 600. A logo image of size 87 X 85 is used as a watermark image. The original and watermark logo images are

Original and logo watermark images and its dimensions:
Image1 (a) image2 (b) image3 (c) and logo image (d)
The Figure1 discuss the process of inserting of logo watermark image into original image and also the results Comparisons.

*Original*  *Edge*  *Logo Embedded*  *Graph*

Embedded Process of a Watermark Logo Image into three Face book Profile Pictures

The PSNR and Jaccard values of embedded images are listed in Table-3.

<table>
<thead>
<tr>
<th>S.NO</th>
<th>Jaccard</th>
<th>PSNR</th>
<th>Jaccard</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image1</td>
<td>0.431111</td>
<td>0.524403</td>
<td>0.2257</td>
<td>0.34403</td>
</tr>
<tr>
<td>Image2</td>
<td>0.59367</td>
<td>0.699542</td>
<td>0.362670</td>
<td>0.62138</td>
</tr>
<tr>
<td>Image3</td>
<td>0.99457</td>
<td>0.603675</td>
<td>0.4335</td>
<td>0.4281</td>
</tr>
</tbody>
</table>

Table-3: Jaccard and PSNR values of three Face book Images with Existing and proposed methods.

To prove the robustness of the proposed method, we examined the effect of the following attacks on digital Watermarked images:

a. Cropping image (up to 30)
b. Rotation of image (with rotation angle = 100).
c. Sharpening image (Sharpen 95)
d. JPEG compression (quality factor= 85)
e. Median blur (blur 5)

The results of extracted watermark image after different types of image processing attacks. In the extraction method, each attack has been verified with each previously labeled watermarked image as well as the extraction results for the watermark binary images, after cropping, rotation, sharpening, JPEG compression and median blur attacks. The extracted images from the embedded images are partially degraded after cropping, JPEG compression, median blur, rotation and sharpening attacks. Still, the extracted watermark images persist recognizable because these attacks change the indexed reference values, which may available the watermark location values of the embedded values. Thus, during extraction of watermark image, extracted values may not be the watermark values of the indexed position values, which have been altered. This outcome can also be observed in Table-4.

<table>
<thead>
<tr>
<th>Method</th>
<th>Original Image</th>
<th>Watermarked</th>
<th>Jaccard</th>
<th>PSNR</th>
<th>Jaccard</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crop= 30%</td>
<td>0.481522</td>
<td>33.1202</td>
<td>0.958168</td>
<td>30.045</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rotate</td>
<td>0.652201</td>
<td>6.2512</td>
<td>0.705421</td>
<td>30.0753</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
False positive error checking:
The proposed approach is tested different false ownership claims and each time the scheme is able to find the claims.
False positive error takes place when a wrong watermark is extracted from the embedded image. The following image is the extracted watermark image without referring the source image using embedded image. We can observe that the extracted watermark logo image become some noise, if we can change the source image by wrong image. So, this is the proof that the approach is secured towards false positive error.

Fig: Extracted watermark logo from the embedded image when the original image not provided

6. CONCLUSIONS AND FUTURE SCOPE
The result set as shown in the tables, clearly depicts and reaches the quality of the resultant embedded watermarked image with high invisibility and also robustness. Our major contribution is that we have proposed a robust watermarking scheme that uses edge features. In order to resist geometric distortions, we also conducted different tests involving various common image processing attacks such as Cropping, rotation, sharpening, JPEG compression and Motion blur against the Watermark. The watermark images were extracted in all tests successfully, but in some attacks the quality may be various. Because of the principal components insertion this scheme is also free from the false positive errors. Drawbacks of the proposed watermarking scheme are related to its vulnerability to large distortion of the aspect ratio. Future work will focus on eliminating those drawbacks. In future this work can also be extended for inserting edge based watermark on videos. A Video is a sequence of images, called as frames, and these frames are more or less same with slight changes and thus position of edges may not vary considerably in adjacent edges.

7. REFERENCES