Robust Watermarking of Color Images using RST Invariant Features

Renu Sharma1 Sachin Sharma2
1M.Tech Scholar
1Department of Computer Engineering
1Galgotias University, Greater Noida, India. 2RIET, Jaipur, Rajasthan,India

Abstract— Watermark refers to digital data embedded in cover data with an intent of copyright protection or proof of ownership. In case of image watermarking, the robustness of watermarks to geometric attacks is considered to be the most challenging design requirements for watermarks. Geometric attacks like Rotation, Scaling and Translation (RST attacks) can desynchronize the location of the watermark and hence cause incorrect watermark detection. In this paper, a new color image watermarking scheme for copyright protection is proposed. This scheme utilizes the features of the image which are invariant under rotation, scaling and translation of images. Moments and functions of moments have been extensively employed as invariant global features of images in pattern recognition. The proposed work utilizes Hu's invariant moments for watermark generation. The same can be detected and extracted at the detector to serve for copyright protection. The moments are invariant against image rotation, scaling and translation. Thus, the proposed watermarking scheme is robust against RST attack. Original unmarked image is not required at the detector for watermark detection and extraction. Thus, the proposed scheme provides a way for blind watermarking. The simulation is done using MATLAB and results are compared with existing techniques of invariant feature based watermarking schemes. Comparison of the results are presented which shows a considerable improvement in Peak Signal to Noise Ratio.

Key words: Watermarking, RST invariant features, PSNR

I. INTRODUCTION

Digital watermark [1] is a kind of technology that embeds copyright information into multimedia data. Unlike encryption, which is useful for transmission but does not provide a way to examine the original data in its protected form, the watermark is supposed to be present in the content in its original form and is not perceptible when a user listening to, view, examine, or manipulate the content. Digital watermarking technology opens a new door to authors, producers, publishers, and service providers for protecting their rights and interests in multimedia documents. An effective image watermarking scheme mainly includes all the three steps, viz, watermark generation, embedding and identification, and watermark attack [2]. Watermark generation refers to what content and form of data a watermarking scheme adopts as watermark. The data may be original or encrypted from copyright information of number, letter, image, and so on. The copyright information to be used as watermark may be meaningful or meaningless. Meaningful information could be easily authenticated and usually needs to be encrypted in practice to strengthen watermarking security. Watermark embedding is the most important part in a watermarking scheme and must meet the two most fundamental requirements under the condition of fixed watermark size, imperceptibility and robustness [3]. The two requirements are in conflict with each other and need to reach a trade-off. Watermark embedding can be done in either spatial domain [4] or frequency domain [5]. The spatial domain watermark embedding manipulates host image pixels, especially on Least Significant Bits (LSB) [6] that have less perceptual effect on the image. Although the spatial domain watermark embedding is simple and easy to implement, it is fragile as compared to frequency domain watermark embedding due to various attacks and noise, which is made on the frequency coefficients of the host image. The existing frequency transformation methods for watermark embedding include Discrete Fourier Transform (DFT) [7], Discrete Cosine Transform (DCT) [8], and Discrete Wavelet Transform (DWT) [9]. Considering watermarking imperceptibility, one needs to select an appropriate embedding algorithm to embed the watermarking bits into certain frequency coefficients so that the quality of watermarked image will not be degraded compared by original host image. Many traditional embedding algorithms in the literature do not optimize the embedding process by experiential method. In recent years, watermarking techniques have been improved using optimization algorithms such as Genetic Algorithm (GA) [10] which is a popular evolutionary optimization technique invented by Holland [11]. In the field of watermarking, GA is mainly used in the embedding procedure to search for locations to embed the watermark. The act of watermark detection can be named as watermark verification in which a watermarking receiver must do a yes or no judgment whether a watermark does exist in the received image. In general, the Normalized Cross-Correlation (NCC) value between the original and extracted watermark is used in watermark detection. Defined a threshold T, a yes judgment can be given if NC ≥ T, or a contrary result will be given. After getting a yes judgment in watermark detection, especially to the meaningful watermark, people may do more things to judge the owner of extracted watermark because of possibility of spurious watermark. Based on the watermark detection, watermark identification is to further judge as to what degree extracted watermark is similar to original watermark and whose extracted watermark belongs to. Although Bit Correct Rate (BCR), NCC and human eyes can be used in watermark identification, they all depend upon experimental results and human experiences. For distinguishing extracted watermark more clearly, meaningful watermark may be recovered partly or entirely from watermarked image by Neural Networks [12]. The introduction of neural networks helps to pave the way for the further development of watermark identification techniques. The goal of watermark attack is to test the robustness of a watermarking system. To simulate the communication conditions and deliberate or unintentional processing, some attacks, including adding noise, filtering, compression and geometrical distortion,
need to be used in the watermarked image. For copyright protection, robust watermarking is required so that the watermark can partially be recognized and the copyright can be preserved after attacked by some means. But based on the applied purpose of robust watermark, a watermarking scheme need not withstand all kinds of attack. This dissertation presents a watermarking scheme based on image invariants so that the watermarked image is resistant to rotational, scaling and translational attack. The watermarking data comes from a meaningful binary image encrypted by two-dimensional bit stream. In the procedure of watermark embedding, linear mapping function is used to map the image regions for subsequent image portion identification. After some kinds of attack, the extracted watermark can be identified expeditiously through the detection process. The experimental results have shown that this scheme has preferable performance of security, imperceptibility and robustness.

A. Desirable Characteristics of Watermark

An effective watermarking scheme should have the following desirable features:

1. To be able to determine whether an image has been altered or not.
2. To be able to locate any alteration made on the image.
3. To be able to integrate authentication data with host image rather than as a separate data file.
4. The embedded authentication data be invisible under normal viewing conditions.

To allow the watermarked image be stored in lossy compression format [13].

B. Motivation

The sudden increase in watermarking interest is most likely due to the increase in concern over copyright protection of content. The Internet had become user friendly with the introduction of Marc Andreessen’s Mosaic web browser in November 1993 [14], and it quickly became clear that people wanted to download pictures, music, and videos. The Internet, however, is one of the most excellent distribution system for digital media because it is inexpensive, eliminates warehousing and stock, and delivery is almost instantaneous. However, content owners (especially large Hollywood studios and music labels) also see a high risk of piracy. This risk of piracy is exacerbated by the proliferation of high capacity digital recording devices. When the only way the average customer who wants to keep a sound track could record a song or a movie was on analog tape, pirated copies were usually of a lower quality than the originals, and the quality of second-generation pirated copies (i.e., copies of a copy) was generally very poor. However, with digital recording devices, songs and movies can be recorded with little, if any, degradation in quality. Using these recording devices and using the Internet for distribution, would-be pirates can easily record and distribute copyright protected material without appropriate compensation being paid to the actual copyright owners. Thus, content owners are eagerly seeking technologies that promise to protect their rights. The first technology content owners turn to is cryptography. Cryptography [15] is probably the most common method of protecting digital content. It is certainly one of the best developed as a science. The content is encrypted prior to the delivery to the host or customer, and a decryption key is provided only to those who have purchased legitimate copies of the content. The encrypted file can then be made available via the Internet, but would be useless to a pirate without an appropriate key. Unfortunately, encryption cannot help the seller monitor how a legitimate customer handles the content after decryption. A pirate can actually purchase the product, use the decryption key to obtain an unprotected copy of the content, and then proceed to distribute illegal copies. In other words, cryptography can protect content in transit, but once decrypted, the content has no further protection. Thus, there is a strong need for an alternative or complement to cryptography: a technology that can protect content even after it is decrypted. Watermarking has the potential to fulfill this need because it places information within the content where it is never removed during normal usage. Decryption, re-encryption, compression, digital-to-analog conversion, and file format changes a watermark can be designed to survive all of these processes. Watermarking has been considered for many copy prevention and copyright protection applications. In copy prevention, the watermark maybe used to inform software or hardware devices that copying should be restricted. In copyright protection applications, the watermark may be used to identify the copyright holder and ensure proper payment of royalties. Although copy prevention and copyright protection have been major driving forces behind research in the watermarking field, there is a number of other applications for which watermarking has been used or suggested. These include broadcast monitoring, transaction tracking, authentication, copy control, and device control.

C. Problem statement

The robustness of watermarks to geometric attacks is considered to be the most challenging design requirements for watermarks. Geometric attacks can desynchronize the location of the watermark and hence cause incorrect watermark detection. In this paper, a new color image watermarking scheme for copyright protection is proposed, based on moments or values which remains invariant under rotation, scaling and translation. Based on these moments, other moments are derived corresponding to different image segments and the set of these transforms are combined to generate the binary watermark. At the detector end, the same watermark is extracted to provide a proof of copyright protection.

D. Research approach

The original image is analyzed to compute Hu's invariant moments. These moments are numeric and 7 in number. Using these seven moments, seven image locations are mapped possibly covering the entire image and Hu's moments are derived. These seven moments, along with the base moments derived for the entire image are used for the purpose of watermark generation. The same procedure is repeated at the detector end to detect the presence of watermark to enable copyright protection.
II. PROPOSED WORK

A. Image Transformations

Consider the image shown in Fig 1.1.

Fig. 1.1: Image A : Lena.jpg [Dimension 400 X 400, actual]

The padding of the image with pixels on all sides can be done using the following MATLAB code:

\[
I = \text{imread('lena.jpg')};
Ip = \text{padarray}(I, [84, 84], 'both');
\text{imtool}(Ip)
\]

Fig. 1.2: Image B : Lena_padded.jpg [Dimension 568 X 568, actual]

The translated image at distance 150 pixels along X and Y axis can be obtained through the following MATLAB code:

\[
I = \text{imread('lena.jpg')};
Ftrans = \text{zeros}(568,568,'uint8')
Ftrans(151:550,151:550) = I;
\text{imshow(Ftrans)}
\]

Fig. 1.3: Image C : Lena_translated.jpg [Dimension 550 X 550, actual]

The mirrored image can be obtained using the following MATLAB code:

\[
I = \text{imread('lena.jpg')};
\text{imgMirror} = \text{flipdim}(I,2);
\text{imtool(imgMirror)}
\]

Fig. 1.4: Image D : Lena_mirrored.jpg [Dimension 400 X 400, actual]

The rotated image can be obtained using the following MATLAB code:

\[
F = \text{imread('lena.jpg')};
f45 = \text{imrotate}(F, 45, 'bilinear');
\text{imtool(f45)}
\]

Fig. 1.5: Image E : Lena_rotated.jpg [45° Rotation, Dimension 569 X 569, actual]
B. Image Invariant Features

For any image, one can obtain the features which can remain invariant under the operations depicted by Fig 3.1 to 3.5. One can obtain the moment invariants using function \texttt{invmoments} using the code as shown below:

```matlab
f1 = imread('lena.jpg');
f2 = imread('lena_padded.jpg');
f3 = imread('lena_translated.jpg');
f4 = imread('lena_mirrorred.jpg');
phi = invmoments(rgb2gray(f1));
disp(phi);
phi = invmoments(rgb2gray(f2));
disp(phi);
phi = invmoments(rgb2gray(f3));
disp(phi);
phi = invmoments(rgb2gray(f4));
disp(phi);
The output of the above code is illustrated in tabular form as shown:

<table>
<thead>
<tr>
<th>Feature values</th>
<th>Lena.jpg</th>
<th>Lena_padded.jpg</th>
<th>Lena_translated.jpg</th>
<th>Lena_mirrorred.jpg</th>
<th>Lena_rotate_d.jpg</th>
</tr>
</thead>
<tbody>
<tr>
<td>X1</td>
<td>1.7340e+03</td>
<td>1.7344e-03</td>
<td>1.7344e-03</td>
<td>1.7344e-03</td>
<td>1.7344e-03</td>
</tr>
<tr>
<td>X2</td>
<td>1.5508e-08</td>
<td>1.5508e-08</td>
<td>1.5508e-08</td>
<td>1.5508e-08</td>
<td>1.5508e-08</td>
</tr>
<tr>
<td>X7</td>
<td>-1.4756e-21</td>
<td>-1.4756e-21</td>
<td>-1.4756e-21</td>
<td>-1.4756e-21</td>
<td>-1.4756e-21</td>
</tr>
</tbody>
</table>

Table 1.1: Invariant Feature Extraction For The Geometrically Operated Images

It is clearly evident from the above features that that these remains invariant under image rotation, scaling and translation.

C. Analysis of Hu's Invariants

The circularly cropped \texttt{lena.jpg} can be obtained from the following MATLAB code:

```matlab
I = imread('lena.jpg');
imageSize = size(I);
width = size(I, 1);
height = size(I, 2);
r1 = width/2;
r2 = height/2;
if r1<r2
    r=r1;
else
    r=r2;
end
ci = [r2, r1, r];
[xx,yy] = ndgrid((1:imageSize(1))-ci(1),(1:imageSize(2))-ci(2));
mask = uint8((xx.^2 + yy.^2)<ci(3)^2);
croppedImage = uint8(zeros(size(I)));
croppedImage(:,:,1) = I(:,:,1).*mask;
croppedImage(:,:,2) = I(:,:,2).*mask;
croppedImage(:,:,3) = I(:,:,3).*mask;
imshow(croppedImage);
```

The circularly rotated image can be obtained by the following code:

```matlab
B = imrotate(croppedImage, 90);
imshow(croppedImage);
```

The phi moments of both images 3.6 and 3.7 are

<table>
<thead>
<tr>
<th>Feature values</th>
<th>Lena_circular_cropped.jpg</th>
<th>Lena_circular_cropped_rotated_90.jpg</th>
</tr>
</thead>
<tbody>
<tr>
<td>X1</td>
<td>1.6513e-03</td>
<td>1.6513e-03</td>
</tr>
<tr>
<td>X2</td>
<td>1.5428e-08</td>
<td>1.5428e-08</td>
</tr>
<tr>
<td>X3</td>
<td>2.5704e-11</td>
<td>2.5704e-11</td>
</tr>
<tr>
<td>X4</td>
<td>3.8857e-11</td>
<td>3.8857e-11</td>
</tr>
<tr>
<td>X5</td>
<td>-1.2165e-21</td>
<td>-1.2165e-21</td>
</tr>
<tr>
<td>X6</td>
<td>-2.6365e-15</td>
<td>-2.6365e-15</td>
</tr>
<tr>
<td>X7</td>
<td>1.6780e-22</td>
<td>1.6780e-22</td>
</tr>
</tbody>
</table>

Table 1.2: Invariant Feature Extraction For The Circularly Cropped Images

It is evident from the above example that Hu's moments are invariant against RST attack but are variant against cropping attacks.
D. Watermark Embedding
The proposed watermarking embedding algorithm works as follows:

- **Input Cover Image (Colored)**
- **Maximum Circular Cropping of Image**
- **Obtaining biggest image segment of circular image which is inscribed in the circle**
- **Obtaining the Hu's Invariant Moments**
- **EMBED WATERMARK using Hu's Moments**

Fig. 1.8: proposed watermarking scheme
For Rotated and Scaled versions of the image, the center of the image remains the same. For translated version of the image, suitable processing needs to be done to find out the centre of the image. It is assumed in the current work that x and y coordinates are translated by the same proportion.

Suppose $H_1$, $H_2$, $H_3$, $H_4$, $H_5$, $H_6$, and $H_7$ represents the seven Hu's invariant moments corresponding to the image segment which is inscribed in the circular section.

Each of the values $H_i$ is mapped to a point in the region of the image outside the circular portion. The moments of these regions again gives 7 moments each thereby providing a total of 49 invariant values of the image. The following section illustrates the mapping scheme:

<table>
<thead>
<tr>
<th>Hu's Moments (Absolute Values)</th>
<th>Values on a log 10 scale</th>
<th>Absolute values rounded to the nearest integer</th>
<th>Linear mapping to a scale [0,1) with rounding</th>
<th>Binary values corresponding to moments</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H_1$</td>
<td>1100</td>
<td>1101</td>
<td>0111</td>
<td>01110</td>
</tr>
<tr>
<td>$H_2$</td>
<td>1100</td>
<td>1101</td>
<td>0111</td>
<td>01110</td>
</tr>
<tr>
<td>$H_3$</td>
<td>1000</td>
<td>1010</td>
<td>0111</td>
<td>01110</td>
</tr>
<tr>
<td>$H_4$</td>
<td>1000</td>
<td>1010</td>
<td>0111</td>
<td>01110</td>
</tr>
</tbody>
</table>

Table 1.3: Mapping Of Hu's Moments To 7 Points On The Image
Thus, we have the set of 7 coordinates with x and y values as specified by the last columns of table 3.1.

For each of these coordinates, the Hu's moments for circular image block of pre specified dimension are obtained. The absolute values corresponding to the moments is obtained in the same manner as shown in table 3.1. The XORRed values of the LSB's of the moments are used as watermark for the purpose watermark detection.

This process is illustrated as shown using the following example:

<table>
<thead>
<tr>
<th>Co-ordinates</th>
<th>(0, 0)</th>
<th>(105, 105)</th>
<th>(168, 168)</th>
<th>(147, 147)</th>
<th>(379, 379)</th>
<th>(253, 253)</th>
<th>(400, 400)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H_1$</td>
<td>27</td>
<td>22</td>
<td>26</td>
<td>29</td>
<td>25</td>
<td>27</td>
<td>30</td>
</tr>
<tr>
<td>$H_2$</td>
<td>28</td>
<td>17</td>
<td>16</td>
<td>30</td>
<td>24</td>
<td>25</td>
<td>20</td>
</tr>
<tr>
<td>$H_3$</td>
<td>16</td>
<td>21</td>
<td>18</td>
<td>16</td>
<td>22</td>
<td>18</td>
<td>21</td>
</tr>
<tr>
<td>$H_4$</td>
<td>17</td>
<td>25</td>
<td>20</td>
<td>23</td>
<td>23</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td>$H_5$</td>
<td>20</td>
<td>30</td>
<td>30</td>
<td>23</td>
<td>23</td>
<td>24</td>
<td>27</td>
</tr>
<tr>
<td>$H_6$</td>
<td>19</td>
<td>23</td>
<td>25</td>
<td>30</td>
<td>20</td>
<td>18</td>
<td>17</td>
</tr>
<tr>
<td>$H_7$</td>
<td>30</td>
<td>22</td>
<td>25</td>
<td>29</td>
<td>26</td>
<td>18</td>
<td>22</td>
</tr>
</tbody>
</table>

Table 1.4: Hu's Moments Corresponding To 7 Points On The Image, Covering All The Sections On The Image
Robust Watermarking of Color Images using RST Invariant Features

Table 1.5: Hu's Moments Corresponding To 7 Points, Represented As Binary Numbers

As XOR is a reversible operation with any of the input values, a corresponding match detects the presence of watermark with any of the 7 image segments that are obtained with the linear mapping of the Hu's moments of the rotated, scaled and translated image.

This process is illustrated in table 1.4 shown below:

<table>
<thead>
<tr>
<th>LSB of moments of image</th>
<th>LSB of Moments of (0,0)</th>
<th>XOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 1.6: Hu's Moments Corresponding To 7 Points, Represented As Binary Numbers

Following the same procedure as depicted in table 1.4, we get a set of 7 such XORed values to be used as watermark. These values, when XOR with any of the Hu's moments will provide the LSB corresponding to Hu's moment and consequently, detects the presence of watermark.

These 7 X 7 values constitute an array of binary numbers, the columns of which are XORed values of the Hu's moments with the moment of the overall image. This 7 X 7 block is the generated watermark and it is inserted redundantly into the non overlapping portions of the image in spacial domain using LSB encoding. Repeatedly embedding these 49 values row-wise in the pixels of the original images provides a way of robust watermarking. This process is illustrated as shown:

Fig. 1.9: Image sections to compute invariant moments

Each of the circle is centered on the points of the form \((a_n, a_n)\) where \(n\) are the normalized pixel values obtained through Hu's invariant moments. Watermark generation process utilizes these 49 invariants to generate a watermark image.

These 7 circular regions are operated again to obtain the Hu's invariants of the corresponding segments, thereby providing a complete set of Hu's moments so that these can be extracted again even after a significant cutting, cropping and rotational operations on the image.

The XORed values of the seven moments corresponding to the circular sections, with the invariants of the complete image are tabulated below. These values corresponds to the Boolean operations on LSB operations of the moment values.

<table>
<thead>
<tr>
<th>LSB of moments of image</th>
<th>LSB of Moments of (0,0)</th>
<th>XOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 1.7: Binary Matrix Corresponding To Xored Values

The generated watermark is

Fig. 10: Generated Watermark

This pattern corresponds to the invariant features extracted in the image. Partial pattern identical to any of the column of the given watermark proves the existence of the watermark in the given image.

E. Watermark Detection

The detection and/or extraction of the watermark is straightforward as per the embedding scheme. The rotated, scaled and possibly translated image is investigated for presence watermark by the extraction of Hu's moments. The other seven moments are also extracted based on the linear mapping function. The reconstruction of the watermark using Hu's moments will provide a confirmation of the presence of watermark.

III. RESULTS

A. PSNR values of watermarked image

The PSNR values tabulated for lena.jpg under different transformations are tabulated as shown below:

<table>
<thead>
<tr>
<th>Watermark Embedding Count</th>
<th>Rotated</th>
<th>Scaled</th>
<th>Translated</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS E</td>
<td>PSNR</td>
<td>MS E</td>
<td>PSNR</td>
</tr>
</tbody>
</table>
value to be embedded in the image so as to provide blind watermarking. It is evident from table 3.1 that Hu's invariant moments changes significantly under cropping operations. In view of the watermarking technique proposed by Ibrahim Alsonosi Nasir et. al [19], the contribution of present work is twofold. Firstly, it provides a robust watermarking of color images against Rotational, Scaling and Transitional attacks, with watermark extraction almost completely without any temperament. Secondly, it offers a method so that the watermark presence can be detected and watermark can be extracted with slight temperament even under cropping attack. Table 1.9 illustrates the feature modeling of both the schemes:

Table 9: Comparison Of Proposed Watermarking Scheme
The PSNR values also depends upon the selection of the embedding block of the cover image and better results can be obtained in the blocks with comparable pixel intensities. However the PSNR depends on how redundantly the watermark is embedded in spatial (pixel domain) of the host image.

A. Future Scope
Future scope of the work investigates the embedding of custom watermark in the image, while at the same time, preserving the robustness against RST attacks. Also, future work will focus on the scaling operations as utilized by most image editing programs so as to investigate the effect of the same while embedding the watermark data in LSB of the pixels of the host image. Moreover, better PSNR values can be achieved with Optimal Pixel Adjustment (OPA) algorithm, so it can be utilized for watermark embedding while at the same time, investigating the effect of scaling operation, more often performed through nearest-neighbor algorithm over the host image, on OPA technique while at the same time, investigating the effect of scaling operation, more often performed through nearest-neighbor algorithm over the host image, on OPA technique.

REFERENCES

Table 1.8: Psnr Values For Various Geometrical Attacks

Fig. 11: PSNR values of watermarked image under various attacks
It is clearly evident from the above figure that PSNR values depends on the redundancy of the embedding of watermark in the host image. More embedding leads to robust watermarking but consequently a low PSNR values thereby causing larger distortions in the watermarked image.

IV. CONCLUSION
The geometrical transformation invariant watermarking proposed by Ibrahim Alsonosi Nasir et. al [19] considers rotational and transformational normalization. However, image circular normalization requires some key feature


