Abstract: In this paper we consider a watermarking technique based on visual cryptography that offers enhancing the security issues in previous works. The proposed method is applied over color images, where the RGB image is converted to the HSV color scheme. The embedding process depends on the saturation plane (S) on which we apply logical X-OR, most significant, and parity operations; to generate the actual plane in which we want to embed our watermark — upon the rules of visual cryptography (as invented by Noar and Shamir, 1995). Finally the generated master share is registered in the third party. In the extraction process, applying the same method over the watermarked image will generate the master share again; combine it with that of the third party to generate the embedded watermark. Different attack scenarios are taken into consideration such as filtering, additive noise, compression, rotation, flipping, cropping, and distortion.

Keywords: Watermarking, Secret Sharing, Visual Cryptography, Parity bit.

1. Introduction

The rapid growth of multimedia content in digital form made the digital images easy to steal, modify, or used illegally by unauthorized people, this creates a pressing need for building more secure methods for legal distribution of the digital content. So, digital watermarking has been proposed to protect the integrity of multimedia.

An image watermark method is now drawing the need for good schemes to protect copyrights for digital data. But the chosen method must be hard to detect and remove. There are many articles reveal and proposes some watermark methods [2, 4, 9, 10], however there are several watermarking methods that are not robust or easy to remove [5]. In this paper we devise a watermarking method based on the visual cryptography that introduced by Naor and Shamir [1].

The paper is organized as follows: Visual Cryptography is discussed in Section 2. In section 3 the used measures are presented. Section 4 discusses the proposed algorithm. The experimental results are provided in Section 5. Finally, the conclusions are presented in Section 6.

2. Visual Cryptography

Cryptography that can be decoded directly by the human visual system without any special calculation for decryption is called Visual Cryptography. It was proposed for the first time by Naor and Shamir. In visual cryptography a secret message can be viewed as nothing more than a collection of black and white pixels as depicted on figure. 1. Each pixel in the original image is represented by at least one subpixel in each of the n generated shares.

Each share is comprised of collections of m black and white subpixels where each collection represents a particular original pixel [1, 2, 3]. R.J. Hwang proposed a watermark method based on visual cryptography, according to his method, the owner should select an h×n black/white image as the watermark. In the embedding processes, the owner should randomly select a number as his secret key S, to embed the watermark into the image K that is a k×l (256 gray-leveled) image. The owner embeds the watermark pattern W into the image K by generating the secret key S, and the verification information V. As illustrated in table 1, if the i\(^{th}\) pixel in the watermark Wi is zero and the left most significant bit (LMB) of the Ri\(^{th}\) pixel in image M is 1 then the verification information equals (0,1), and so on.

In the extraction process, the notarial organization retrieves the verification information V and the watermark pattern W, which the owner has registered, and verifies the ownership of the watermarked image K\(^{'}\), for more details see [2].

<table>
<thead>
<tr>
<th>W</th>
<th>M</th>
<th>LMB (R(i) th)</th>
<th>Assign (v1, v2) of V</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>(0,1)</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>(1,0)</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>(1,0)</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>(0,1)</td>
</tr>
</tbody>
</table>

Table 1. Verification Rules

On 2009, Surekha proposed a visual cryptography algorithm in image watermarking that offers better security than Hwang’s method, so that, attackers will not be able to detect ownership information [3]. Our proposed method offers an enhancement for Surekha’s algorithm.
3. Measures

To prove the effect of our method theoretically by measures, the following metrics are used to measure distortion and similarity between the original watermark and the extracted watermark:

1. **Root Mean Square Error (RMSE)**, as defined in equation 1.

\[
RMSE = \sqrt{\frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} (W_{ij} - W'_{ij})^2}
\]

where \( m \times n \) is the size of the watermark, \( W_{ij} \) is the watermark pixel in the \( i \)th row and \( j \)th column, and \( W'_{ij} \) is the \( W' \) in the \( i \)th row and \( j \)th column.

2. **Peak Signal to Noise Ratio (PSNR)**, as defined in equation 2.

\[
PSNR = 10 \times \log_{10} \frac{HE}{MSE}
\]

3. **Correlation (Corr)**, as defined in equation 3.

\[
\text{Corr} = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} (W_{ij} - \bar{W})(W'_{ij} - \bar{W}')}{\sqrt{\sum_{i=1}^{m} \sum_{j=1}^{n} (W_{ij} - \bar{W})^2 \sum_{i=1}^{m} \sum_{j=1}^{n} (W'_{ij} - \bar{W}')^2}}
\]

4. Proposed Algorithm

This section reveals the proposed method for watermark embedding and detection.

4.1 General Model

The general diagrams of our method are described in Figure 2 and Figure 3. Where Figure 2 shows the watermark embedding Model, in which we convert the host image from RGB color scheme to the HSV color scheme. Then we extract the S (saturation) from HSV image. After that we start the embedding process as illustrated in section 4.2, at the end we generate the Master share M, that is registered in a trusted third party.

Figure 3 shows the extraction Model, in which we start by reading the watermarked image \( I' \) and convert it to the HSV scheme, then we extract the saturation from the HSV image. Then we start the extracting process as discussed in section 4.3. Finally the secret image is extracted.

4.2 Watermark Embedding

As shown in Figure 5 the embedding process is as follows:

- Read the RGB image \( I \) of size \( r \times c \)
- Convert the image to the HSV scheme
- Extract the saturation plane (S) from the HSV image
- Read the black-white watermark image \( W \) of size \( w \times h \)
- Select a secret key \( K \) as a seed to generate \( w \times h \) random numbers over the interval \([1 \text{ to } r \times c]\). Let \( R_{ij} \) be the \( i \)th random number.
• Create a binary matrix MSB of size wxh, it contains the most significant bits of $R_i$ of the host image.
• Create a binary matrix P of size wxh that represents the parity for the first three bits of $R_i$ of the host image.
• Compute Y such that it finds the logical xor between P and MSB as in the following equation, $Y = P \oplus MSB$
• Create a binary matrix Z of size wxh such that the entries in the array are the most significant bits of the $R_i$ random number.

- Create a binary matrix Y of size wxh such that $F_i = \text{XOR}(Y_i, Z_i)$
- Generate the Master Share M by assigning a pair of bits for each element in the binary matrix F according to the encryption rules of VC. As discussed before in table 1.
- M is registered to the trusted third party.

Figure 5. Watermark embedding

Figure 6. Watermark extraction
4.3 Watermark Extraction
As shown in Figure 6 the extraction process is as follows:
- Read the watermarked image I’ of size rxc
- Convert I’ to HSV scheme
- Extract the saturation plane (S) from I’
- Read the black-white watermark image (W) of size wxh
- Use the secret key K as a seed to generate wxh random numbers over the interval [1 to rxc]. Let \( R_i \) be the \( i^{th} \) random number.
- Create a binary matrix MSB’ of size wxh, it contains the most significant bits of \( R_i \) pixel of the host image.
- Create a binary matrix P’ of size wxh that represents the parity for the first three bits of \( R_i \) pixel of the host image.
- Create a binary matrix Z’ of size wxh such that the entries in the array are the most significant bits of the \( R_i \) random number.
- Create a binary matrix F’ of size wxh such that \( F’ = \text{XOR}(Y’, Z’) \)
- Create the Verification Share such that, if the element in the binary matrix F’ is ‘0’ then \( V_i = (0, 1) \), else \( V_i = (1, 0) \)
- The secret image can be extracted by performing logical OR between the master share M and the Verification share V.

5. Experimental Results
The robustness of our approach is tested by applying several attacks over the “Peppers” image of size (512x512) and the binary watermark image of size (144 x 148). Figures 7,8 show the original peppers image and the binary watermark respectively.

![Figure 7. Peppers original image](image1)

![Figure 8. Binary watermark image](image2)

The robustness of the method is confirmed by experimental results that display the immunity of the embedded watermark over different types of attacks, such as compression, filtering, cropping, rotation, additive noise, and distortion. Table 2 shows the detailed results.

<table>
<thead>
<tr>
<th>Attack</th>
<th>Watermarked Image</th>
<th>RMSE</th>
<th>PSNR</th>
<th>Corr</th>
<th>Extracted Watermark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filtering</td>
<td>Blurred (gaussian, with filter size=5)</td>
<td>42.4664</td>
<td>31.8503</td>
<td>0.9368</td>
<td><img src="image3" alt="Extracted Watermark" /></td>
</tr>
<tr>
<td></td>
<td>Linear motion of a camera by len pixels=31, angle theta degree=11</td>
<td>49.5357</td>
<td>31.1816</td>
<td>0.9142</td>
<td><img src="image4" alt="Extracted Watermark" /></td>
</tr>
<tr>
<td>Additive Noise</td>
<td><img src="image1" alt="Peppers original image" /></td>
<td>59.902</td>
<td>30.3564</td>
<td>0.8756</td>
<td><img src="image5" alt="Extracted Watermark" /></td>
</tr>
<tr>
<td></td>
<td><img src="image2" alt="Binary watermark image" /></td>
<td>96.7933</td>
<td>28.2724</td>
<td>0.6867</td>
<td><img src="image6" alt="Extracted Watermark" /></td>
</tr>
<tr>
<td>Compression</td>
<td><img src="image1" alt="Peppers original image" /></td>
<td>77.0675</td>
<td>29.2621</td>
<td>0.7981</td>
<td><img src="image7" alt="Extracted Watermark" /></td>
</tr>
</tbody>
</table>

Table 2. Experimental results
Table 2. Experimental results (continued)

<table>
<thead>
<tr>
<th></th>
<th>Rotation</th>
<th>Flipping</th>
<th>Cropping</th>
<th>Distortion</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>95.362</td>
<td>90.6041</td>
<td>61.3170</td>
<td>92.2124</td>
</tr>
<tr>
<td></td>
<td>28.337</td>
<td>28.5593</td>
<td>30.2550</td>
<td>28.4829</td>
</tr>
<tr>
<td></td>
<td>0.698</td>
<td>0.7225</td>
<td>0.8708</td>
<td>0.7148</td>
</tr>
</tbody>
</table>

6. Conclusions

The need of efficient method that makes it hard to detect the marked image, it will become more prevalent. This paper, proposed a good watermark method that is build up on the visual cryptography watermarking technique for secure image authentication for colored images.

The features of our method are listed below:
- This method is applied over colored images; especially we have used the saturation plane from the HSV model for secure authentication.
- To increase the security of the proposed model, the logical X-OR and parities are used.
- According to our model we achieve good results against several kinds of attacks such as filtering, additive noise, compression, rotation, flipping, cropping and distortion.

References


Author Biographies

E Rawashdeh received a B.S. degree in Computer information system from applied science University, Jordan in 2004 and the M.S. degrees in Computer science from Jordanian University, Jordan in 2006, where she is currently working in MIS Department of Al-Balqa’a Applied University, Jordan. Her research interests include image processing.

R Zaghloul received a B.S. degree in Computer Science from Al-Balqa’a Applied University, Jordan in 2003 and the M.S. degrees in Computer science from Jordanian University, Jordan in 2005, where she is currently working in MIS Department of Al-Balqa’a Applied University, Jordan. Her research interests include image processing.