2-D DISCRETE WAVELET TRANSFORM BASED VISUAL CRYPTOGRAPHY
TECHNIQUE FOR COLOR IMAGES
N. Rajesh Kumar1*, N. R. Raajan2

*1Department of Computer Science and Engineering, Srinivasa Ramanujan Centre1,
SASTRA University, Kumbakonam – 612001, Tamil Nadu, India;
2Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering,
SASTRA University, Thanjavur – 613401, Tamil Nadu, India;
Email: rk6030@gmail.com

Abstract

Today, the security of digital image transmission became a great significant issue. Hence, security coverage is required
to accomplish the secure image transmission. Discrete Wavelet Transformation is an effective, systematic way to carry
out an image compression operation. Visual Cryptography acts as a special cryptographic technique that allows useable
information can be enciphered in the form of secret shares and the original image is obtained by stacking operation. This
paper nominates a two dimensional wavelet transform based visual cryptography technique for color images. The
proposed scheme splits the color image into multiple indecipherable patterns in the wavelet domain for secure image
transfer. Image quality metrics are computed and show that the proposed scheme has enhanced level security transfer of
color images with greater visual quality.

Keywords: Color image, Secret shares, DWT, Visual Cryptography, stacking.

1. Introduction

Information communication is an essential task in the modish information technology world. Usually, multiple medium
of information is carried out through the communication channel for interchanging the data between groups of members.
Especially image and video communications required some encryption standard with compression techniques for
efficient transmission. In order to accomplish the strong data communication, former researchers were introduced
cryptography, digital watermarking and steganography methods. Cryptography technique encrypts the secret information
into an unreadable format by fixed length of the key. The decryption phase required the reverse of the key to restore the
secret information. Furthermore, digital watermarking is introduced to protect the various types of intellectual properties such as copyright contents, trademarks, patents, industrial patterns and geographical denotations.

In watermarking, these intellectual properties are embedded into the digital information for enabling the secure data communication without affecting the original digital information. Digital watermarking techniques should be transparent, simple embedding and extracting methods with robustness for all disciplines. Bramara Neelima et. al., [1] presented a detailed study about various watermarking techniques and comparisons.

A random transform based effective watermarking technique is proposed by Ruichen Jin and Jongweon Kim [2]. At the same moment, information hiding techniques have significant growth in the area of data communication and networking. Particularly, steganography hides the secret information into the any portion of cover image by information hiding techniques.

A Sudoku based Ken Ken Puzzle information hiding technique is suggested by G. Vidya et al [3]. In this effort, they achieved best PSNR results and an improvement in the restored image quality. Nawlesh kumar and V. Kalpana [4] proposed a novel reversible steganography method using dynamic key generation for medical images. In this reversible technique recovered the cover image without any pixel deprivation. To increase the embedding capacity of steganography approach T. Somassoundaram and N. P. Subramaniam [5] proposed High capacity image steganography using secret key for medical information.

Conventional crypto, steganography and watermarking schemes execute the cipher process by single image transmission with two participants. But Naor and Shamir [6] introduced a new cryptographic technique named as “Visual Cryptography”.

In this technique secret image is commuted into a group of share images by any encryption technique and distributed to ‘n’ number of participants. The secret image is revealed by stacking the sufficient number of collected share images. The special feature of this technique is a n – 1 share images don’t reveal the secret image.

In 2016 Justie et al., [7] proposed shift tolerant visual secret sharing schemes without pixel expansion technique. This method achieved the goal to increase the number secret shares and the restoration could be more clear. In the same manner, a reversible secret sharing technique for binary images was proposed by Abhishek Mishra and Ashutosh Gupta [8]. But this is not a suitable scheme for grayscale images. Moreover, B. Pushpa Devi et al., [9] described a
watermarking technique on shuffled SVD and visual cryptography technique for copyright protection. Many cryptography and information hiding algorithms have been suggested and implemented by both traditional and novel researchers.

However, still the transfer of digital images over the communication medium is unsafe. In order to achieve the highest visual quality with secure transmission, we present a two dimensional discrete wavelet transform based visual cryptography technique for color images.

2. Proposed Method

The block diagram of our method is illustrated in Figure 1.

![Proposed Visual Cryptography Scheme](image)

Figure 1. Proposed Visual Cryptography Scheme

Image processing involves many areas for different purposes. This process also needs preprocessing, encryption, decryption, compression, segmentation, extraction, recognition on the image. Different domains use various types of images such as binary images, grayscale images and color images. In our method we have taken color image for wavelet and visual cryptography transformation.

Figure 2 shows that the disintegration color image into three channels such as RED, GREEN and BLUE. The pixel intensities of all channels range from 0 to 255. After decomposition, the channels are processed on the wavelet domain for more security.

Depend on the wavelet transformation image is split up into two sub bands such as high frequency sub band and low frequency sub band. In connection with wavelet theory, we are concentrated on both high frequency and low components for visual secret sharing. These components are further divided into eight visual secret shares for secure image transmission.
2.1 Discrete Wavelet Transform

In Discrete wavelet transform, the digital image is forked into low and high frequency components. The most of pixel intensities of host image information are located in high frequency components and low frequency component has less information. This frequency pair is called an analysis filter pair. It is further expanded into four sub bands of data to represent the array of coefficients to obtain the single level decomposition (SVD). The four sub-bands are low-low (LL), High-low (HL), low-high (LH), and High-High (HH). In the same manner LL band is decomposed into the second and third level of DWT. The layout of wavelet transformation is shown in Figure 3.

2.2 Visual Cryptography Scheme

With the employment of wavelet transformation the image is converted into third level decomposition of DWT.
Algorithm 1: Visual secret Sharing scheme

**Input:** Color Image

**Output:** Visual Secret Shares.

**Step 1:** Read the input color image.

**Step 2:** Decompose the color image into three channels.

**Step 3:** Apply DWT to each channel separately to obtain the co-efficient of third level decomposition.

**Step 4:** Determine the size of wavelet image.

**Step 5:** Set the total number of secret shares with pixel orientation

**Step 6:** Find the remainder value by using total number of shares on the given image size.

**Step 7:** For i=1:size of the image

   If (remainder_value==0)
   Keep the original value
   
   else
   Change the intensity into black
   
   End for

**Step 8:** Repeat step7 with increased remainder value to generate secret shares

**Step 9:** Finally display the secret shares.

Algorithm 2: Visual overlapping scheme

**Input:** Collected secret shares

**Output:** Original Secret Image.

**Step 1:** Test the sufficient shares are collected.

**Step 2:** Overlap all the secret shares to reveal the Wavelet transformed image.

**Step 3:** Compose all the channels into one primary component.

**Step 4:** Regress the current wavelet transform into previous wavelet image.

**Step 5:** Repeat step 4 until to obtain the original Image

**Step 6:** Display the reconstructed image.
3. **Experimental Results**

Visual cryptography technique is implemented on wavelet transformed image. In our scheme the digital image is completely modified into third level wavelet decomposition. It is clearly organized the high and low level frequencies at third level wavelet processing. The rely on observation is performed on a portable computer with Intel ® Core™ i3-3110M CPU @ 2.40 GHz processor with 2 GB RAM.

3.1 **Image quality metrics**

Image transmission should be secure, fast and high visual quality restoration. To measure the effectiveness of the proposed algorithm the following parameters are needed.

1. **Mean Squared Error**

\[
MSE = \frac{1}{MN} \sum_{j=1}^{M} \sum_{k=1}^{N} (x_{jk} - x'_{jk})^2
\]  

(1)

2. **Peak Signal to Noise Ratio**

\[
PSNR = 10 \log \left(\frac{2^n - 1}{MSE}\right) = 10 \log \frac{255^2}{MSE} 
\]  

(2)

![Figure 4. Test Images for Wavelet Transform](image1)

![Figure 5. Color image representation.](image2)
The test images and image decomposition process is depicted in Figure 4 and Figure 5. The proposed visual secret sharing scheme generates secret shares on wavelet domain is shown in Figure 6. The pixel intensities of original image are decomposed into three channels and each channel are further transformed into wavelet field. Afterward, the transformation is extended to second and third level wavelet decomposition.

The histogram representation of wavelet transformation is depicted in Figure 7 (a), (b), (c) and (d). This transformed original image is divided into 8 shares by our proposed visual secret sharing scheme. In addition histogram of visual secret share construction is shown in the Figure 8. Table 1 described the cumulative squared error value between original color image and transformed image.

Mean squared error and Peak signal to noise ratio is also computed between original color image and visual secret shares and depicted in Table 2.

**Figure 6.**  (a) Single Wavelet Transform (b) 2^{nd} Wavelet Transform (c) 3^{rd} Wavelet Transform (d) Share 1 (e) Share 4 (g) Share 8
### Table 1. Tabulation for various level of Wavelet transforms.

<table>
<thead>
<tr>
<th>S. No</th>
<th>Name</th>
<th>MSE</th>
<th>PSNR (db)</th>
<th>PSNR (db)</th>
<th>PSNR (db)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Singular</td>
<td>Second</td>
<td>Third level</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>value</td>
<td>level</td>
<td>decomposition</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>decomposition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PSNR (db)</td>
<td>PSNR (db)</td>
<td>PSNR (db)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Red</td>
<td>Green</td>
<td>Blue</td>
<td>Red</td>
</tr>
</tbody>
</table>

### Table 2. Tabulation for Visual Secret shares

<table>
<thead>
<tr>
<th>Name</th>
<th>MSE</th>
<th>PSNR (db)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Share1</td>
<td>Share4</td>
</tr>
<tr>
<td>Basketball.tif</td>
<td>1.020465e+004</td>
<td>1.022668e+004</td>
</tr>
<tr>
<td>Fabric.tif</td>
<td>5.834842e+003</td>
<td>5.231759e+003</td>
</tr>
<tr>
<td>Lena.bmp</td>
<td>1.118850e+004</td>
<td>1.118850e+004</td>
</tr>
<tr>
<td>Baboon.bmp</td>
<td>7.632823e+003</td>
<td>7.613461e+003</td>
</tr>
<tr>
<td>Peppers.png</td>
<td>8.186916e+003</td>
<td>8.219753e+003</td>
</tr>
</tbody>
</table>

![Figure 7. a) Original Image (b),(c),(d) Wavelet Image Transform of Secret Color image-](image-url)
4. Conclusion

Gratuitously new Visual Cryptography Technique is presented in this work. Visual secret shares are generated to protect the third level wavelet decomposed images. Insecurity aspect, this approach is more reliable, faster and high visually restored transmission. Image quality metrics and histogram for wavelet transform is also tabulated. Our scheme is well suitable for color image processing. In the future, we can extend this work for generating secret share only on high level components with the availability of more information.

5. References

