Improved Image Steganography Technique for Colored Images using Wavelet Transform

Saddaf Rubab  
Department of Computer Engineering, College of  
Electrical & Mechanical Engineering,  
National University of Sciences & Technology (NUST),  
Islamabad, Pakistan

M. Younus  
Department of Computer Engineering, College of  
Electrical & Mechanical Engineering,  
National University of Sciences & Technology (NUST),  
Islamabad, Pakistan

ABSTRACT  
Steganography is the most used technique for data hiding. We can implement it using any cover media like text, images, and videos. In this paper we devised a new algorithm to hide our text in any colored image of any size using wavelet transform. It improves the image quality and imperceptibility. Our method sustains the security attacks. Extensive testing is performed using different sizes of images and presented our results in payload and PSNR values.

General Terms  
Steganography, payload, wavelet, transforms, stego image, colored image, blowfish

1. INTRODUCTION  
Data hiding can be done by cryptography, steganography and watermarking. We are here only considering steganography, which literally means “covered writing”. The steganography is science of data hiding within another one, so that its presence is undetectable and suffers less security threats or attacks. It hides the content in cover media as not to provoke any doubt that there is some information or message hidden in the media [1]. Sometimes people mix it with encryption. In encryption the content is not hidden but not readable by the reader if the key is not known to him. But the encrypted content can be intercepted by anyone and chances always present that he will try to decode it or affect it by attempting to decode it for a purpose or just for the sake of curiosity. Whereas, steganography gives us more freedom to communicate and send secret information without leaving any evidence that opponent will intercept and try decoding your information.

For this, different cover media can be used like, text, image, video etc. The content to be covertly sent is payload which is called stego text after application of any steganographic technique and media used is called stego image/text/video/protocol (depending on the choice of media you are using). The opposite of it is steganalysis, which is out of the scope of this paper.

The most popular cover object is image to perform steganography. Image steganography is divided into spatial and transform domain. In spatial domain messages are embedded in the intensity of image pixel like in LSB. Whereas in transform domain, image is first transformed and then message is encoded like discrete cosine transform (DCT), discrete wavelet transform (DWT) and many others. Many different image file formats exists, but jpeg format proved to be the best among all [2].

2. WAVELET TRANSFORM  
Wavelet transform gives the best result for image transformation [6]. It decomposes signal into a set of basic functions. There are two flavors of wavelet transform, one is discrete and other is continuous. We here focus on discrete wavelet transform. In DWT we have 1-D, 2-D... n-D levels. 2DWT is used in our work. It uses the scaling and wavelet functions of IDWT. Figure 1 illustrate the 2DWT level. We can increase levels at the cost of complexity. It is two times decomposition of original signal via sub-division. to use any wavelet we have to select the filters and families like Coiflets, haar, Symlet. We have selected Symlet 6 for our experimental work.

3. BLOWFISH (ENCRYPTION ALGORITHM)  
It was designed by a cryptologist named Bruce Schneier and made it accessible for public. It is a 64-bit block cipher and variable key length. It has two parts. A first deal with the key expansion and second part performs the encryption of information. It increases contrast value in image by reducing the redundant information. In [5], it is presented that blowfish performs outclass compared to other encryption algorithms like AES, DES. We have selected blowfish to fulfill need of encrypted information.

4. RELATED WORK  
Amitava Nag, Sushanta Biswas, Debasree Sarkar & Partha Pratim Sarkar in [7] presented a novel technique using DWT transform for the cover image transformation and then Huffman is used on secret message before embedding. It uses only high frequency coefficients for embedding message bits and neglected low ones to get better image quality.

Another image steganographic method using wavelet and Microsoft Utility for RC4 encryption [8] proposed which proves to be more secure.

M. F. Tolba, M. A. Ghonemy, I. A. Taha, and A. S. Khalifa in 2004 [9] utilizes wavelet transforms that map integers to integers and proposed an algorithm that embeds the message bitstream into the LSB's of the integer wavelet coefficients of a true-color image. Experimental results showed the high invisibility of the proposed model even with large message size.
5. PROPOSED STEGANOGRAPHY METHOD

Our work is improvement of results presented in [4]. My proposed algorithm was implemented in MATLAB 7.9 and Visual Studio 2010. My devised method consists of two main processes. First one deals with the MATLAB implementation which passes some controls to Visual Studio 2010 for C# implementation of blowfish algorithm. The other process then returns back the control to MATLAB from Visual Studio 2010. I have developed main steganographic routines in MATLAB using the wavelet toolbox and Blowfish algorithm for enhanced security in C# using Visual Studio 2010. Following is my devised method:

Step 1: image histogram test
Input: Cover image
Output: Cover image
Action: If the cover image passes the histogram test
Then
accept the cover image
Else
search for another cover image.
End

Step 2: image corrections
Input: Cover image
Output: Processed cover image
Action: For each pixel of cover image apply level correction
end
For each pixel of cover image apply contrast correction
end
For each pixel of cover image apply color balance correction
end

Step 3: Apply wavelet transform
Input: Processed cover image
Output: Transformed image
Action: Apply 2D wavelet transform
End

Step 4: Calculate threshold (Th)
Input: Transformed image
Output: number of pixels can be changed (n), DWT of the cover image
Action: Calculate Th
Th = (correlation factor/Number of coefficient) \( \sum \) (mod value of all 2D wavelet coefficients)
(1)
Select DWT coefficient of every pixel in cover image
if coefficient value < Th
then
keep coefficient index and n=n+1
end

Step 5: Message encryption process
Input: Information
Output: Encrypted information
Action: Pass control from Matlab 7.9 to Visual Studio 2010
Encrypt information with Blowfish
Pass control back to Matlab
End

Step 6: Bit streaming
Input: n, encrypted information
Output: 1D bit streamed information
Action: convert the encrypted information to 1D bit stream using n
End

Step 7: 2D wavelet transform of encrypted information
Input: encrypted bit stream of the message
Output: DWT transform of the encrypted message.
Action: transform the encrypted bit stream of the message to Wavelet domain
End

Step 8: Coefficient placement
Input: 2D wavelet transform of cover image and 2D wavelet transform of the encrypted information.
Output: stego image
Action:
  a. Put coefficients of wavelet transform of encrypted information in the indexes stored in Step 4
  b. Perform inverse wavelet transform
End

6. EXPERIMENTAL RESULTS

We selected three (03) image sizes and created groups each consists of ten (10) jpeg images to perform our testing:
a. 256x256
b. 306x648
c. 512x512

The image imperceptibility is shown by PSNR values [3].

\[
MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{ij} - \hat{X}_{ij})^2
\]

\[
PSNR (dB) = 10 \log_{10} \left( \frac{I_{max}^2}{MSE} \right)
\]

\( X_{ij} \) represents the ith rows and jth columns of transformed image and \( \hat{X}_{ij} \) represents the ith rows and jth columns of original image. Higher the PSNR value means more difficult to perceive that any hidden message is hidden. In our experimental work we have found that by increasing the payload, PSNR value drops down. We have to make a compromise between payload and PSNR. Table 1 shows the average results for each group of colored images and Figure 2 shows the results in graph to help study results more easily. If we change our set of images, results will change accordingly. The payload values can also be changed by using a different information or content to be stegan by the proposed method.

As it is clear when we increase the value of correlation factor, value of MSE increases and ultimately decreases the value of PSNR (see Table 1). It was experimentally tested that our method is an improved one as it is less visible to others that any information is hidden in image that makes is more secure from enemies attacks. We have shown a 512x512 image and its stego image in Figure 3a and 3b. In our proposed method, we provided with the double security. Information is encrypted and bit streamed before performing wavelet transform on information. Then wavelet transform of information is placed in wavelet domain of cover image.
7. CONCLUSIONS
In this paper we presented an improved image steganography technique for any colored image of any size using wavelet transform and blowfish encryption algorithm in comparison with the work presented in [8]. This new method gives better invisibility and security of communication. Our method provides double security by involving blowfish, which satisfies the need of imperceptibility. Future work may be carried out to increase the payload and maintain the higher PSNR values.
Table 1: Average Payload and PSNR values for 256x256, 306x648 and 512x512 images

<table>
<thead>
<tr>
<th>Image Size</th>
<th>Correlation Factor</th>
<th>Payload %</th>
<th>MSE %</th>
<th>PSNR dB</th>
</tr>
</thead>
<tbody>
<tr>
<td>256x256</td>
<td>.1</td>
<td>31.544</td>
<td>0.3241</td>
<td>50.286</td>
</tr>
<tr>
<td></td>
<td>.2</td>
<td>40.094</td>
<td>0.453</td>
<td>47.207</td>
</tr>
<tr>
<td></td>
<td>.3</td>
<td>45.069</td>
<td>0.61</td>
<td>43.61</td>
</tr>
<tr>
<td></td>
<td>.4</td>
<td>51.226</td>
<td>1.544</td>
<td>41.677</td>
</tr>
<tr>
<td></td>
<td>.5</td>
<td>55.545</td>
<td>1.835</td>
<td>38.122</td>
</tr>
<tr>
<td></td>
<td>.6</td>
<td>62.933</td>
<td>2.673</td>
<td>32.659</td>
</tr>
<tr>
<td></td>
<td>.7</td>
<td>64.675</td>
<td>3.588</td>
<td>29.926</td>
</tr>
<tr>
<td></td>
<td>.8</td>
<td>67.501</td>
<td>4.837</td>
<td>27.754</td>
</tr>
<tr>
<td></td>
<td>.9</td>
<td>69.258</td>
<td>6.142</td>
<td>24.257</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>72.126</td>
<td>7.906</td>
<td>21.984</td>
</tr>
<tr>
<td>306x648</td>
<td>.1</td>
<td>38.395</td>
<td>0.349</td>
<td>52.046</td>
</tr>
<tr>
<td></td>
<td>.2</td>
<td>42.703</td>
<td>0.543</td>
<td>50.079</td>
</tr>
<tr>
<td></td>
<td>.3</td>
<td>49.946</td>
<td>0.693</td>
<td>48.284</td>
</tr>
<tr>
<td></td>
<td>.4</td>
<td>56.858</td>
<td>1.253</td>
<td>45.799</td>
</tr>
<tr>
<td></td>
<td>.5</td>
<td>61.938</td>
<td>1.936</td>
<td>42.284</td>
</tr>
<tr>
<td></td>
<td>.6</td>
<td>65.853</td>
<td>2.775</td>
<td>38.348</td>
</tr>
<tr>
<td></td>
<td>.7</td>
<td>71.038</td>
<td>3.766</td>
<td>36.823</td>
</tr>
<tr>
<td></td>
<td>.8</td>
<td>71.621</td>
<td>4.873</td>
<td>34.563</td>
</tr>
<tr>
<td></td>
<td>.9</td>
<td>73.606</td>
<td>6.38</td>
<td>32.363</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>74.684</td>
<td>7.824</td>
<td>28.233</td>
</tr>
<tr>
<td>512x512</td>
<td>.1</td>
<td>39.275</td>
<td>0.3931</td>
<td>55.251</td>
</tr>
<tr>
<td></td>
<td>.2</td>
<td>44.176</td>
<td>0.552</td>
<td>52.511</td>
</tr>
<tr>
<td></td>
<td>.3</td>
<td>50.389</td>
<td>0.754</td>
<td>50.594</td>
</tr>
<tr>
<td></td>
<td>.4</td>
<td>56.544</td>
<td>1.353</td>
<td>47.844</td>
</tr>
<tr>
<td></td>
<td>.5</td>
<td>61.432</td>
<td>1.974</td>
<td>44.159</td>
</tr>
<tr>
<td></td>
<td>.6</td>
<td>65.886</td>
<td>2.826</td>
<td>41.271</td>
</tr>
<tr>
<td></td>
<td>.7</td>
<td>69.412</td>
<td>3.824</td>
<td>38.566</td>
</tr>
<tr>
<td></td>
<td>.8</td>
<td>71.784</td>
<td>5.031</td>
<td>36.525</td>
</tr>
<tr>
<td></td>
<td>.9</td>
<td>74.164</td>
<td>6.366</td>
<td>34.115</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>76.143</td>
<td>7.671</td>
<td>31.065</td>
</tr>
</tbody>
</table>

8. REFERENCES


