Implementation of Variable Tone Variable Bits Gray-Scale Image Stegnography Using Discrete Cosine Transform

Sahib Khan*, Muhammad Nawaz Khan†, Somia Iqbal†, Syed Yaqoob Shah‡, Nasir Ahmad‡

†Department of Electrical Engineering, University of Engineering & Technology, Peshawar, Pakistan; ‡Department of Computer System Engineering, University of Engineering & Technology, Peshawar, Pakistan.

Email: *engrsahib_khn@yahoo.com

Received July 23rd, 2013; revised August 24th, 2013; accepted September 1st, 2013

Copyright © 2013 Sahib Khan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT

Secure exchange of information is the basic need of modern digital world of e-communication which is achieved either by encrypting information or by hiding information in other information called cover media. Concealing information requires a well designed technique of Stegnography. This work presents a technique, variable tone variable bits (VTVB) Stegnography, to hide information in a cover image. The VTVB Stegnography hides variable data in discrete cosine transform (DCT) coefficients of the cover image. VTVB Stegnography provides variable data hiding capacity and variable distortion. Additional large data hiding this technique provide extra security due to the large key size making VTVB Stegnography technique much more immune to steganalysis. The hiding makes the existence of information imperceptible for steganalysis and the key of keeping a secret makes the recovering of information difficult for an intruder. The key size is depending on cover image and numbers of bits of discrete cosine transform (DCT) coefficients used for information embedding. This is a very flexible technique and can be used for low payload applications, e.g. watermarking to high payload applications, e.g. network Stegnography.

Keywords: Information Security; Image Processing; Stegnography; Steganalysis; Discrete Cosine Transform (DCT)

1. Introduction

This Stegnography is a method of secure exchange of information; implemented by concealing covert messages in cover-medium like text, digital images [1], audios [2,3] and videos [4]. Stegnography keeps the presence of secret information undetectable and Stego-file having secret information looks like the cover-file. But there are some chances of detection. To hide information in an undetectable manner is key feature of a good Stegnographic method [4]. A method using a cover medium with a large degree of redundancy is considered the most suitable one [5]. The redundant bits are replaced with information resulting trivial change in Stego-Image [4,6]. Crandall for the first time presented a matrix coding technique with improved hiding efficiency [7]. The relation between Stegnographic codes (Stego-codes) and covering codes was studied in [8].

Information can be hidden in the cover file in spatial domain modifying cover elements and transform domain modifying transform coefficients. This paper presents a Stegnographic technique used for DCT coefficients of a cover image. The proposed technique provides a self encryption and hides variable amount of data in different DCT coefficients. As each coefficient represents a frequency component (Tone) and different amounts of data are hidden in different coefficients, that’s why it is named as variable tone variable bits (VTVB) Stegnography.

2. Previous Work

Stegnography like Cryptography is technique for secure communication of information. Various researchers made their efforts and proposed some best technique of that time. A brief description of the developments made in the field of Stegnography is given as:

The mathematical equations of Discrete Cosine Transform (DCT) and its uses in image compression [9] and the conversion of a signal to its basic components [10] opened new way for the Stegnography using DCT. A trustworthy and precise procedure has been proposed by Jessica Fridrich et al. for detecting least significant bit
In varying tone varying bits (VTVB) Steganography instead of fixed; varying data is hidden in various DCT coefficients. As each DCT coefficient’s value is represented by 16 bits i.e. of type double and any/any number of the bits can be used for data hiding using VTVB Steganography. The number of bits utilized is determined by the user depending on the requirement i.e. Hiding Capacity, Signal to Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) [30,31]. Using more bits per coefficient for data hiding in cover image, results in increase in data hiding capacity and MSE. The DCT coefficients are subjected to 2, 8, 4, 9, 6, 7 and 8 bits substitution respectively. The same sequence is followed for the other combination/s can be used for data hiding. For example if a group size of 8 coefficients is used for data hiding then there are 8 different no. of bits can be used for data hiding defined by the user as given in Figure 1.

In VTVB Steganography DCT coefficients are arranged in a group of “1” coefficients. The group size depends on the number of bits variation i.e. how many different no. of bits are used for data hiding in a group. As in double format each DCT coefficient is represented using 16 bits so using double format there are 17 different possible combination of no. of bit and any of the combination/s can be used for data hiding. For example if a group size of 8 coefficients is used for data hiding then there are 8 different no. of bits can be used for data hiding.

In coefficient “C1” of defined group only 1 bit data is hidden, in coefficient “C2 - C8” of the same group are subjected to 2, 8, 4, 9, 6, 7 and 8 bits substitution respectively. The same sequence is followed for the other groups of the same cover file. The group size may be varied depending on application. Any group size of DCT coefficients, 17 at maximum, can be used. As shown in Figure 2. The process is repeated for the whole cover file.

After hiding information in DCT coefficients the Inverse DCT transform is applied on the modified coefficient for data hiding. This work is presenting a new technique for data hiding i.e. Steganography by hiding varying amount of data in different DCT coefficients. Different amount of data is hidden within different frequency components i.e. DCT coefficients. As in communication a frequency is also called tone that’s why technique is termed as Varying Tone Varying Bits Steganography.

<table>
<thead>
<tr>
<th>C1</th>
<th>C2</th>
<th>C3</th>
<th>C4</th>
<th>C5</th>
<th>C6</th>
<th>C7</th>
<th>C8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>8</td>
<td>4</td>
<td>9</td>
<td>6</td>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>

Figure 1. Coefficients and no. of bits assignment for group size 8.
3.1. Hiding Capacity Steganography
In VTVB Steganography variable amount of data is hidden in different coefficients of each group of DCT coefficients of predefined size. The data hiding capacity depends totally on the no. of bits assigned to each coefficient of the group. More bits used for data hiding greater will be the data hiding capacity. Let consider a cover grayscale image of size \( N \times M \) is transformed using discrete cosine transform (DCT) to get DCT coefficients and DCT coefficients are divided into \( j \) number of groups with group size \( n \) i.e. each group consists of \( n \) coefficients and let “\( \text{Bi} \)” number of bits are hidden in \( \text{ith} \) coefficient of \( j \)th group. Then the total data hidden in each group \( "D_j" \) will be:

\[
D_j = \sum_{i=1}^{C} Bi
\]  

(1)

where \( D_j \) is total amount of data hidden in the \( j \)th group of DCT coefficients.

Now the total amount of data hidden in the cover “Data” will be:

\[
\text{Data} = \sum_{j=1}^{N \times M} D_j
\]  

(2)

The data hiding capacity in bits per pixel (BPP) is of VTVB Steganography is:

\[
\text{Capacity (BPP)} = \frac{\text{Data}}{N \times M}
\]  

(3)

The data capacity in percentage will be:

\[
\text{Capacity (%) } = \frac{\text{Data}}{N \times M \times 8} \times 100
\]  

(4)

The data hiding capacity of VTVB can be varied by varying the no. of bits to be embedded in DCT coefficients of the predefined group.

3.2. Key Size of VTVB Steganography
VTVB Steganography is a secure technique for data hiding in a cover file. As the data hidden in a coefficient vary from coefficient to coefficient according to a predefined key. How much number of bits are hidden in which coefficient is the key of VTVB Steganography; making it distinctive and more secure from other Steganography techniques.

Consider in image cover image of size \( N \times M \). Applying DCT on the cover image \( N \times M \) no. of DCT coefficients are obtained. As each DCT coefficient is represented by 16 bits and any combination of bits, 0 to 16 bits, can be hidden in a coefficient. So the total possible combination for a single coefficient “\( k_c \)” is given as:

\[
k_c = c_0^{16} + c_1^{16} + c_2^{16} + c_3^{16} + \ldots + c_{16}^{16}
\]  

(5)

\[
k_c = \sum_{n=0}^{16} c^n
\]  

(6)

As the key there are a total of \( N \times M \) no. of coefficients then the maximum key size “\( K \)” is:

\[
K = (N \times M) \sum_{n=0}^{16} c^n
\]  

(7)

where \( K \) is the maximum key size.

3.3. SNR, MSE and PSNR
SNR, PSNR and MSE is measurement parameters these parameter used to measure the quality and error between cover image and Stego image these parameter are calculated using the following formulas [Gonzalez, 2ed]:

\[
\text{SNR} = 10 \log_{10} \left[ \frac{\sum_{i,j} \sum_{j=1}^{C} [\text{Cov}(i,j)]^2}{\sum_{i,j} \sum_{j=1}^{C} [\text{Cov}(i,j) - \text{Stego}(i,j)]^2} \right]
\]  

(8)

\[
\text{MSE} = \frac{1}{R \times C} \sum_{i=1}^{R} \sum_{j=1}^{C} [\text{Cov}(i,j) - \text{Stego}(i,j)]^2
\]  

(9)

\[
\text{PSNR} = 10 \log_{10} \left[ \frac{255^2}{\text{MSE}} \right]
\]  

(10)

4. Implementation of VTVB Steganography
To hide variable data in discrete cosine transform (DCT) coefficients using VTVB mechanism, different combination of least significant bits of each combination are utilized. To Implement VTVB Steganography discrete cosine transform is applied on cover image resulting in DCT coefficients. The DCT coefficients are arranged in groups of specific size varying from 1 to 16. Then each coefficient of the group is subject to a fix number of bits substitution for hiding data. The group size and number of bits substituted in a coefficient are the most important factor of VTVB Steganography. These two factors decide the hiding capacity and the key size. In other words the security strength of the VTVB implemented. After hiding data/information each DCT coefficient the inverse DCT is applied on the modified coefficients having hidden data resulting in Stego Image. The whole process is shown in Figure 3 in detail.
VTVB Steganography is very flexible technique of data hiding providing the liberty to use any group size and any number of least significant bits of DCT coefficient. In this paper VTVB is implemented different group size i.e. 1 - 3 and so on and in all groups 1 bit is hidden in 1st coefficient, 2 bits in 2nd, and 3 bits in 3rd and so on. The group size and number of bits substituted in each coefficient of each group are shown in Figure 4 in detail. For each group size signal to noise ratio (SNR), peak signal to noise ratio (PSNR), mean square error (MSE) and hiding capacity is find out and is given in the results section.

The SNR, PSNR, MSE, hiding capacity and Stego images for each group size are given in results section. Hiding one bit in 1st coefficient, two bits in 2nd coefficient, three bits in 3rd coefficient and so on in each group is not the only way to hide data different number bits may be used in a coefficient of a group for example we may hide two bits in 1st coefficient, eight bits in 2nd coefficient etc as shown in Figure 5.

5. Results

Technology Both qualitative and quantitative analysis is made for different group of DCT coefficients of different sizes i.e. 1 - 16 and for each group different number of bits are substituted in different coefficients. The MSE, SNR, PSNR and hiding capacity are calculated experimentally by using the combinations of different bits for different coefficients of different sizes shown in Figures 6(a)-(p). The cover image used for data hiding is shown in Figure 6(a) and Stego images obtained for group size 1 to 8 are shown in Figures 6(b)-(i) and for rest of the group size the Stego images are not shown due to significant distortion and reduction in contrast level. The MSE, SNR, PSNR and hiding capacity for each group size are listed in Table 1 and are shown graphically in Figures 7-10 respectively.

The experimental results obtained, by implementing variable tone variable bits (VTVB) Steganography for different groups of different sizes, show the behavior of payload i.e. hiding capacity and quality measuring parameters i.e. MSE, SNR and PSNR. The results shows that as the group size increases and more data is hidden in cover file the hiding capacity increases gradually as given in Figure 7. An average increase of 6 percent occurs with increase of 1 in group size. The results also show the non-

![Block diagram of VTVB.](image-url)
Figure 4. Various group size and bits substitution in the coefficients of each group. (a) Group size 1; (b) Group size 2; (c) Group size 3; (d) Group size 4; (e) Group size 5; (f) Group size 6; (g) Group size 7; (h) Group size 8; (i) Group size 9; (j) Group size 10; (k) Group size 11; (l) Group size 12; (m) Group size 13; (n) Group size 14; (o) Group size 15; (p) Group size 16.
linear increasing trend of MSE with the increase in group size as shown in Figure 9 while the SNR and PSNR decreases with the increasing group size as shown in Figures 8 and 10.

It is clear from the results listed in Table 1 and the results presented in graphical form in Figures 7-10 respectively that increasing group size increases hiding capacity and MSE while decreasing SNR and PSNR.

6. Conclusion

VTVB Stegnography is a secure technique with a large key size making the existence of information undetectable at a low payload level and makes the recovering information difficult for any unauthorized third party due to its own encryption mechanism. VTVB has been proven to be much immune to Steganalysis. It is a flexible technique providing variable hiding capacity, SNR, PSNR and MSE and

<table>
<thead>
<tr>
<th></th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
<th>C4</th>
<th>C5</th>
<th>C6</th>
<th>C7</th>
<th>C8</th>
<th>C9</th>
<th>C10</th>
<th>C11</th>
<th>C12</th>
<th>C13</th>
<th>C14</th>
<th>C15</th>
<th>C16</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>8</td>
<td>5</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>9</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>7</td>
<td>9</td>
<td>3</td>
<td>7</td>
</tr>
</tbody>
</table>

Figure 5. Random selection of number bits for data hiding.

Figure 6. Cover image and Stego images of different group size. (a) Cover image; (b) Stego image of group size 1; (c) Stego image of group size 2; (d) Stego image of group size 3; (e) Stego image of group size 4; (f) Stego image of group size 5; (g) Stego image of group size 6; (h) Stego image of group size 7; (i) Stego image of group size 8.
Table 1. Hiding capacity, SNR, PSNR and MSE.

<table>
<thead>
<tr>
<th>SNO</th>
<th>Group Size</th>
<th>Capacity (%)</th>
<th>SNR (db)</th>
<th>PSNR (db)</th>
<th>MSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>12.5000</td>
<td>29.0102</td>
<td>53.0757</td>
<td>0.3203</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>18.7500</td>
<td>25.0695</td>
<td>49.1350</td>
<td>0.7936</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>24.9512</td>
<td>20.5156</td>
<td>44.5811</td>
<td>2.2645</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>31.2500</td>
<td>16.5834</td>
<td>40.6489</td>
<td>5.6000</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>37.4023</td>
<td>11.1257</td>
<td>35.1912</td>
<td>19.6771</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>43.5547</td>
<td>7.0410</td>
<td>31.1065</td>
<td>50.3997</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>49.7070</td>
<td>4.8326</td>
<td>28.8982</td>
<td>83.8036</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>56.2500</td>
<td>4.8056</td>
<td>28.8711</td>
<td>84.3276</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>62.0117</td>
<td>4.0229</td>
<td>28.0884</td>
<td>100.9801</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>68.1641</td>
<td>3.5679</td>
<td>27.6334</td>
<td>112.1351</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>74.4141</td>
<td>3.2933</td>
<td>27.3588</td>
<td>119.4542</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>80.4688</td>
<td>3.1353</td>
<td>27.2008</td>
<td>123.8784</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>86.6211</td>
<td>3.0820</td>
<td>27.1475</td>
<td>125.4099</td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>92.7334</td>
<td>3.0287</td>
<td>27.0942</td>
<td>126.9580</td>
</tr>
<tr>
<td>15</td>
<td>15</td>
<td>99.6582</td>
<td>3.0192</td>
<td>27.0847</td>
<td>127.2347</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>106.2500</td>
<td>3.0048</td>
<td>27.0490</td>
<td>128.2874</td>
</tr>
</tbody>
</table>

Figure 7. Capacity of VTVB from 1 to 16 bits.

Figure 8. SNR of VTVB from 1 to 16 bits.

Figure 9. MSE of VTVB from 1 to 16 bits.

Figure 10. PSNR of VTVB from 1 to 16 bits.

can be used for all types of applications requiring low hiding or large hiding capacity. SNR and PSNR decrease with an increase in hiding capacity and MSE trade is made between these parameters depending on application.

REFERENCES


Implementation of Variable Tone Variable Bits Gray-Scale Image Steganography Using Discrete Cosine Transform

23-38. http://dx.doi.org/10.1007/3-540-61996-8 29


http://dx.doi.org/10.1109/49.668971


http://os.inf.tu-dresden.de/westfeld/crandall.pdf


http://online.redwoods.cc.ca.us/instruct/darnold/LAPROJ/Fall98/PCKen/dct.pdf


http://dx.doi.org/10.1080/02533839.2011.565618


http://dx.doi.org/10.1080/02533839.2012.679054


http://dx.doi.org/10.1007/978-1-4614-3535-8 43

