Journal of Signal and Information Processing, **2013, 4, 343-350**
Published Online November 2013 (http://www.scirp.org/journal/jsip)
http://dx.doi.org/10.4236/jsip.2013.44043

Scientific Research

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

Sahib Khan[1*], Muhammad Nawaz Khan[1], Somia Iqbal[1], Syed Yaqoob Shah[2], Nasir Ahmad[2]

[1]Department of Electrical Engineering, University of Engineering & Technology, Peshawar, Pakistan; [2]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

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

[*]Corresponding author.

(LSB) non sequential embedding in digital images [11-13]. The image signature concept has been implemented by Mohesen A shourian, R. C. Jain and Yo-Sung Ho [14]. J. R. Krenn has proposed a pseudo-code algorithm to hide message in LSB of DC coefficients of cover image [15]. Ren-Junn Hwang *et al*. have proposed data hiding based on JPEG technique [16]. H. W. Tseng and C. C. Chang have proposed a novel high capacity data hiding method based on JPEG [17]. Youngran Park *et al*. have proposed and implemented a method, in spatial domain, to authenticate whether the hidden message had been deleted, forged or changed by attackers [18]. Neeta Deshpandeet *et al*. have set in data in least significant bits of cover image [19]. M. Chaumont and W. Puech have proposed a method with secret key to hide the color information in a compressed grey-level image [20]. Aneesh Jain and In-dranil Sengupta have proposed a method, resistant to JPEG compression, of hiding information using bitmap image as cover [21]. KokSheik Wong, Xiaojun Qi, and Kiyoshi Tanaka have proposed Mod4 Stegnography method, capabale of hiding information into both uncompressed and JPEG compressed image, in discrete cosine transform (DCT) domain [22]. Takayuki Ishida *et al*. have discussed an improved version of JPEG2000 Stegnography, named QIM-JPEG2000 Stegnography, using quantization index modulation (QIM) [23]. In 2010 Ching-Tsorng Tsai *et al*. presented a steganographic scheme that conceals secret information in image mosaics based on tile [24]. In 2011 Chung-Ming Wang and Peng-Cheng Wang schemes presented two new scheme SSA and ESA, for digital Stegnography of point sampled geometry in the spatial domain image features [25]. Debnath Bhattacharyya proposed a data hiding technique that exploits some features of audio signals that was able to hide data from perception robustly [26]. A distance based algorithm named decreasing distance decreasing bits (DDDB) was proposed and implemented by Sahib Khan *et al*. in 2011 [27] and in 2013 modular distance technique (MDT) was adopted for the implementation of image Stegnography [28].

3. Proposed Work

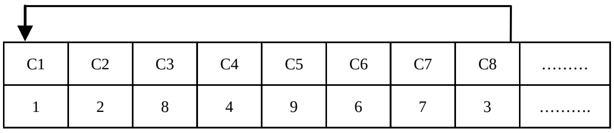
Stegnography can be implemented in spatial domain as well as transform domain. In spatial domain data is hidden directly in cover file pixels by varying the signal intensity while in transform domain the transform coefficients are modified according the message. This work deals with the implementation of Image Stegnography in Discrete Cosine Transform (DCT). As most of the Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT [29]. Due to this distribution of energy the higher frequency were mostly used for data hiding. Almost all the previous work used either fixed data hiding or targeted a specific region of DCT coefficients for data hiding. This work is presenting a new technique for data hiding *i.e.* Stegnography 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 Stegnography.

In varying tone varying bits (VTVB) Stegnography 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 Stegnography. 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 subject to varying bits substitution ranging from 0 bits *i.e.* no hiding to 16 bits. How much number of bits are hidden in which coefficient is the key of VTVB Stegnography; making it distinctive and more secure from other Stegnography techniques.

In VTVB Stegnography DCT coefficients are arranged in a group of "I" 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 defined by the user as given in **Figure 1**.

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 coeffi-



C1	C2	C3	C4	C5	C6	C7	C8	………
1	2	8	4	9	6	7	3	……….

Figure 1. Coefficients and no. of bits assignment for group size 8.

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17
1	2	3	4	5	6	7	8	4	3	6	10	11	…	…	…	…

Figure 2. Coefficients and no. of bits assignment for group size 13.

coefficients to get Stego file.

3.1. Hiding Capacity Stegnography

In VTVB Stegnography variable amount of data is hidden in different coefficients of each groups of DCT coefficient 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* × *M* is transformed using discrete cosine transform (DCT) to get DCT coefficients and DCT coefficients are divided in to "*j*" number of groups with group size "*n*" *i.e.* each group consists of "*n*" coefficients and let "*Bi*" number of bits are hidden in ith coefficient of *j*th group. Then the total data hidden in each group "D_j" will be:

$$D_j = \sum_{i=1}^{n} Bi \tag{1}$$

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:

$$\text{Data} = \sum_{j=1}^{N\times M} D_j \tag{2}$$

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

$$\text{Capacity}(\text{BPP}) = \frac{\text{Data}}{N\times M} \tag{3}$$

The data capacity in percentage will be:

$$\text{Capacity}(\%) = \frac{\text{Data}}{N\times M\times 8}\times 100 \tag{4}$$

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

3.2. Key Size of VTVB Stegnography

VTVB Stegnography 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 predefine key. How much number of bits are hidden in which coefficient is the key of VTVB Stegnography; making it distinctive and more secure from other Stegnography techniques.

Consider in image cover image of size *N* × *M*. Applying DCT on the cover image *N* × *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:

$$k_c = c_0^{16} + c_1^{16} + c_2^{16} + c_3^{16} + \cdots + c_{16}^{16} \tag{5}$$

$$k_c = \sum_{n=0}^{16} c_n^{16} \tag{6}$$

As the key there are a total of *N* × *M* no. of coefficients then the maximum key size "*K*" is:

$$K = (N\times M)\sum_{n=0}^{16} c_n^{16} \tag{7}$$

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]:

$$\text{SNR} = 10*\log_{10}\left[\frac{\sum_{i=1}^{R}\sum_{j=1}^{C}\left[\text{Cov}(i,j)\right]^2}{\sum_{i=1}^{R}\sum_{j=1}^{C}\left[\text{Cov}(i,j)-\text{Stego}(I,j)\right]^2}\right] \tag{8}$$

$$\text{MSE} = \frac{1}{R*C}\sum_{i=1}^{R}\sum_{j=1}^{C}\left[\text{Cov}(i,j)-\text{Stego}(i,j)\right]^2 \tag{9}$$

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

4. Implementation of VTVB Stegnography

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 Stegnography 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 Stegnography. 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.

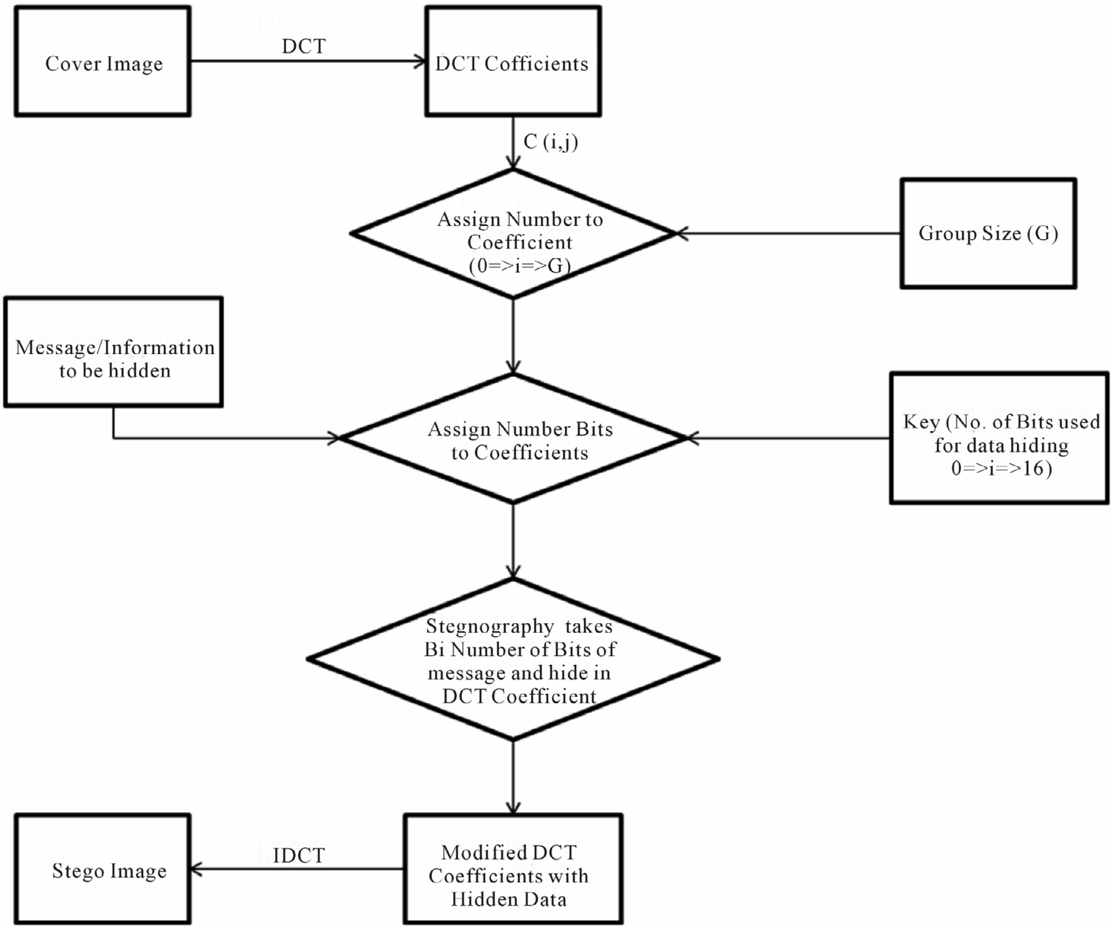

Cover Image
DCT
DCT Cofficients
C (i,j)
Assign Number to Coefficient (0=>i=>G)
Group Size (G)
Message/Information to be hidden
Assign Number Bits to Coefficients
Key (No. of Bits used for data hiding 0=>i=>16)
Stegnography takes Bi Number of Bits of message and hide in DCT Coefficient
Stego Image
IDCT
Modified DCT Coefficients with Hidden Data

Figure 3. Block diagram of VTVB.

VTVB Stegnography 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) Stegnography 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-

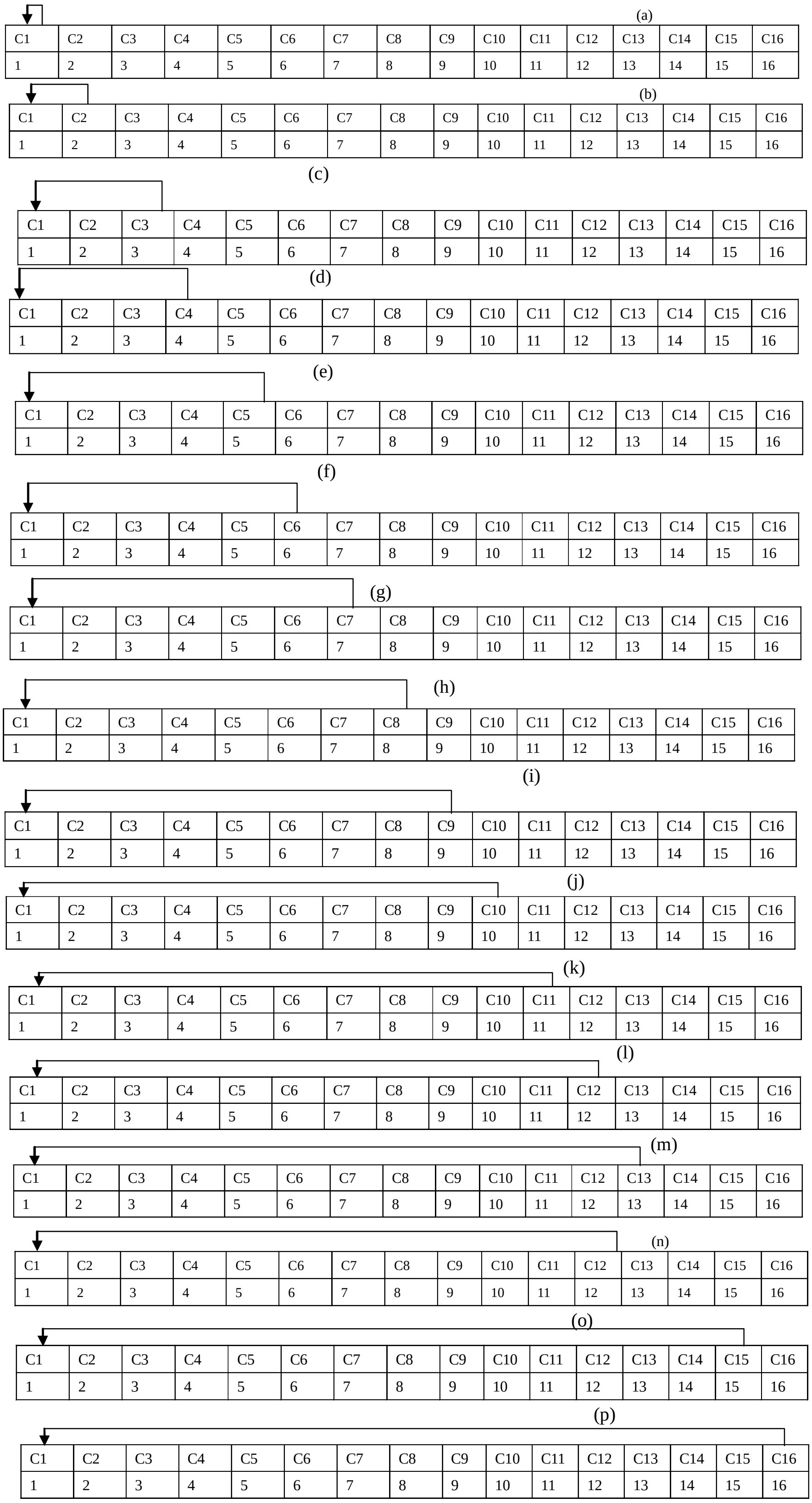

(a)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(b)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(c)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(d)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(e)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(f)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(g)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(h)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(i)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(j)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(k)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(l)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(m)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(n)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(o)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
(p)
C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

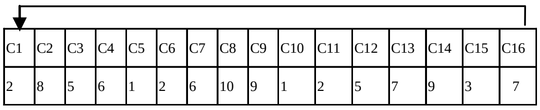
Figure 4. Various group size and bits substation in the coefficients of each group. (a) Group size 1; (b) Group size 2; (c) Group size 3; (d) Group size 4; (e) Group size 5; (f) Group size 6; (g) Group size7; (h) Group size 8; (i) Group size 9; (j) Group size 10; (k) Group size 11; (l) Group size 12; (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



C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16
2	8	5	6	1	2	6	10	9	1	2	5	7	9	3	7

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

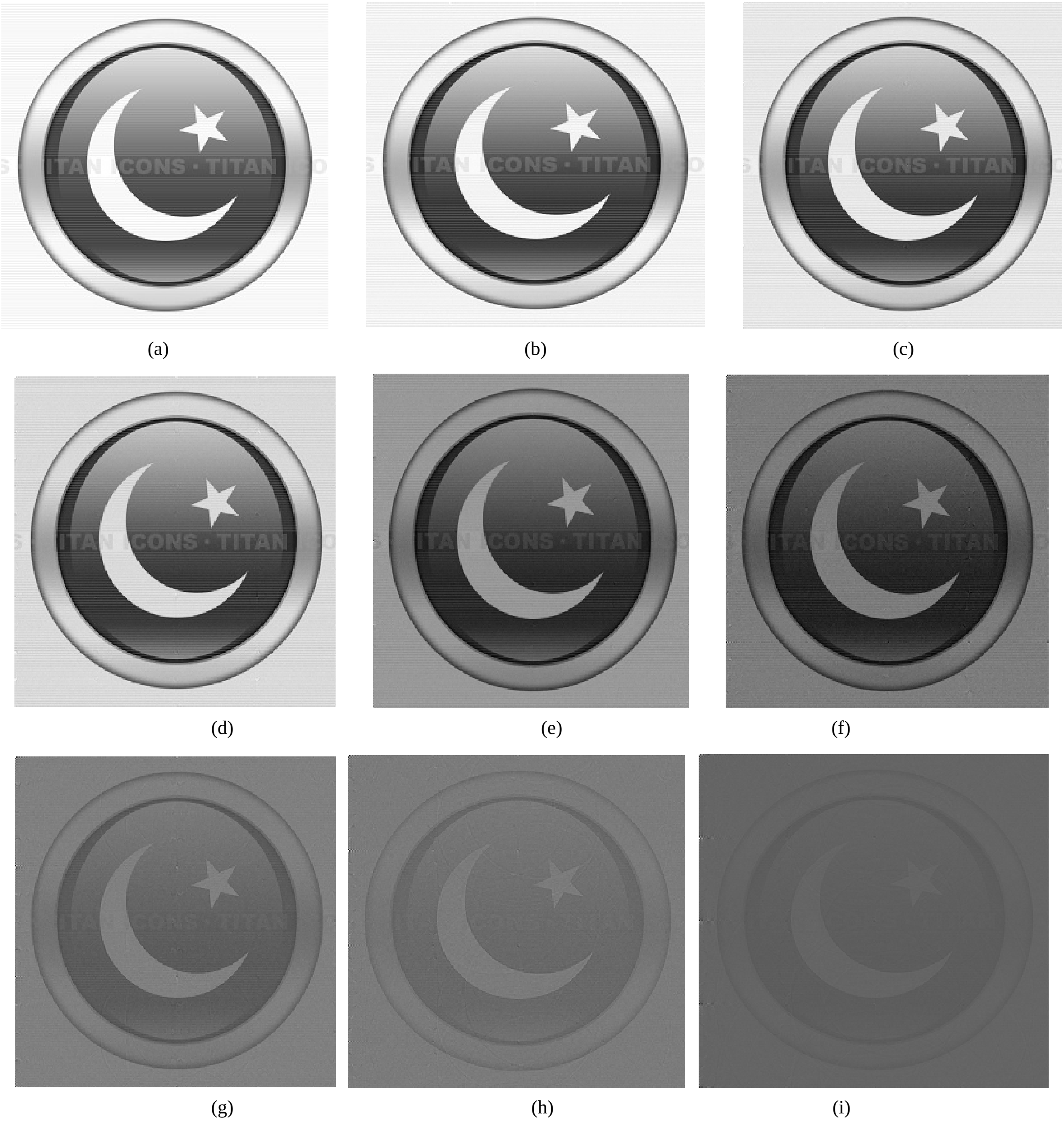

(a) (b) (c)
(d) (e) (f)
(g) (h) (i)

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.

SNO	Group Size	Capacity (%)	SNR (db)	PSNR (db)	MSE
1	1	12.5000	29.0102	53.0757	0.3203
2	2	18.7500	25.0695	49.1350	0.7936
3	3	24.9512	20.5156	44.5811	2.2645
4	4	31.2500	16.5834	40.6489	5.6000
5	5	37.4023	11.1257	35.1912	19.6771
6	6	43.5547	7.0410	31.1065	50.3997
7	7	49.7070	4.8326	28.8982	83.8036
8	8	56.2500	4.8056	28.8711	84.3276
9	9	62.0117	4.0229	28.0884	100.9801
10	10	68.1641	3.5679	27.6334	112.1351
11	11	74.4141	3.2933	27.3588	119.4542
12	12	80.4688	3.1353	27.2008	123.8784
13	13	86.6211	3.0820	27.1475	125.4099
14	14	92.7734	3.0287	27.0942	126.9580
15	15	99.6582	3.0192	27.0847	127.2347
16	16	106.2500	3.0048	27.0490	128.2874

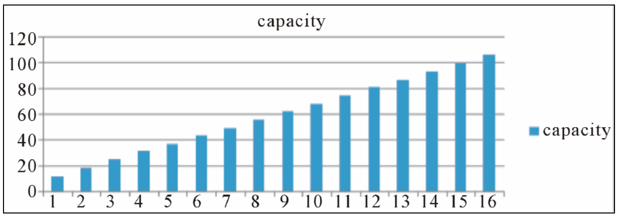


Figure 7. Capacity of VTVB from 1 to 16 bits.

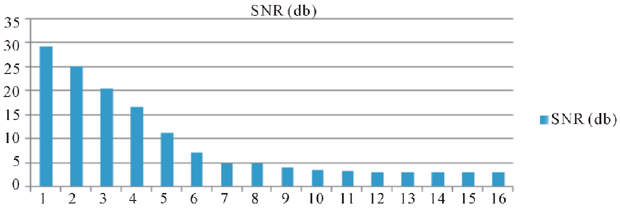


Figure 8. SNR of VTVB from 1 to 16 bits.

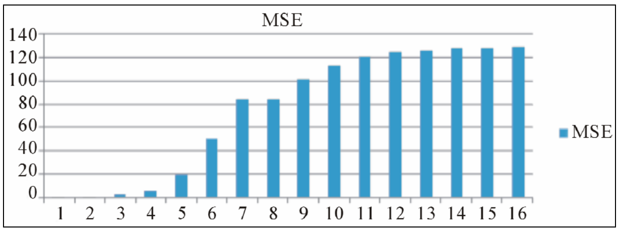


Figure 9. MSE of VTVB from 1 to 16 bits.

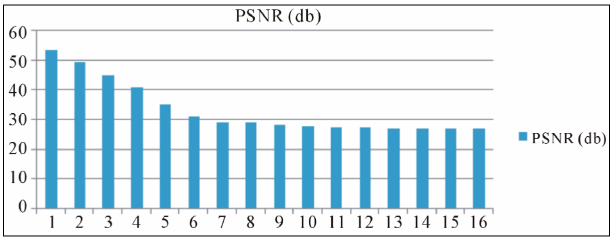


Figure 10. PSNR of VTVB from 1 to 16 bits.

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

[1] T. Moerland, “Stegnography and Steganalysis,” Leiden Institute of Advanced Computing Science, 2003. www.liacs.nl/home/ tmoerl/privtech.pdf

[2] D. Artz, “Digital Stegnography: Hiding Data within Data,” *IEEE Internet Computing Journal*, Vol. 5, No. 3, 2001, pp. 75-80.

[3] T. Handel and M. Sandford, “Hiding Data in the OSI Network Model,” *Proceedings of the 1st International Workshop on Information Hiding*, Vol. 1174, 1996, pp.

23-38. http://dx.doi.org/10.1007/3-540-61996-8_29

[4] K. Solanki, K. Sullivan and U. Madhow, Eds., "Maximizing Steganographic Embedding Efficiency by Combining Hamming Codes and Wet Paper Codes," *Lecture Notes in Computer Science*, Vol. 5284, 2008, pp. 60-71.

[5] K. Ahsan and D. Kundur, "Practical Data Hiding in TCP/ IP", *Proceedings of the Workshop on Multimedia Security at ACM Multimedia*, 2002.

[6] R. J. Anderson and F. A. P. Petitcolas, "On the Limits of Stegnography," *IEEE Journal of Selected Areas in Communications*, Vol. 16, No. 4, 1998, pp. 474-481. http://dx.doi.org/10.1109/49.668971

[7] R. Crandall, "Some Notes on Stegnography," *Steganography Mailing List*, 1998. http://os.inf.tu-dresden.de/westfeld/crandall.pdf

[8] F. Galand and G. Kabatiansky, "Information Hiding by Coverings," *Proceedings of the IEEE Information Theory Workshop*, 2004, pp. 151-154.

[9] K. Cabeen and P. Gent, "Image Compression and Discrete Cosine Transform," College of Redwoods. http://online.redwoods.cc.ca.us/instruct/darnold/LAPROJ/ Fall98/PKen/dct.pdf

[10] A. B. Watson, "Image Compression Using the Discrete Cosine Transform," *NASA Ames Research Center*, *Mathematica Journal*, Vol. 4, No. 1, 1994, pp. 81-88.

[11] J. Fridrich, M. Goljan and R. Du, "Detecting LSB Steganography in Color and Gray-Scale Images," *Magazine of IEEE Multimedia*, *Special Issue on Multimedia and Security*, Vol. 8, No. 4, 2001, pp. 22-28.

[12] J. Bierbrauer and J. Fridrich, "Constructing Good Covering Codes for Applications in Stegnography," *Transactions on Data Hiding and Multimedia Security*, Springer, Heidelberg, 2007. http://www.math.mtu.edu/jbierbra/

[13] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Stegnography," *IEEE Security & Privacy*, Vol. 1, No. 3, 2003, pp. 32-44.

[14] M. A. Shourian, R. C. Jain and Y.-S. Ho, "Dithered Quantization for Image Data Hiding in the DCT Domain," *Proceedings of IST* 2003, 16-18 August 2003, Isfahan, pp. 171-175.

[15] J. R. Krenn, "Stegnography and Steganalysis," 2004.

[16] R.-J. Hwang, T. K. Shih and C.-H. Kao, "A Lossy Compression Tolerant Data Hiding Method Based on JPEG and VQ," *Journal of Internet Technology*, Vol. 5, No. 3, 2004, pp. 171-178

[17] H.-W. Tseng and C.-C. Chang, "High Capacity Data Hiding in JPEG Compressed Images," *Informatica*, Vol. 15, No. 1, 2004, pp. 127-142.

[18] Y. Park, H. Kang, K. Yamaguchi and K. Kobayashi, "Integrity Verification of Secret Information in Image Steganography," *Symposium on Information Theory and Its Applications*, Hakodate, 2006.

[19] N. Deshpande, K. Sneha and D. Jacobs, "Implementation of LSB Stegnography and Its Evaluation for Various Bits," 1*st International Conference on Digital Information Management*, Bangalore, 6 December 2006, pp. 173-178. http://dx.doi.org/10.1109/ICDIM.2007.369349

[20] M. Chaumont and W. Puech, "DCT-Based Data Hiding Method to Embed the Color Information in a JPEG Grey Level Image," 14*th European Signal Processing Conference* (*EUSIPCO* 2006), Florence, 4-8 September, 2006.

[21] A. Jain and I. S. Gupta, "A JPEG Compression Resistant Stegnography Scheme for Raster Graphics Images," *IEEE Region* 10 *Conference of TENCON*, 30 October - 2 November 2007, Taipei, pp. 1-4.

[22] K. Wong, X. J. Qi and K. Tanaka, "A DCT Based Mod4 Stegnography Method," *Signal Processing*, Vol. 87, No. 6, 2007, pp. 1251-1263. http://dx.doi.org/10.1016/j.sigpro.2006.10.014

[23] T. Ishida, K. Yamawaki, H. Noda and M. Niimi, "Performance Improvement of JPEG2000 Stegnography Using QIM," *Journal of Communication and Computer*, Vol. 6, No. 1, 2009.

[24] C.-T. Tsai, C. Liaw, Y.-H. Liao and C.-H. Ko, "Concealing Information in Image Mosaics Based on Tile Image Features," *Journal of the Chinese Institute of Engineers*, Vol. 34, No. 3, 2011, pp. 429-440. http://dx.doi.org/10.1080/02533839.2011.565618

[25] C.-M. Wang and P.-C. Wang, "Data Hiding on Point-Sampled Geometry," *Journal of the Chinese Institute of Engineers*, Vol. 29, No. 3, 2006, pp. 539-542.

[26] D. Bhattacharyya, T.-H. Kim and P. Dutta, "A Method of Data Hiding in Audio Signal," *Journal of the Chinese Institute of Engineers*, Vol. 35, No. 5, 2012, pp. 523-528. http://dx.doi.org/10.1080/02533839.2012.679054

[27] S. Khan, M. H. Yousaf and M. J. Akram, "Implementation of Variable Least Significant Bits Stegnography Using Decreasing Distance Decreasing Bits Algorithm," *International Journal of Computer Science Issues*, Vol. 8, No. 6, 2011.

[28] S. Khan and M. H. Yousaf, "Implementation of VLSB Stegnography Using Modular Distance Technique," *Innovations and Advances in Computer*, *Information*, *Systems Sciences*, *and Engineering Lecture Notes in Electrical Engineering*, Vol. 152, 2013, pp. 511-525. http://dx.doi.org/10.1007/978-1-4614-3535-8_43

[29] E. Walia and P. J. Navdeep, "An Analysis of LSB & DCT Based Stegnography," *Global Journal of Computer Science and Technology*, Vol. 10, No. 1, 2010, pp. 4-8.

[30] E. Neuman, "MATLA B Tutorials," Department of Mathematics, Board of Trustees, Southem Illinois University, Carbondale, 2009.

[31] R. C. Gonzalez and R. E. Woods, "Digital Image Processing," 2nd Edition, Prentice-Hall, 2002.