 CMES, vol.117, no.1, pp.1-16, 2018

Increasing Distance Increasing Bits Substitution (IDIBS) Algorithm for Implementation of VTVB Steganography

Sahib Khan[1,*], Arslan Arif[1], Syed Tahir Hussain Rizvi[2] and Nasir Ahmad[3]

Abstract: Cryptography and steganography are two important and related fields of information security. But, steganography is slightly different in the sense that it hides the existence of secret information from unauthorized users. It is one of the most appealing research domains, have applications like copyright protection, data integrity protection and manipulation detection. Several steganography techniques have been proposed in literature. But, in this work a new information hiding algorithm is presented. The proposed technique de-correlates frequency components of cover image using discrete cosine transform and uses the least significant bits of frequency components for hiding secret information. The tech-nique hides variable number of bits of secret message in different frequency components. Therefore, it hides different amount of secret information in different regions of cover im-age and results in enhancement of security. The algorithm has the flexibility to change the hiding capacity and quality of final stego image. It has been observed from experimental results that a hiding a capacity from 3% to 43% can be achieved with significantly good quality of 41 dB to 37 dB in term of peak signal to noise ratio. The successful recovery of the hidden information need the pattern, called stego key, in which is used in hiding process. The algorithm provides twofold security; hiding keeps the existence of hidden information secret and the large key size makes the retrieval of hidden information difficult for intruders.

Keywords: VTVB steganography, image processing, information security, data hiding.

1 Introduction

Cryptography [Bender, Gruhl, Morimot et al. (1996); Dodis (2017)] and steganography [Karabatak and Yigit (2018); Jain, Trivedi and Tiwari (2008)] are two most prominent and broad sets of techniques used for securing information. Especially, in case of communication of secret messages using sensitive systems, to stop the unauthorized access and attempt to get access to the secret information and also protect information while store on any storage media. In cryptography, the encryption mechanism is used to convert plane message

[1] Department of Electronics and Telecommunications, Politecnico di Torino, 10129 Torino, Italy.
[2] DAUIN, Politecnico di Torino, 10129 Torino, Italy.
[3] Department of Electronic and Electrical Engineering, Loughborough University, United Kingdom.
* Corresponding Author: Sahib Khan. Email: sahib.khan@polito.it.

to cipher message also called encrypted message. The encryption convert message from readable format to an unreadable format before transmission or storage. The authorized user accesses the encrypted message by decrypting it through the secret key [Ferguson and Schneier (1982); Schneier (2007); Stallings (2010)]. The cryptographic technique, does not hide the presence of hidden information, rather, it convert secret information in other unreadable format and changes made can be detected by experts and attempts can be made to decrypt the information back [Cheddad, Condell, Curran et al. (2010)].

Steganography focuses on hiding, contrary to cryptography, and keep the existence of secret information undetectable. Therefore, it is a skill of hiding the secret message in a cover medium without attracting suspect of attackers. It keeps the existence of the veiled message un-perceivable [Fridrich (2009)]. There are different kinds of covering medium used in steganography namely text, audio, image and video. However, Images attracted the intention of steganographers the most, due to high level redundant of bits. Moreover, it is easy to achieve a reasonable hiding capacity and significantly high image quality and distortion tolerance [Katzenbeisser and Petitcolas (2000)]. Compared with cryptography, steganography has a high privacy measures and security by making secret message, on the whole, invisible.

The exclusive aim of steganography is to keep secret message imperceptible to human visual systems (HVS) [Khan, Ahmad, Ismail et al. (2015)]. To hide data efficiently, Steganographers developed different techniques by embedding secret message in the least significant bits (LSB) of image pixels in spatial domain. These methods include 4 LSB steganography [Bhattacharyya, Kim and Dutta (2012)], VLSB steganography [Khan, Yousaf and Akram (2011); Khan and Yousaf (2013); Khan, Ahmad and Wahid (2016)], data hiding in Edges [Khan, Ahmad, Ismail et al. (2015)] and others. Along with spatial domain technique, researchers also made use of different transform for data hiding. Discrete cosine transform (DCT) [Chang, Lin, Tseng et al. (2007); Li and Wang (2007); Lin (2012)] and wavelet transform [Amirtharajan and Rayappan (2012); Xie, Lin and Chang (2018)] are broadly used for data hiding. In transform domain, transformed coefficients are in charge of the secret content. These techniques have advantage of robustness to withstand different image processing technique as rotations or cropping.

For example, secret messages were hidden in the DCT coefficients, for hiding data in image exploits how the HVS perceived images. HVS is more sensitive to lower frequency components. The HVS drowns higher frequency components of an image and emphasizes lower frequencies. To convert image to its frequency components, DCT is used. DCT is used to transform cover image to frequencies coefficients. This is a de-correlation process and divide image details into high medium and low frequency coefficients. The DCT transform represent all the details of image but, in terms of frequency coefficients instead of pixel values. High DCT coefficients represent the texture details of cover image while. low coefficients have energy details.

It has been observed that the DC and first few AC coefficients are of great importance. The low frequency coefficients of DCT, even less than 25%, contain most of the energy of image [Khan, Khan, Iqbal et al. (2013); Saha, Ghosal, Chakraborty et al. (2018)]. So, to

keep these energy in mind the 75% DCT coefficients are less significant and using them for data hiding does not affect image quality significantly. The aim of image steganography in DCT domain is to exploit these characteristics of DCT coefficients. The insignificant DCT coefficients are used for data hiding using image as cover media.
In this paper a new method, increasing distance increasing bits substitution(IDIBS) algorithm, is presented to implement variable tone varying bits (VTVB) steganography. The IDIBSA hide data in higher DCT coefficient than lower coefficient. Hence, the smooth region of cover image is less affected than complex region. Which makes the presence of hidden information invisible and results in a quality stego image. Besides this the hiding capacity can be increased/decreased depending on applications.

2 VTVB steganography

Steganography is an important field of information security and has a wide range of applications in the modern era of communication [Lu, He, Yeung et al. (2018)]. It is used in information protection [Ulker and Arslan (2018)], copyright protection [Hussain, Wahab, Idris et al. (2018)] and data integrity protection [Sharma, Srivastava and Mathur (2018)]. Some state of the art data hiding techniques are focused on achieving high quality stego images, while some other techniques aim to protect information from statistical attacks and steganalysis [Lu, He, Yeung et al. (2018)]. However, the information hiding technique proposed in this paper is focused on hiding secret information the DCT frequency components of the image used as cover media, in a distributed manner. The distribution of secret message bits, is done completely on distance basis. The coefficients near to reference points are subjected to less number of bits substitution and far coefficients are used to hide more bits. The technique is termed as variable tone variable bits (VTVB) steganography [Khan, Khan, Iqbal et al. (2013)]. In this paper an efficient algorithm named, increasing distance increasing bits substitution algorithm, is presented to implement VTVB steganography. As reported in literature and proved experimentally, most of cover image energy is limited to low frequency components of DCT; which appear in top left corner of DCT coefficients [Khan, Khan, Iqbal et al. (2013)]. While, high frequency components of DCT have a very little amount of total energy. From data hiding perspective, a little change in low frequency components is more vulnerable and detectable to HVS, while changes in high frequency component is invisible to HVS. Therefore, the high frequency components of DCT are used for information embedding purpose. VTVB steganography is such a technique that hides different number of information bits in various DCT components of cover image. In contrast to fixed data hiding, VTVB steganography embed different amount secret data in different frequency components of cover image. The DCT coefficients are represented in double i.e. 16 bits format and VTVB steganography utilizes any number of bits, from 0 to 16, for data hiding.
The number bits of a DCT coefficient, used for data hiding are the key factor for the implementation of VTVB steganography. This work presents an algorithm, IDIBSA, for the implementation of VTVB steganography. This algorithm divides DCT components of the cover image in various sectors on the basis of distance from a reference point (reference

DCT coefficient) and different amount of secret information is hidden in each sector. The number of cover bits used for data embedding is decided, depending on the distance of a specific sector from the reference point. The number of bits increases with the increasing distance of the sector from the reference point.
Here it is worth mentioning that the number of bits used for embedding secret information play a key role and is totaly decided by the user according to application and requirements, i.e. hiding capacity, peak signal to noise ratio (PSNR) and mean square error (MSE) Jain, Trivedi and Tiwari (2008); Bhattacharyya, Kim and Dutta (2012). Larger this number, larger the hiding capacity and indeed larger the MSE and vice versa. The number of bits vary from 0 bits i.e. no hiding, to 16 bits and play as a key to recover the hidden information, and shows the distinction of the proposed technique and make it secure than other steganography techniques.

3 Increasing distance increasing bits substitution algorithm

As discussed in the previous section VTVB steganography hide secret information in a distributed way in LSB of DCT components of cover image and hide different number bits in different coefficients. But, how can we hide and how these information be recovered is important question. For this VTVB steganography needs a an effective and efficient algorithm. The algorithm must decide how the variable data hiding can be done on sender side to make information secure and how can it be recovered on the receiver side by the intended received only. Here, in section new algorithm to implement VTVB steganograpgy is presented. This algorithm is named as increasing distance increasing bits substitution (IDIBS) algorithm. IDIBS algorithm hides different amount of secret data in different coefficients. It divides the coefficients in different number of sectors. The coefficients are classified on the basis of their distances from the reference point i.e. reference coefficient. Let $Cover$ is the cover image of $R \times C$, where, R and C represent the number of rows and columns of the cover image. After processing complete cover image, an array of DCT coefficients D is obtained. The array has a size the same as that of the cover image $Cover$. This is shown mathematically in Eq. (1).

$$D = dct\,(Cover) \tag{1}$$

The DCT coefficients are then divided in N_s number of sectors, where the N_s ranges from 1 to 17. The IDIBS algorithm considers first coefficient as reference and the maximum possible distance d_{max}, i.e. the distance of the reference point to bottom left coefficient, is calculated. Here to $D(1,1)$ is considered as reference point and $D(R,C)$ is far most DCT coefficient in the array. The d_{max} is calculated according to Eq. (2).

$$d_{max} = \sqrt{(R-1)^2 + (C-1)^2} \tag{2}$$

The DCT coefficients are divided into a number of sector of equal size. The sector size W_s is calculated as given by Eq. (3).

$$W_s = \frac{d_{max}}{N_s} \tag{3}$$

Then, the distance d_{ij} of each and every individual DCT coefficient $D(i,j)$ from the reference point $D(1,1)$, is calculated, illustrated in Eq. (4).

$$d_{ij} = \sqrt{(i-1)^2 + (j-1)^2} \tag{4}$$

Now, DCT coefficients are classified on the basis of their distances from the reference point. Each DCT coefficient i s a ssigned t o s ector a nd t he n umber o f b its t o b e used for data hiding is also decided for each sector. The sector near to the reference point is subjected to less data embedding, as it has the coefficients h aving m ost t he c over im-age energy. Therefore, these coefficients a re s ubjected t o l ess n umber o f b its substitu-tion to preserve image quality and avoid distortion to a large extent. The number of bits used for data hiding in a sector increases as sector distance form the reference point in-creases. This procedure affects the smooth area of the cover image at minimum, while hide more data in complex regions of the cover image. The process is explained here as: Where in Fig. 1, k and N are defined as under:

- k is the sector number and $0 \leq k \leq (N-1)$
- N is the number of bits substituted in N^{th} sector

The allocation of a DCT coefficient $D\,(i,\,j)$ to a specific sector depends on the distance of the coefficient from the reference point. That is why the assignment is done completely on the basis of the distance and the total number of sectors and sector size individual sector size plays important rule in hiding process. The sector allocation is given in Eq. (5).

$$\begin{cases} \text{if } 0 \leq d_{ij} < W_s, & D\,(i,j) \in S_1 \\ \text{if } W_s \leq d_{ij} < 2W_s, & D\,(i,j) \in S_2 \\ \text{if } 2W_s \leq d_{ij} < 3W_s, & D\,(i,j) \in S_3 \\ . & \\ . & \\ \text{if } \ (N-1)\,W_s \leq d_{ij} < NW_s, & D\,(i,j) \in S_N \end{cases} \tag{5}$$

Where, S_1, S_2, S_3, ..., S_N, represent the individual sectors i.e. Sector 1, Sector 2, Sector 3,...., and Sector N, respectively. The DCT coefficients are the processed for information hiding using the increasing distance increasing bits substitution algorithm. The a number of least significant bits of a DCT coefficient $D\,(i,j)$ are substituted with secret message bits. This substitution results in new coefficient $Steg\_dct_{ij}$ called stego DCT coefficient. The number of bits to be substituted get increase as the distance of the coefficient increases with respect to reference point. The hiding procedure is explained in Eq. (6).

$$Steg\_dct_{ij} = \begin{cases} D(i,j) \bullet m_0, & \text{if } 0 \le d_{ij} < W_s \\ D(i,j) \bullet m_1, & \text{if } W_s \le d_{ij} < 2W_s \\ D(i,j) \bullet m_2, & \text{if } 2W_s \le d_{ij} < 3W_s \\ . & \\ . & \\ D(i,j) \bullet m_{N-1}, & \text{if } (N-1)W_s \le d_{ij} < NW_s \end{cases} \tag{6}$$

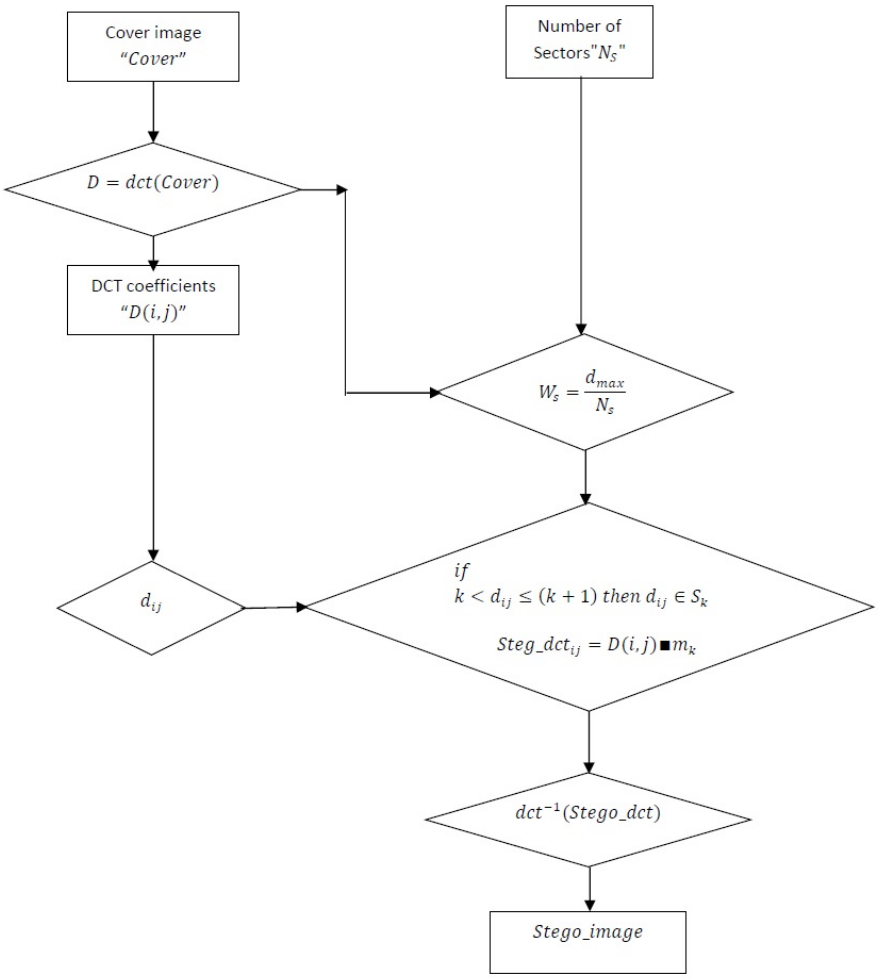

Figure 1: Block diagram implementation of IDIBS Algorithm

Where, m_o, m_1, m_2,..., m_N show the number of secret message bits hidden in the least significant bits of Sector 1, Sector 2, Sector 3,..., and Sector N, respectively. And N is the n^{th} sector.After processing all the DCT coefficients a new set of stego DCT coefficients are obtained. To covert these modified coefficients to stego image inverse DCT transformation is applied to these processed coefficients, as given in Eq. (7).

$$Stego\_image = DCT^{-1}\left(Steg\_dct\right) \tag{7}$$

The implementation process of VTVB steganography using IDIBS algorithm is explained in a flowchart diagram, shown in Fig. 1.

The VTVB steganography using IDIBS algorithm, doesn't hide secret data bits in lower frequency components, and hide large data bits in the higher frequency components of DCT. In other words, no hiding is done flat parts of cover image, and high level of hiding in complex part of cover image. The number of bits to be hidden increases as the frequency of component increase. The algorithm generate high quality stego images, and the changes introduce during the process are not attractive for HVS, due to limitation of HVS having less sensitivity for changes in complex parts of image than smooth parts.

The variation number of substituted bits with increasing sector distance is shown here in Fig. 2. In Fig. 2, each cell is representing a sector constructed according to the procedure explained in the previous section. The Fig. 2, also shows that DCT coefficients are divided in 11 sectors i.e. $N = 11$. It is shown that no data is hidden in the sector near the reference point as indicated by index 0, the 2nd near most sectors is for 1 bit substitution i.e. 1 bit of secret message is hidden in the DCT coefficient of this sector, similarly 2 bits of secret message are hidden in the 3rd near most sectors DCT coefficients, and so on. In far most sectors DCT coefficients 10 bits of secret message are hidden. Remember that is just one possible arrangement of DCT coefficients in different sectors and allocation of number of bits. Here in this paper, different possible number of sectors are used for experimentation in the coming section.

0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	2	3	4	5	6	7	8	9	10
3	3	3	3	4	5	6	7	8	9	10
4	4	4	4	4	5	6	7	8	9	10
5	5	5	5	5	5	6	7	8	9	10
6	6	6	6	6	6	6	7	8	9	10
7	7	7	7	7	7	7	7	8	9	10
8	8	8	8	8	8	8	8	8	9	10
9	9	9	9	9	9	9	9	9	9	10
10	10	10	10	10	10	10	10	10	10	10

Figure 2: Sample assignment of number od bits substituted in different sectors on the basis of increasing distance

4 Hiding capacity

IDIBS algorithm takes DCT of cover image and divides DCT coefficients in different number of sectors. Then each sectors coefficients are subjected to a specific number of bits substitution. Letś consider a cover image of size $R \times C$. As each of cover image pixel, in spatial domain, is represented by 8 bits, so the total hiding space available in spatial domain, $C_{available}$ is given in Eq. (8).

$$C_{available} = R \times C \times 8 \tag{8}$$

The cover image coefficients are divided in N_s number of sector each of sector size S_k. Let m_k number of are hidden each coefficients of a sector k of size S_k. Then the total number of message bits B_k hidden in that sector is given by Eq. (9).

$$B_{total} = \sum_{k=1}^{N_S} B_k \tag{9}$$

So, the total hiding capacity HC is given as the ration of total number of bits hidden B_{total} in the cover media and the total capacity available $C_{available}$, as given by Eq. (10) and Eq. (11).

$$HC = \frac{B_{total}}{C_{available}} \times 100 \tag{10}$$

$$HC = \frac{\sum_{k=1}^{N_S} B_k}{R \times C \times 8} \times 100 \tag{11}$$

where,
R is the number of rows in the cover image
C is the number of columns in the cover image

5 Key size

As each DCT coefficient have the capability to hide a maximum of 16 bits message in it. So, any number bits from 0 to 16 can be assigned to sector for hiding purpose. So, a total number of possible combinations K_{s_k} for a sector S_k is given by Eq. (12).

$$K_{S_k} = C_0^{16} \tag{12}$$

Now, as cover coefficients are classified in a total of N_s numbers of sectors, so the total key size K is given Eq. (13).

$$K = N_s \times C_0^{16} \tag{13}$$

6 Experimental results and analysis

VTVB steganography technique using IDIBS algorithm is used to hide different number bits in different DCT coefficients, depending on its distance from reference point. The cover image is transformed first to frequency domain using DCT. Then the DCT coefficients are classified in different sectors of equal size. As discuss in previous sections that the size

of a sector depends on the number of sectors. Each sector is allocated a number i.e. the number of bits to be substituted. As DCT coefficient in double format have a bits depth of 16. Therefore, the IDIBS algorithm can assign 0 to 16 bits to sector, and can used for data hiding. Here, different number of sectors and number of bits allocation is used for experimentation and the results are generated and demonstrated at appropriate place in the paper. For experimentation image of Leena is used as a cover media, as shown in Fig. 3.

Figure 3: Leena image used as cover image to hide secret information

Discrete cosine transform is applied to generate an array of DCT coefficients. IDIBS algorithm classifies the frequency components of cover image in different of sectors and a fixed number of message bits,but different for each sector, are hidden in each sectors coefficients. The experiments are performed for different number of sectors and the results are generated. The stego images for Sectors 2, 3, 4 and so on up to 17 are obtained and shown in Fig. 4.
The results obtained, show that VTVB steganography using IDIBS algorithm resulted in significant quality of stego images and no significant distortion has been created by the information hiding process.

a **b**

c **d**

e **f**

g

h

i

j

k

l

m **n**

o **p**

Figure 4: Stego images obtained after hiding secret information in Leena cover image using IDIBS Algorithm. The stego images are obtained using different number of sectors. The srego image generated using, (a) 2 number of sectors, (b) 3 number of sectors, (c) 4 number of sectors, (d) 5 number of sectors, (e) 6 number of sectors, (f) 7 number of sectors, (g) 8 number of sectors, (h) 9 number of sectors, (i) 10 number of sectors, (j) 11 number of sectors, (k) 12 number of sectors, (l) 13 number of sectors, (m) 14 number of sectors, (n) 15 number of sectors, (o) 16 number of sectors, (p) 17 number of sectors

Table 1: MSE,$PSNR$ and Hiding Capacity (HC) of IDIBS algorithm on Leena

Sr. No.	No. of Sectors (N_s)	Sector Size (W_s)	MSE (dB)	$PSNR$ (dB)	HC $(\%)$
1	2	$\left(\frac{R\times C}{2}\right)$	4.970	41.320	3.08
2	3	$\left(\frac{R\times C}{3}\right)$	5.390	40.820	6.15
3	4	$\left(\frac{R\times C}{4}\right)$	6.290	40.140	9.23
4	5	$\left(\frac{R\times C}{5}\right)$	7.840	39.180	12.31
5	6	$\left(\frac{R\times C}{6}\right)$	9.080	38.550	15.38
6	7	$\left(\frac{R\times C}{7}\right)$	9.380	38.400	18.46
7	8	$\left(\frac{R\times C}{8}\right)$	9.420	38.390	21.53
8	9	$\left(\frac{R\times C}{9}\right)$	9.450	38.377	24.61
9	10	$\left(\frac{R\times C}{10}\right)$	9.453	38.375	27.68
10	11	$\left(\frac{R\times C}{11}\right)$	10.220	38.036	30.76
11	12	$\left(\frac{R\times C}{12}\right)$	10.800	37.790	33.84
12	13	$\left(\frac{R\times C}{13}\right)$	11.000	37.720	36.92
13	14	$\left(\frac{R\times C}{14}\right)$	11.400	37.560	39.99
14	15	$\left(\frac{R\times C}{15}\right)$	11.850	37.390	43.07
15	16	$\left(\frac{R\times C}{16}\right)$	13.200	36.925	46.14
16	17	$\left(\frac{R\times C}{17}\right)$	33.180	32.920	49.22

The quality of stego images up to 13 number of sectors is very good and do not attract attention of human and changes are not detectable for human visual system HVS. While, increase in the number of sectors beyond 13, the distortion gets visually significant. Along with visual quality and the quality of stego images are calculated quantitatively using the measure of MSE and $PSNR$. The hiding capacity, MSE and $PSNR$ for each number of sectors.

To check and quantitatively analyze the performance of VTVB steganography implemented with IDIBS algorithm, two cover images i.e. Leena and House are used. The experimental results obtained for Leena as cover are Tab. 1. While, the results found for House image are mentioned in Tab. 2. The results show that hiding capacity HC and MSE increase with increase in numbers of sectors. While, $PSNR$, decreases with increase in the number sectors. The experimental results show that VTVB steganography using IDIBS algorithm can efficiently achieve a data hiding capacity HC of 43 % with image quality of 37.39 dB in term of $PSNR$. The hiding capacity HC and quality of stego image i.e. $PSNR$ can be controlled by changing the two factors i.e. number of sectors, the DCT coefficients are divided in and the number of LSB processed for hiding in each sector. This hiding technique can be, efficiently, used to embed any amount of data from 3 % to 43 % of cover image size with image quality of 41 dB to 37.39 dB.

In addition to high quality of stego images and significant hiding capacity, the presented technique has a large setgo key. The large key size further enhances the security of hidden

information. And in case the existence of hidden message is suspected, it is difficult to retrieve secret message exactly without a right stego key i.e. combination of bits hidden in each sector. Therefore, the proposed technique provide twofold security and can be a good choice for information hiding.

Table 2: MSE,$PSNR$ and Hiding Capacity (HC) of IDIBS algorithm on House

Sr. No.	No. of Sectors (N_s)	Sector Size (W_s)	MSE (dB)	$PSNR$ (dB)	HC $(\%)$
1	2	$\left(\frac{R\times C}{2}\right)$	4.970	41.320	3.08
2	3	$\left(\frac{R\times C}{3}\right)$	5.390	40.820	6.15
3	4	$\left(\frac{R\times C}{4}\right)$	6.290	40.140	9.23
4	5	$\left(\frac{R\times C}{5}\right)$	7.840	39.180	12.31
5	6	$\left(\frac{R\times C}{6}\right)$	9.080	38.550	15.38
6	7	$\left(\frac{R\times C}{7}\right)$	9.380	38.400	18.46
7	8	$\left(\frac{R\times C}{8}\right)$	9.420	38.390	21.53
8	9	$\left(\frac{R\times C}{9}\right)$	9.450	38.377	24.61
9	10	$\left(\frac{R\times C}{10}\right)$	9.453	38.375	27.68
10	11	$\left(\frac{R\times C}{11}\right)$	10.220	38.036	30.76
11	12	$\left(\frac{R\times C}{12}\right)$	10.800	37.790	33.84
12	13	$\left(\frac{R\times C}{13}\right)$	11.000	37.720	36.92
13	14	$\left(\frac{R\times C}{14}\right)$	11.400	37.560	39.99
14	15	$\left(\frac{R\times C}{15}\right)$	11.850	37.390	43.07
15	16	$\left(\frac{R\times C}{16}\right)$	13.200	36.925	46.14
16	17	$\left(\frac{R\times C}{17}\right)$	33.180	32.920	49.22

7 Conclusion

The proposed steganography technique is very secure two hide information. It provides twofold security, one by making the existence of hidden information undetectable and other the large stego key size make it difficult to retrieve the hidden information for an unauthorized person. The proposed technique changes the number of bits used for substitution on the basis of varying distance from the reference point. This is achieved by using IDIBS algorithm that decide the secret information distribution throughout the cover media. It has a high hiding capacity which can be varied by changing the number of sector and the number of bits assigned to a sector. At the same time it results in high visual quality of stego image. Hence, it keeps the existence undetectable to HVS. The technique is capable of hiding 3% to 43% information in cover image, while keeping stego image quality, in term of $PSNR$, in affordable range i.e. 41 dB to 37 dB.

References

Amirtharajan, R.; Rayappan, J. (2012): Inverted pattern in inverted time domain for icon steganography. *Information Technology Journal*, vol. 11, no. 5, pp. 587-595.

Bender, W.; Gruhl, D.; Morimoto, N.; Lu, A. (1996): Techniques for data hiding. *IBM Systems Journal*, vol. 35, no. 3,4, pp. 313-335.

Bhattacharyya, D.; Kim, T.; Dutta, P. (2012): A method of data hiding in audio signal. *Journal of the Chinese Institute of Engineers*, vol. 35, no. 5, pp. 523-528.

Chang, C.; Lin, C.; Tseng, C.; Tai, W. (2007): Reversible hiding in DCT-based compressed images. *Information Sciences*, vol. 177, no. 13, pp. 2768-2786.

Cheddad, A.; Condell, J.; Curran, K.; Mc Kevitt, P. (2010): Digital image steganography: Survey and analysis of current methods. *Signal Processing*, vol. 90, no. 3, pp. 727-752.

Dodis, Y. (2017): Basing cryptography on biometrics and other noisy data. *51st Annual Conference on Information Sciences and Systems*, pp. 1.

Ferguson, N.; Schneier, B. (1982): *Practical Cryptography*, volume 23. Wiley, New York.

Fridrich, J. (2009): *Steganography in Digital Media: Principles, Algorithms, and Applications*, vol. 1. Cambridge University Press, New York, USA.

Hussain, M.; Wahab, A.; Idris, Y.; Ho, A.; Jung, K. (2018): Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, vol. 65, pp. 46-66.

Jain, R.; Trivedi, M.; Tiwari, S. (2008): Digital audio watermarking: A survey. *Advances in Computer and Computational Sciences*, vol. 554, pp. 433-443.

Karabatak, M.; Yigit, Y. (2018): Developing lsb method using mask in colored images. *6th International Symposium on Digital Forensic and Security*, pp. 1-6.

Katzenbeisser, S.; Petitcolas, F. (2000): *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, London, UK.

Khan, S.; Ahmad, N.; Ismail, M.; Minallah, N.; Khan, T. (2015): A secure true edge based 4 least significant bits steganography. *International Conference on Emerging Technologies*, pp. 1-4.

Khan, S.; Ahmad, N.; Wahid, M. (2016): Varying index varying bits substitution algorithm for the implementation of vlsb steganography. *Journal of the Chinese Institute of Engineers*, vol. 39, no. 1, pp. 101-109.

Khan, S.; Khan, M.; Iqbal, S.; Shah, S.; Ahmad, N. (2013): Implementation of variable tone variable bits gray-scale image stegnography using discrete cosine transform. *Journal of Signal and Information Processing*, vol. 4, no. 4, pp. 343-350.

Khan, S.; Yousaf, M. (2013): 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, pp. 511-525.

Khan, S.; Yousaf, M.; Akram, M. (2011): Implementation of variable least significant bits stegnography using decreasing distance decreasing bits algorithm. *International Journal of Computer Science Issues*, vol. 8, no. 6, pp. 292-296.

Li, X.; Wang, J. (2007): A steganographic method based upon jpeg and particle swarm optimization algorithm. *Information Sciences*, vol. 177, no. 15, pp. 3099-3109.

Lin, Y. (2012): High capacity reversible data hiding scheme based upon discrete cosine transformation. *Journal of Systems and Software*, vol. 85, no. 10, pp. 2395-2404.

Lu, W.; He, L.; Yeung, Y.; Xue, Y.; Liu, H. et al. (2018): Secure binary image steganography based on fused distortion measurement. *IEEE Transactions on Circuits and Systems for Video Technology*, pp. 1-7.

Saha, S.; Ghosal, S.; Chakraborty, A.; Dhargupta, S.; Sarkar, R. et al. (2018): Improved exploiting modification direction-based steganography using dynamic weightage array. *Electronics Letters*, vol. 54, no. 8, pp. 498-500.

Schneier, B. (2007): *Applied Cryptography Protocols, Algorithm and Source Code*, vol. 2. Wiley, India.

Sharma, V.; Srivastava, D.; Mathur, P. (2018): Efficient i mage s teganography using graph signal processing. *IET Image Processing*, vol. 15, no. 6, pp. 1065-1071.

Stallings, W. (2010): *Cryptography and Network Security: Principles and Practice*, vol. 2. Prentice Hall Press.

Ulker, M.; Arslan, B. (2018): A novel secure model: Image steganography with logistic map and secret key. *6th International Symposium on Digital Forensic and Security*, pp. 1-5.

Xie, X.; Lin, C.; Chang, C. (2018): Data hiding based on a two-layer turtle shell matrix. *Symmetry*, vol. 10, no. 2, pp. 1-14.