 CMES, vol.118, no.3, pp.529-546, 2019

On Hiding Secret Information in Medium Frequency DCT Components Using Least Significant Bits Steganography

Sahib Khan[1], M A Irfan[1], Arslan Arif[1], Syed Tahir Hussain Rizvi[2], Asma Gul[3], Muhammad Naeem[4] and Nasir Ahmad[5]

Abstract: This work presents a new method of data hiding in digital images, in discrete cosine transform domain. The proposed method uses the least significant bits of the medium frequency components of the cover image for hiding the secret information, while the low and high frequency coefficients are kept unaltered. The unaltered low frequency DCT coefficients preserves the quality of the smooth region of the cover image, while no changes in the high DCT coefficient preserve the quality of the edges. As the medium frequency components have less contribution towards energy and image details, so the modification of these coefficients for data hiding results in high quality stego images. The distortion due to the changes in the medium frequency coefficients is insignificant to be detected by the human visual system. The proposed methods demonstrated a hiding capacity of 43.11% with the stego image quality of a peak signal to the noise ration of 36.3 dB, which is significantly higher than the threshold of 30 dB for a stego image quality. The proposed technique is immune to steganalysis and has proved to be highly secured against both spatial and DCT domain steganalysis techniques.

Keywords: DCT steganography, image processing, information security, data hiding, steganalyisis.

1 Introduction

A steganography technique embeds secret information in a digital cover medium (e.g., image, audio, or video), in such a way that its existence remain imperceivable and do not stir up an intruders' doubt. It is different from cryptography in the sense that in cryptography the message is encrypted, and the third person knows about the secret communication between two parties, but a decryption method is required to know what actually is communicated. It totally depends on the strength of encryption algorithm to prevent intruders

[1] Department of Electronics and Telecommunications, Politecnico di Torino, 10129 Torino, Italy.
[2] Department of Computer Engineering, University of Lahore, Pakistan.
[3] Department of Statistics, Shaheed Benazir Bhutto Women University Peshawar, Pakistan.
[4] Department of Computer Science, University of Peshawar, Pakistan.
[5] Department of Electronic and Electrical Engineering, Loughborough University, United Kingdom.
* Corresponding Author: Sahib Khan. Email: sahib.khan@polito.it.

from getting access to the messages exchanged between the sender and the desired receiver [Morsy, Nossair, Hamdy and Amer (2011)].

In steganography, the exchange of the message occurs in a manner such that an intruder cannot detect the exchange of secret communication other than sending and receiving of media files. To avoid an eavesdroppers' suspicion the least significant bits in the covering medium are used to hide the secret messages. The use of redundant bits transfers information without affecting the cover medium statistical properties [Giri and Bashir (2017); Wong, Qi and Tanaka (2017)]. The medium having high levels of redundant bits is considered most suitable for hiding secret messages and is always the preferred medium to be used by the steganographers.

The steganography can be performed either in the spatial domain or a suitable transformation of the image such as discrete cosine transform (DCT). In the spatial domain steganography techniques, the least significant bits (LSB) of the cover medium pixels are used directly to hide the secret messages [Wang, Ni, Zhang et al. (2017); Khan, Arif, Rizvi et al. 2018]. LSB steganography and 4LSB steganography are among the well-known spatial domain steganography methods. In variable least significant bits (VLSB) steganography, a different number of LSB of the cover pixels are used for hiding the secret message [Khan, Ismail, Khan et al. (2016)]. The VLSB steganography has been implemented using decreasing distance decreasing bits algorithm (DDDBA) [Khan, Yousaf and Akram (2011)], modular distance technique (MDT), and varying index varying bits substitution (VIVBS) [Khan, Ahmad and Wahid (2016); Khan and Tiziano (2018)].

In transform domain steganography, the secret message is hidden in the coefficients of transformed image instead of the image pixels directly. The Discrete cosine transforms (DCT) is one of the widely used transformed domain used by the steganographers. The method proposed in Hazra et al. [Hazra, Ghosh and Rahman (2018)], the secret message is hidden in the least significant bits of DCT transform coefficients. The work presented in Vleeschouwer et al. [Vleeschouwer, Delaigle and Macq (2001)], and Goljan et al. [Goljan, Fridrich and Du (2001)], proposed invertible steganography techniques in the transform domain. However, the reported hiding efficiency was very low and increase in hiding efficiency resulted in the severe degradation of the image quality. In Xuan et al. [Xuan, Zhu, Chen et al. (2002)], a steganography method with high hiding efficiency has been proposed using wavelet transform; however, the quality of the resultant stego image was very low. A variable data hiding method in the DCT domain is proposed in Khan et al. [Khan, Khan, Iqbal et al. (2013)].

The main goal of the steganography techniques is to keep the presence of hidden information unnoticed. The natural characteristic of the human visual system (HVS) is that it is much sensitive to distortions in the smooth areas of the image and less sensitive to those in the complex regions [Zhang and Wang (2005)]. DCT is a better classifier of the smooth and complex region in the image. The information about the smooth regions are captured in low frequency coefficients while those of the edges are captured in the high frequency coefficients [Qian, Wang and Qiao (2012); Chang, Lin, Tseng et al. (2007)]. Thus, keep in view the HVS characteristics, researchers prefer to use high frequency DCT coefficients

for data hiding while keeping the low frequency coefficients unaltered. However, data hiding in high frequency DCT coefficients affects the edges and results in blurring effect. To preserve the quality of a stego image, both the smooth areas and edges are important from the steganography point of view.
In this paper, a new data hiding technique is proposed which utilizes the medium frequency coefficients of DCT transform for data hiding. The proposed method divides DCT coefficients into three groups, i.e., low frequency coefficients, high frequency coefficients and medium frequency coefficients. The secret information is hidden in the LSB of medium frequency coefficients. The low and high frequency coefficients are left unaltered thus both the smooth and complex regions of the cover image are preserved. The results show that the technique provides high data hiding capacity with high quality stego images as compared to the other state of art techniques. The key contributions of this work includes good quality stego images, 100% recovery of the hidden message, high hiding capacity and significant evaluation metrics.
The rest of the paper is prearranged as follows. Section 2 describes the proposed data hiding technique. Section 3 presents the experimental results and discusses the robustness of the proposed technique to various steganalysis attacks. The comparison of the proposed technique with the state of art techniques is demonstrated in Section 4. The final Section 5, concludes the findings of this research.

2 Proposed technique

The main goal of steganography is to hide secret information in the cover media in a way that the data seems to be unchanged. In case of image steganography, the aim is to avoid such distortion in the images which can be detectable by the HVS. The proposed method attempts to achieve this goal by hiding the secret message in the image in such a way that both smooth and complex region of the cover images are least affected [Qian, Wang and Qiao (2012)]. For this purpose, the information relating to the smooth region, the intermediate region and complex region are de-correlated by taking the DCT of the cover image. The intermediate portion of the image is then utilized for hiding the secret information.
The main characteristics of DCT transform is the de-correction, i.e., DCT transform remove the interdependencies between the coefficients. DCT transform convert the cover image to an array of statistically independent coefficients, concentrating most of the energy in the top left coefficients and most details in bottom right coefficients. The top left coefficients have most of the energy and represent the smooth region of the image while, bottom right coefficients i.e., high frequency coefficients correspond to the edges. To preserve the edges and the overall view of the image, the high and low frequency coefficients are left unaltered and only the medium frequency coefficients are used for data hiding. The medfrequency coefficients consisting of the 50% central DCT coefficients are used for hiding secret information.
The data hiding process is divided into four steps: de-correlation of cover image data using DCT and segmentation of DCT coefficients into low, high and medium frequency com-

ponents; embedding secret information in the least significant bits of med-frequency coefficients; converting the modified DCT coefficients back to the spatial domain by taking inverse Discrete Cosine Transform (IDCT); and, calculating quality measuring parameters and hiding capacity.

2.1 De-correlation and segmentation

For hiding secret information in a cover image using the proposed technique, the image is converted to statistically independent coefficients by applying DCT transform. The DCT transform removes the interdependencies between coefficients and helps to get insight of the image's details such as edges, energy, etc. To get intermediate DCT coefficients extract, the desired region for data hiding, DCT has been used.
A cover image $C(i,j)$ of size $(M \times N)$, is subjected to DCT and results in an array of coefficients $C(u,v)$ of the same dimension $(M \times N)$. The calculation of DCT coefficients is done through the Eq. (1) given below [Cintra and Bayer (2011);Kim, Lee, Lee et al. (2018)].

$$C(u,v) = c(u)c(v) \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} CI(i,j) cos\left[\frac{\pi u\,(2i+1)}{2N}\right] cos\left[\frac{\pi v\,(2j+1)}{2M}\right] \tag{1}$$

where

$$c(u) \begin{cases} \frac{1}{\sqrt{2}} & if\ u = 0 \\ 1 & otherwise \end{cases} \tag{2}$$

and

$$c(v) \begin{cases} \frac{1}{\sqrt{2}} & if\ v = 0 \\ 1 & otherwise \end{cases} \tag{3}$$

The DCT arranges the frequency content of an image in order of their frequencies, from low to high. The first coefficient, also called DC coefficient, represents the average intensity of the image. The remaining coefficients are called AC coefficients. The low frequency components are concentrated in upper left corner of DCT coefficients array, while, high frequency components are placed at bottom right of the array. The medium frequency components are present in the mid-range of the DCT coefficients array. The DCT coefficients matrix obtained is converted into vector C_z of size $L = N \times M$, using the zigzag pattern in Eq. (4).

$$C_z = ZigZag\,(C) \tag{4}$$

where vector C_z is further divided into three sub-vectors of low frequency coefficients L_c, medium frequency coefficients M_c and high frequency coefficients H_c using Eq. (5), Eq. (6) and Eq. (7), respectively.

$$L_c = C_z\,(l) \text{ if } 1 \leqslant l \leqslant 0.25L \tag{5}$$

$$M_c = C_z\,(l) \text{ if } 0.25L < l \leqslant 0.75L \tag{6}$$

$$H_c = C_z\,(l) \text{ if } 0.75L < l \leqslant L \tag{7}$$

The hiding capacity of the proposed method depends on the number of coefficients selected for data hiding, while the quality of resulting image depends on the redundancy in least significant bits of the selected coefficients. Using more DCT components create more distortion and hence creates very significant artifacts in the stego images that attract the intruder attention. For good steganography techniques, the quality of stego image should be high 30 dB. On the other side the use of less number of medium frequency DCT coefficients will results in a decrease in hiding capacity. The tradeoff between hiding capacity and image quality was investigated in the proposed techniques, and it was found that using 50% medium frequency DCT components is the best choice as the quality of stego image degrades significantly above 50%.

2.2 LSB substitution

The medium frequency components vector obtained in the segmentation step is used for data hiding. The coefficients of the medium frequency components vector, i.e., M_c are subjected to LSB substitution one by one. The n least significant bits of each of the coefficients are replaced with n number of message bits. The number of substituted LSB i.e., n, determine the hiding efficiency and the distortion created in the stego image. Greater the number of bits n,higher the hiding capacity and more distortion. The modified medium frequency coefficients M_{cm} vector is obtained. The substitution operation is expressed as;

$$M_{mc}\,(k) = M_c\,(k) \circ m\,(k) \tag{8}$$

where $\circ$ represents the substitution operation and m(k) represent the message bits substituted in k_{th} medium frequency coefficient.

2.3 Inverse transformation

The modified stego vector obtained in LSB substitution step is combined with the unaffected low and high frequency coefficient vectors within their respective order to get the final stego vector S_v as given in Eq. (9).

$$S_v\,(l) = [L_c; M_c; H_c] \tag{9}$$

The stego vector is then converted into a stego matrix of DCT coefficients S of size $M \times N$ using the inverse zigzag process.

$$S = ZigZag^{-1}\,(S_v) \tag{10}$$

To get the final stego image, the modified DCT coefficients' matrix S is transformed back to the spatial domain by applying inverse discrete cosine transform (IDCT). The IDCT is given mathematically in Eq. (9) [Cintra and Bayer (2011); Kim, Lee, Lee et al. (2018)].

$$SI(i,j) = c(u)c(v) \sum_{u=0}^{N-1} \sum_{v=0}^{M-1} S(u,v) cos \left[\frac{\pi u\,(2i+1)}{2N}\right] cos \left[\frac{\pi v\,(2j+1)}{2M}\right] \tag{11}$$

where

$$i = 0, 1, 2, ..., N-1 \text{ and } j = 0, 1, 2, ..., M-1 \tag{12}$$

$$c(u) \begin{cases} \frac{1}{\sqrt{2}} & for\ u = 0 \\ 1 & otherwise \end{cases} \tag{13}$$

and

$$c(v) \begin{cases} \frac{1}{\sqrt{2}} & for\ v = 0 \\ 1 & otherwise \end{cases} \tag{14}$$

The final stego image SI with the embedded secret message is of the same size as that of cover image CI.

The Fig. 1, shows the implementation of the proposed data hiding technique. The processes of de-correlating DCT coefficients, extracting medium frequency components, hiding secret message in these components and obtaining resultant stego image are explained with the help of block diagram.

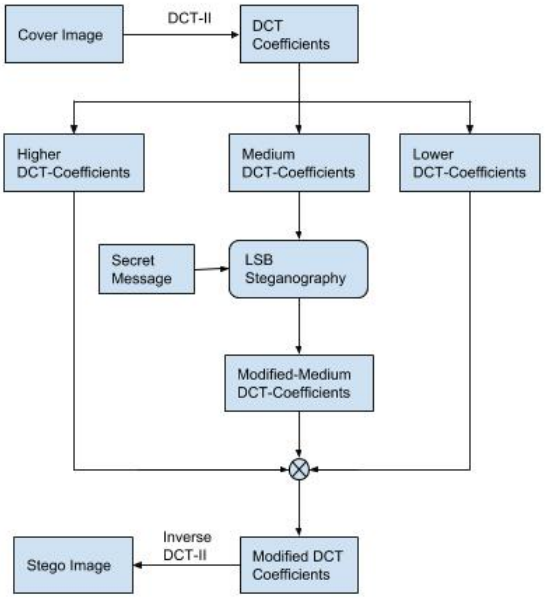


Figure 1: The process of hiding a secret message in the medium frequency components of the cover image

2.4 Message retrieval

After hiding a secret message in the least significant bits of medium frequency components the stego image can be stored or transmitted to send the hidden information to the intended receiver. The receiver, after receiving the stego image, will retrieve the hidden message

following the retrieval process.
To retrieve the hidden message, the stego image is transformed to DCT coefficients using DCT-II transform. As the secret message is hidden the LSB of the medium frequency components, therefore the medium frequency components are extracted from the array of coefficients. The hidden message is obtained by retrieving the LSB of the medium frequency components. The process of message retrieval is explained with the help of block diagram, shown in Fig. 2.

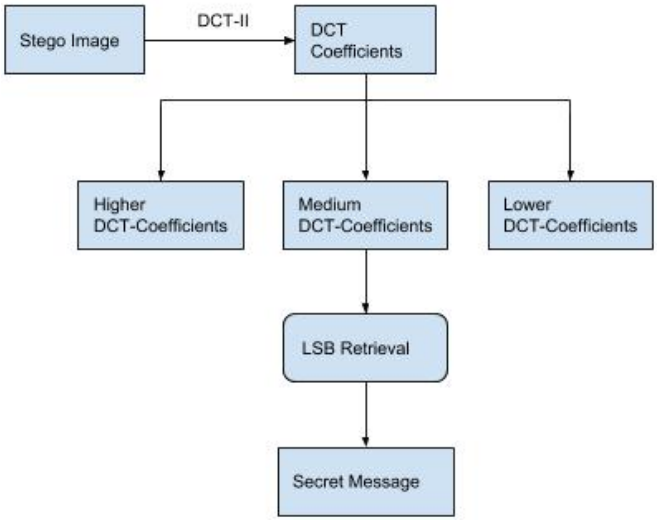


Figure 2: Retrieval of secret message

2.5 Hiding capacity

The hiding capacity is the ratio of the number of bits hidden to the number bits of the cover image and is expressed mathematically as in Eq. (15).

$$hc = \frac{Totalnumberbitshidden}{Totalnumberofbitsofcoverimage} \tag{15}$$

Lets n be the number of bits substituted in a single medium frequency coefficient and N_{mf} be the number of medium frequency coefficients selected for LSB substitution. As each DCT coefficient has 16 bits formation, so the hiding capacity in transform domain hc_t can be calculated as in Eq. (16).

$$hc_t = \frac{n \times N_{mf}}{16 \times N \times M} \times 100 \tag{16}$$

In the spatial domain, the gray scale image has a bit depth of 8 bits. So, the spatial domain hiding capacity hc_s is mathematically given by Eq. (17) as:

$$hc_s = \frac{n \times N_{mf}}{8 \times N \times M} \times 100 \tag{17}$$

The spatial domain hiding capacity is the effective hiding capacity and is directly proportional to the number of bits n hidden in a medium frequency coefficient and the number of medium frequency coefficient N_{mf}.

2.6 Evaluation measures

The quality of the stego image with respect to the original cover images, can be measured using different quality measuring parameters for example mean square error MSE, peak signal to noise ratio $PSNR$ and mean structure similarity index $MSSIM$ [Hore and Ziou (2010); Amirtharajan and Rayappan (2012)]. The MSE gives a measure of difference between the original image and the stego image. The zero MSE means no difference and both the images are perfectly same. In perspective of steganography, the MSE should be as minimum as possible. On the other side the $PSNR$, expressed in dB, gives measure closeness of the stego image to the original cover images. Higher the $PSNR$, closer the images are. However, it worth mentioning that $PSNR$ works for intensity comparison and it does not provide any structural information. Therefore, $MSSIM$ has been used as to take structural information in account and compare setgo image with cover image. The MSE, $PSNR$ and $MSSIM$ are mathematically expressed as:

$$MSE = \frac{1}{N \times M} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [SI(i,j) - CI(i,j)]^2 \tag{18}$$

$$PSNR = 10 \times \log_{10} \left(\frac{255^2}{MSE} \right) \tag{19}$$

$$SSIM = \frac{(2\mu_c\mu_s + C_1)(2\sigma_{sc} + C_2)}{(\mu_c^2\mu_s^2 + C_1)(\sigma_c^2 + \sigma_s^2 + C_2)} \tag{20}$$

where μ_c *the mean of cover image*
μ_s *the mean of stego image*
σ_c^2 *the variance of cover image*
σ_s^2 *the variance of stego image*
σ_{sc} *the covariance of the cover and stego images*
C_1 and C_2 *the variables to stabilize the division with weak denominator.*

3 Experimental results

The proposed method is tested by using different cover images taken from USC-SIPI image database [Wu, Han, Niu et al. (2018)], and other images taken using different cell phones. The results obtained for one cover image from the USC-SIPI image database, i.e., House, as shown in Fig. 1(a), are presented here. The image shown in Fig. 3(b), is used as a secret message. For complete message hiding, the message image is resized according to the hiding capacity. The image is first converted into a gray-scale image. The cover image data is de-correlated using DCT and the coefficients are segmented in low, medium and high frequency components as explained in Section 2. In these experiments, the first

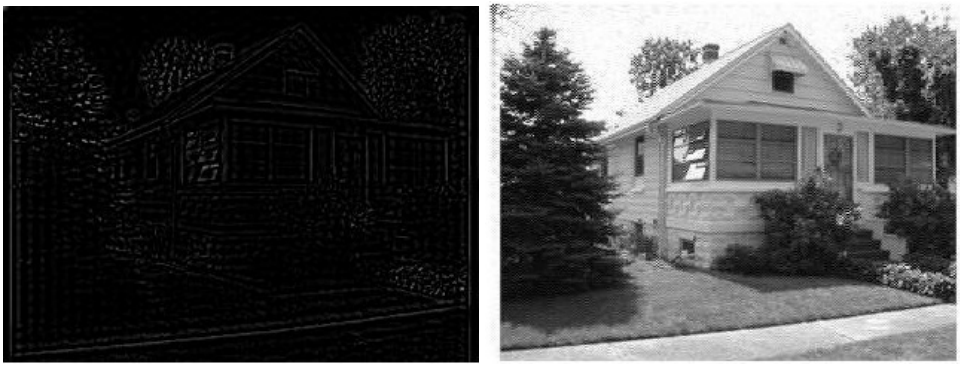
a **b**

Figure 3: Images used, (a) Cover Image, (b)The secret message

25% coefficients are labeled as low frequency coefficients and the last 25% coefficients are labeled as high frequency coefficients. The 50% coefficients in the middle are declared as medium frequency component.

The lower and high frequency coefficients are not subjected to data hiding. Because, hiding messages in the lower frequency coefficients create significant distortion. While, hiding messages in the high frequency coefficients affects the texture of the image. To experimentally check the effect of hiding in the lower and higher frequency components, secret messages are hidden in these coefficients separately. Only 3 least significant bits are used for embedding secret messages. The stego images obtained are shown in Fig. 4. It can be clearly observed that the resultant stego images are significantly distorted.

Experimentally, analysing the effect of data hiding in medium frequency coefficients, the



a **b**

Figure 4: Stego images of (a) 3 bits substitution in 25% lower frequency coefficients (b) 3 bits substitution in 25% higher frequency coefficients

medium frequency coefficients are subjected to data hiding process i.e., LSB substitution. A different number of least significant bits substitutions, ranging from 1 bit to 15 bits have been used in each coefficient of the medium frequency coefficients. The hiding capacity, MSE, $PSNR$ and $MSSIM$ are calculated for each case. The resultant stego images for 1 to 15 bits substitutions are shown in Fig. 5. The result shows that by hiding upto 12 bits data in each medium frequency DCT coefficient of the cover image, i.e., Fig. 5(a-l), the quality of the stego image is quite good. However, hiding more than 12 bits of data per coefficients i.e., Fig. 5(m, n, o), results in visually significant distortion.

a **b**

c **d**

e

f

g

h

i

j

k **l**

m **n**

o

Figure 5: Stego images of (a) 1 bit substitution, (b) 2 bits substitution, (c) 3 bits substitution, (d) 4 bits substitution, (e) 5 bits substitution, (f) 6 bits substitution, (g) 7 bits substitution, (h) 8 bits substitution, (i) 9 bits substitution, (j) 10 bits substitution, (k) 11 bits substitution, (l) 12 bits substitution, (m) 13 bits substitution, (n) 14 bits substitution, (o) 15 bits substitution

Figure 6: Retrieved secret message

In each of the experiment the secret message image Fig. 3(a), is resized to meet the hiding capacity. In this way the message is completely hidden in the cover image. However, in practice the case is differen and the message size may be larger or smaller than the hiding capacity. In the scenario of a large size message, the secret message is hidden in more than one cover image. While in the case of small size of secret message some coefficients are left unaffected. The proposed algorithm of data hiding has the property of reversibility and hidden message is recovered in its full strength. The secret message recovered from a stego image of 8 bits hiding is shown in Fig. 6.

The resultant hiding capacity, MSE, $PSNR$ and $MSSIM$ for a different number of LSB substitution are listed in Tab. 1. The results shown in Tab. 1 reveals that the hiding capacity and MSE increases with increasing the number of bits used for data hiding, while the $PNSR$ and $MSSIM$ decreases with increasing the number of hiding bits per coefficient. This is quite obvious because increasing the number bits used for data hiding the medium frequency coefficients of the cover image are modified more. Which helps to accommodate a larger number of secret message bits and also contribute to the distortion of the resultant stego image.

Steganalysis process tries to detect and retrieve the hidden data and/or tries to retrieve the hidden information. It is very important for a steganography technique to resist the steganalysis attacks. The results of different steganalysis attacks on the proposed technique are presented in this section. Some well know images such as Lena, Mandrill, Tiffany, Peppers, Jellybeans and others, from USC-SIPI image database were used [Wu, Han, Niu et al. (2018)]. The images were first converted to the gray-scale image of different format e.g., JPEG, PNG and BMP as a different steganalysis technique works on different formats only. These images were subjected to data hiding using the proposed technique. The setgo images are generated for 1 bit, 2 bits, 3 bits and so on up to 16 bits data hiding in the medium frequency components. All these images are tested for steganography using StegExpose [Boehm (2014)] and StegSecret [Muñoz (2015)] tools.

The StegExpose is a steganalysis tool, detecting LSB steganography. It analyses digital images in bulk and generates a comprehensive report for steganalysis experts. StegExpose

Table 1: Hiding capacity, $PSNR$, $MSSIM$ and MSE for different number of hiding bits using 50 % DCT coefficients

No. of Bits	DCT Domain Hiding Capacity "hc_t" (%)	Spatial Domain Hiding Capacity "hc_s"(%)	Hiding Capacity (*bpp*)	$PSNR$ (dB)	$MSSIM$	MSE
1	3.125	6.250	0.50	39.08	0.9671	8.045
2	6.25	12.500	1.00	39.08	0.9651	8.62
3	9.375	18.750	1.50	39.08	0.9606	9.79
4	12.500	25.000	0.00	39.08	0.9509	12.10
5	15.625	31.250	2.50	39.08	0.9394	15.15
6	18.750	37.500	3.00	39.08	0.9377	16.17
7	21.875	43.750	3.50	39.08	0.9377	16.21
8	25.000	50.000	4.00	39.08	0.9377	16.22
9	28.125	56.250	4.50	39.08	0.9380	16.18
10	31.250	62.50	5.00	39.08	0.9399	15.80
11	34.375	68.750	5.50	36.37	0.9439	15.00
12	37.500	75.000	6.00	36.80	0.9490	13.58
13	40.625	81.250	6.50	37.36	0.9467	11.95
14	43.750	87.500	7.00	36.30	0.9032	15.37
15	46.875	93.750	7.50	31.97	0.7536	41.22
16	50.00	100.000	8.00	29.58	0.5068	71.67

uses, on the other hand, not only detects steganography, but also determines the length of hidden message [Boehm (2014)]. First StegExpose is applied to a group of 391 images including 17 cover images and 17 stego images of each of the 1 bit, 2 bits, 3 bits and so on up to 16 bits data hiding. A steganalysis report is generated in the form of .CSV file. It was observed from the report that no steganography is detected in the stego images of 1 bit, 2 bits up to 14 bits data hiding. Only a few images were detected for 15 bits and 16 bits hiding. However, the 15 bits and 16 bits substitution also create significant visible distortion as shown in the previous section and these two combinations are not used for data hiding. However, the stego images of these two combinations are included to test the strength of the proposed methods. The result shows that steganography is even not detected in all stego images of these two combinations 15 bits and 16 bits stego images. The reason for the negative result may be due to the fact that the proposed technique is DCT coefficients based and is not a spatial domain LSB steganography technique, due to which the steganography is not detected.

To further test the strength of the proposed technique against steganalysis and another tool called StegSecret was used. StegSecret is a Java based, open source steganalysis project (GNU/GPL) is used to detect hidden information digital media. StegSecret is capable of detecting EOF, LSB, DCTs and other techniques [Muñoz (2015)]. The tool was applied to

the set of images including cover and stego images of JPEG and PNG formats and these experiments also resulted in negative and steganography is not detected even in a single case. The result is shown here in Fig. 7. The result shows that the proposed technique is immune not only to spatial domain steganalysis technique but also resistant to DCT domain techniques.

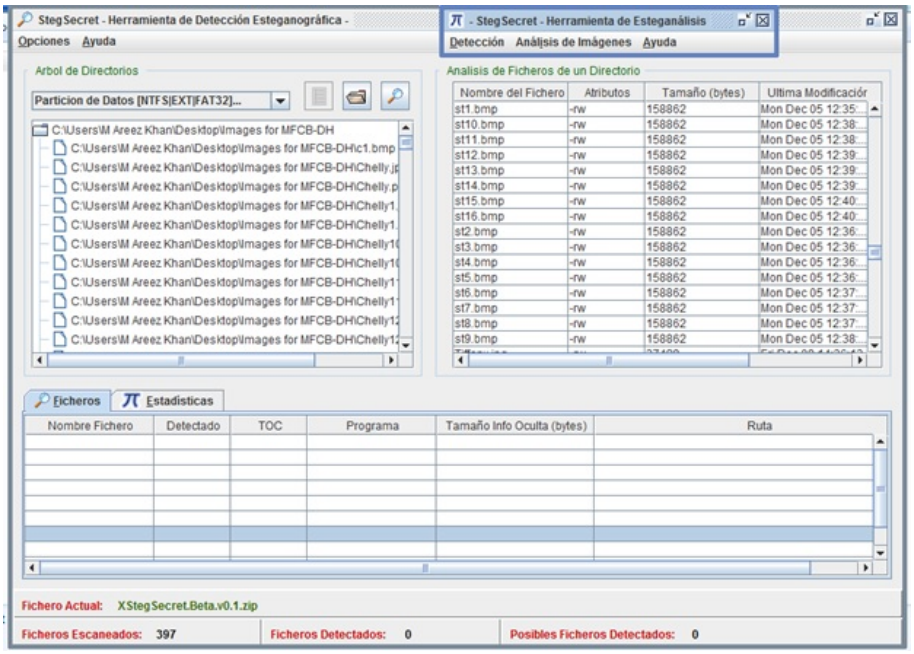


Figure 7: Steganalysis results of StegSecret

4 Comparison with other techniques

The main purpose of steganography is to ensure the secrecy of the secret information, and the selection of a suitable steganography technique plays the key role in achieving this goal. The steganography technique should be able to hide large amount of information in cover file without creating any visible artifacts imperceptible by an intruder. The overall performance of a steganography technique is measured by its hiding capacity and quality of resultant stego image.

The proposed data hiding technique is compared with state of the art technqiues.The hiding capacity and stego image quality of the proposed technique is compared with the previously reported steganography techniques and the results are shown in Tab. 2. From these results, it is evident that the hiding capacity of the proposed technique is higher than all these techniques. The proposed technique and the state of the art techniques are applied to a set of images from USC-SIPI image database [Wu, Han, Niu et al. (2018)] and average values

are reported for comparison. The experimental results obtained show that [Alam, Zakariya and Akhtar (2014)] results in the best quality stego images with a $PSNR = 51.098$, but the hiding capacity of this technique very low and is equal to 10.96% on the average. While, the proposed algorithm results in different values of hiding capacity depending on the choice of number of LSB used for substitution and also results in stego images. The proposed technique can achieve a hiding capacity of 87.5% with a $PSNR$ of resultant stego image equal to 36 dB, which is well above the required threshold of 30 dB.

Table 2: Hiding capacity, $PSNR$, $MSSIM$ and MSE for different number of hiding bits using 50 $\%$ DCT coefficients

Technique	$PSNR$ (dB)	Hiding Capacity (%)	Hiding Capacity (*bpp*)
Khan and Yousaf (2013)	27.26	50.00	4.00
Khan, Ahmad and Wahid (2016)	30.98	50.00	4.00
Khamrui and Mandal (2013)	44.78	3.80	0.3050
Chang, Lin, Tseng et al. (2007)	34.34	1.76	1.40
Alam, Zakariya and Akhtar (2014)	51.098	10.96	0.88
Wang, Wu, Tsai et al. (2008)	47.74	19.66	1.57
Lee and Chen (2010)	39.58	50.00	4.00
Proposed Technique	>36.30	87.50	7.00

5 Conclusion

The medium frequency coefficients based LSB image steganography technique proposed in this research uses the medium frequency coefficients of DCT domain representation of the image for data hiding. The technique preserves both, the edges and smooth areas of images as only the medium range coefficients of DCT are subjected to LSB substitution. It provides a hiding capacity of 0.5 bpp to 7 bpp with a reasonably high quality stego image with $PSNR$ ranging from 39.08 dB to 36.30 dB. The hiding capacity can be changed according to user needs by varying the number of bits used for LSB substitution or by changing the number of coefficients in medium frequency range. The variations created in stego image are not visually insignificant and can not be detected by HVS. The proposed technique gives quite high hiding capacity as compared to other steganography techniques. Moreover, the medium frequency coefficients based LSB image steganography technique is immune to steganalysis and shows significant resistance to staganalysis methods like Sample Pairs, RS Analysis, Chi Square Attack and Primary Sets attacks as well as EOP, LSB and DCT detection techniques.

References

Alam, S.; Zakariya, S.; Akhtar, N. (2014): Analysis of modified triple a steganography technique using fisher yates algorithm. *IEEE 14th International Conference on Hybrid Intelligent Systems*, pp. 207-212.

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

Boehm, B. (2014): Stegexpose-a tool for detecting lsb steganography. arxiv preprint arxiv:1410.6656.

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.

Cintra, R.; Bayer, F. (2011): A dct approximation for image compression. *IEEE Signal Processing Letters*, vol. 18, no. 10, pp. 579-582.

Giri, K.; Bashir, R. (2017): Digital watermarking: a potential solution for multimedia authentication. *Intelligent Techniques in Signal Processing for Multimedia Security*, vol. 660, pp. 93-112.

Goljan, M.; Fridrich, J.; Du, R. (2001): Distortion-free data embedding for images. *Lecture Notes in Computer Science*, vol. 2137, pp. 27-41.

Hazra, S.; Ghosh, S.; Rahman, H. (2018): Fpga implementation of semi-fragile reversible watermarking by histogram bin shifting in real time. *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 193-221.

Hore, A.; Ziou, D. (2010): Image quality metrics: Psnr vs. ssim. *IEEE 20th International Conference on Pattern Recognition*, pp. 2366-2369.

Khamrui, A.; Mandal, J. (2013): A genetic algorithm based steganography using discrete cosine transformation (gasdct). *Procedia Technology*, vol. 10, pp. 105-111.

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.; Arif, A.; Rizvi, S.; Ahmad, N. (2018): Increasing distance increasing bits substitution (idibs) algorithm for implementation of vtvb steganography. *Computer Modeling in Engineering & Sciences*, vol. 117, no. 1, pp. 1-16.

Khan, S.; Ismail, M.; Khan, T.; Ahmad, N. (2016): Enhanced stego block chaining (esbc) for low bandwidth channels. *Security Communication and Networks*, vol. 9, no. 18, pp. 6239-6247.

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.; Tiziano, B. (2018): Ant colony optimization (aco) based data hiding in image complex region. *International Journal of Electricaland Computer Engineering*, vol. 8, no. 1, pp. 379-389.

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.

Kim, K.; Lee, K.; Lee, H.; Joo, S.; Kang, J. (2018): An iterative sinogram gap-filling method with object-and scanner-dedicated discrete cosine transform (dct)-domain filters for high resolution pet scanners. *Japanese Journal of Radiology*, vol. 36, no. 1, pp. 59-67.

Lee, C.; Chen, H. (2010): A novel data hiding scheme based on modulus function. *Journal of Systems and Software*, vol. 83, no. 5, pp. 832-843.

Morsy, H.; Nossair, Z.; Hamdy, A.; Amer, F. (2011): Utilizing image block properties to embed data in the dct coefficients with minimum mse. *International Journal of Computer and Electrical Engineering*, vol. 3, no. 3, pp. 449-453.

Muñoz, A. (2015): Stegsecret. a simple steganalysis tool. *Stegsecret. Sourceforge. Net*.

Qian, Z.; Wang, W.; Qiao, T. (2012): An edge detection method in dct domain. *Procedia Engineering*, vol. 29, pp. 344-348.

Vleeschouwer, C.; Delaigle, J.; Macq, B. (2001): Circular interpretation of histogram for reversible watermarking. *Proceedings of the IEEE 4th Workshop on Multimedia Signal Processing*, pp. 345-350.

Wang, C.; Wu, N.; Tsai, C.; Hwang, M. (2008): A high quality steganographic method with pixel-value differencing and modulus function. *Journal of Systems and Software*, vol. 81, no. 1, pp. 150-158.

Wang, J.; Ni, J.; Zhang, X.; Shi, Y. (2017): Rate and distortion optimization for reversible data hiding using multiple histogram shifting. *IEEE Transactions on Cybernetics*, vol. 47, no. 2, pp. 315-326.

Wong, K.; Qi, X.; Tanaka, K. (2017): A dct-based mod4 steganographic method. *Signal Processing*, vol. 87, no. 6, pp. 1251-1263.

Wu, X.; Han, Q.; Niu, X.; Zhang, H.; Yiu, S.; et al. (2018): Jpeg image width estimation for file carving. *IET Image Processing*, vol. 12, no. 7, pp. 1245-1252.

Xuan, G.; Zhu, J.; Chen, J.; Shi, Y.; Ni, Z.; et al. (2002): Distortionless data hiding based on integer wavelet transform. *Electronics Letters*, vol. 38, no. 25, pp. 1646-1648.

Zhang, X.; Wang, S. (2005): Steganography using multiple-base notational system and human vision sensitivity. *Signal Processing Letters*, vol. 12, no. 1, pp. 67-70.