A New Algorithm for Less Distortion and High Capacity Steganography Model Using Blocks-Based Method

Salah Mahdi Saleh* & Wathiq L. Abd Ali**

Received on: 7/2/2009
Accepted on: 11/3/2010

Abstract

Most steganography methods suffer from many problems that effect on their efficiency and performance. Some of these are the capacity of cover media, the distortion of cover media, and etc. In this paper we are proposed a new method to hide audio file (WAV format) in image (BMP format) that overcomes most of these problems. Also the proposed method aims to meet most the requirements of any steganography system (like capacity, security and undetectability). It depends on finding the similarity between the embedded data blocks and others in the cover-image. It can be used as a powerful tool to get a high capacity data embedding and a less distortion stego-image, where the PSNR for the stego-image is large.

Keywords: Steganography; Information hiding; Capacity; Security; Block-based.

خوارزمية جديدة لنموذج إخفاء ذو تشوه قليل وسعة عالية باستعمال طريقة القطاعات المتشابهة

الخلاصة

تعاني معظم طرائق إخفاء المعلومات من عدة مشاكل تؤثر على كفاءتها وأدائها. وبعض هذه المشاكل هي سعة الوسط الغطاء وتشويهه، الخ. اقترحنا في هذا البحث طريقة جديدة لإخفاء ملف صوت (بهيئة WAV) في ملف صورة (بهيئة BMP) تتجاوز معظم تلك المشاكل. كما تحاول تلبية متطلبات أي نظام تشفير مثل (السعة، السرية وعدم القدرة على الاكتشاف). وهي تعتمد على إيجاد التشابه بين قطاعات البيانات المراد إخفاءها وتلك الموجودة في الصورة الغطاء. إذ يمكن أن تستعمل هذه الآلية كأداة قادرة على الحصول على إخفاء بسعة كبيرة مع تشوه قليل أو معدوم في الصورة الغطاء، إذ كانت قيم PSNR لصورة الإخفاء عالية.

1-Introduction

Steganography is a means of storing information in a way that hides information's existence. Steganography contains the techniques for secret hiding of messages in another wise innocent looking carrier message. The purpose of steganography is not to keep others from knowing the hidden information, but is to keep others from thinking that the information even exists [1]. Therefore, the main goal is to not raise suspicion and avoid introducing statistically detectable modifications into the

***Sciences for Women College, Babylon University/ Babylon.**
**** Technical Institute of Kerbalaa/ Kerbalaa.**

https://doi.org/10.30684/etj.28.13.7
2412-0758/University of Technology-Iraq, Baghdad, Iraq

carrier media [2][3][4].Historically, the first steganography techniques included invisible writing using special inks or chemical[5]. Today, it seems natural to use digital images, digital video or audio for hiding secret message[6]. Steganography, like watermarking and fingerprinting, is a branch of information hiding. Unlike watermarking and fingerprinting, steganography imposes the requirement that the presence of a hidden message within the stegotext (transmitted data) should be undetectable [7]. One of the most common uses of modern steganography in digital world of computers is to hide information from one file in the contents of another file [8][9].Most steganography methods suffer from many problems (or impose constraints), make the results of its failure against steganalysis. One of the limitations of steganography is the one-to-one relationship between an embedded and cover file [10]: to hide one byte of covert data requires one byte of overt data. The amount of data that can be effectively hidden in a given medium tends to be restricted by the size of the medium itself [1]. The common well-known steganographic method is the least significant bits (LSBs) substitution [11].Many public steganographical software , such as S-Tools , EZstego and Steganos apply this method [12]. In this method there is a limit for the number of substituted bits [13](the maximum depth of LSB insertion is 4-LSB [14]).

Images are a good media for hiding data and have the lenient constraints [1]. This media have many problems when it used in steganography as a cover. One common drawback of virtually current data embedding methods is the fact that the original image is inevitably distorted by some small amount of noise due to data embedding itself [15]. Another problem, we did not have to change all of the LSB's (underlined), which means that on average 50% of the pixels of an image will not be affected by embedding (the embedding capacity is 50% of the cover-image size). The problem above appear when LSB's insertion is used [8][14]. Third, is that the limitation on the available colors imposed by the finite palette makes the process of message hiding a difficult challenge (the order of the palette will change after embedding) [6].This paper has been attempted to solve these problems and aim to satisfy the requirements of steganography system (capacity, security and undetectability). A new, simple, and secure method has been proposed which splitting the secret message and cover media into blocks, to maximize the capacity of cover media and simplifying the limits on the size of secret massage. Also guarantees best restoration for the secret message and creating less distortion stego-media to meet the main goal of steganography. The rest of this paper is organized as follows. The new scheme is presented in Section 2. Implementation results are in Section 3. Conclusions are drawn in Section 4.

2-The proposed algorithm

Most researches are concerned on the LSB method for data hiding.

This method, as explain previously, have many problems that effect on the performance of the embedding method. For this and to get a secure embedding, we proposed a new method that hiding audio file with WAV format in a BMP image file by using a similar blocks between the cover image and embedded audio. It's overcome LSB's problems and aiming to satisfy most the requirements of steganography system, especially the two main aspects (security and capacity), that affecting on the steganography and its usefulness. The block diagram in figure 1 describes the proposed method.

First, the algorithm starts with dividing the data of audio file into separated blocks with size (N×N) bytes for each. It has been used different size for block in each experiment and comparing the results. However, the size of block effects on the restored audio and the length of secret key. Whereas the cover-image is divided into overlapped blocks with the same size in order to get large capacity. Then, the number of audio's blocks has been reduced, one block from many similar block seeks at a time and the another blocks take the same result as of that block, in order to reduce the time of search and to modify the relation one to one into multi to one relation by indicating to many similar blocks using one block.

In second step, the similarity between each embedded audio's block and all blocks of the cover-image has been experimented using the following equation:

$$f(S_i) = \left| \sum_{j=1}^{nb} S_i - B_j \right| \quad \ldots.(1)$$

where S_i and B_j represent the *ith* and *jth* audio's block and image's block, respectively, and nb represents the numbers of blocks in cover-image. Then select the near (less absolute difference) and store its number (meaning j) in a separate file. This separated file represents a key sequence (secret key) for a stego-image ,and without it can't restoring the embedded audio. There is some notes about the key sequence, ones is that the length of this key depends on the size of block, and as a result the number of blocks in the audio file. However, where the number of blocks are large, then the length of key will be large too. Second, from the other hand, if the length of key be large, the restored message will be good, and vice versa. The next scheme describe the embedding algorithm:

Embedding Algorithm

Input : The cover-image and the embedding audio message.

Output :The stego-image and secret key.

Step1: Select the embedded-audio and the cover-image.

Step2: Split the embedded-audio and the cover-image into blocks with size (N*N).

Step3: For I=1 to no. of embedded-audio blocks, do

-Select emb-block[I] from embedded-audio blocks.

-For J=1 to no. of cover-image blocks, do

-Select cover-blocks[J] and perform equation

(1) , search for less absolute difference.
End for

-Save the block number in a file (key file).

End for

Step4: End.

For the header part of audio file, it is embedded in the forth column of color table (palette table) of stego-image. This part of color table provides 256 free bytes.

In the stage of extraction, every block of audio is extracted from the stego-image depending on the positions that stored in the separated file (the key file) which is transmit independently from stego-image. The receiver cannot able to extract the embedded-image without know the embedded positions, therefore this method is more secure. The next scheme describe the extracting algorithm :

Extracting Algorithm

Input: The stego-image, the key file and block size.

Output: The embedded-audio.

Step1: Extract the embedded header of audio from palette table of the stego-image.

Step2: For I=1 to no. of embedded-audio blocks , do

-From the key file get the position I.

-Extract the emb-block[I] from the stego-block[position I].

End for

Step3: End.

3-The results

To stand on the performance of the proposed method, two different audio files with different sizes are applied. Also, we are used color images with 8 bits/pixel. The method emphases in selecting the audio files that its sizes larger than the image files in all experiments in order to explain how the proposed method have high-capacity feature. We are used subject and object criteria as measures of stego-image and restored message quality. In object criteria, the following formulas are used :

i) Root mean square error (**RMSE**[*]).

$$RMSE = \sqrt{\frac{\sum_{r=0}^{M-1}\sum_{c=0}^{N-1}\left[\hat{I}(r,c) - I(r,c)\right]^2}{(M \times N)}} \quad .....(2)$$

ii) Peak signal to noise ratio (**PSNR**[*]): Here we are used two different formulas, one for images as following:

$$PSNR = 10\log_{10}\frac{(L-1)^2}{\frac{1}{M\times N}\sum_{r=0}^{M-1}\sum_{c=0}^{N-1}\left[\hat{I}(r,c) - I(r,c)\right]^2} \quad .....(3)$$

where L represent the number of gray levels, $\hat{I}$ is the stego-image, and I is cover-image with size (MxN). Whereas, for measuring the quality of restored

audio, the following PSNR** formula is used:

$$PSNR = 10\log_{10} \frac{\sum_n x^2(n)}{\sum_n [x(n) - y(n)]^2} \quad ...(4)$$

where x(n) represent sample of embedded audio sequence and y(n) stand for sample of restored audio sequence.

3-1: Satisfying the requirements of capacity, and undetectability.

In this experiment we attempt to embed an audio message its size larger than the cover image. We have been tested the proposed method on a number of color images (**8 bits/pixel**) with size (**128x128**), to embed an audio message its size (**17.8 KB**). The embedding capacity approximately **104%.** The size of block that used here is (1x1). The **RMSE** and **PSNR** values for restored audio message are given in table (1).

It can be seen from table 1 that the proposed algorithm with generally higher **PSNR** values for restored audio message. This indicates that the restored audio file is semi to the origin. Here we don't substituted the similar blocks in order to make the stego-image without distortion. The 4th column in table (1) represents the maximum error between two blocks resulting from equation (1).

*: S. E. Umbaugh. Computer Vision and Image Processing: A Practical Approach Using CVIPtools, Prentice Hall PTR, USA, 1998.

**: Reference [13].

Also, we can substitute the similar blocks in order to guarantee best (**full**) restoration for audio message. The table 2 shows the results of **RMSE** and **PSNR** between the cover-images and stego-images.

It can be seen from table 2 that the proposed algorithm with generally higher **PSNR** values for stego-images. In such case, the embedding message is totally incorporated into cover-image. This indicates that all images less distortion, and the attacker (steganalysis) can't easily detects the embedded message. This makes the mission of the attacker is more difficult. The cover-images and stego-images of the tables 1 and 2 appear in appendix (A). When we see the images in appendix A and analysis the results of **RMSE** and **PSNR** in table (2), can be concluded from the viewpoint of human vision system (HVS) that the PSNR values of cover-images and stego-images it's acceptable and the distortions are imperceptibility to human vision. It means such distortions will be less noticeable from the viewpoint of attacker.

3-2: Effecting the increase size of Message.

In this experiment we attempt to embed an audio message its size larger than in previous test to explain the power of the proposed method from the view point of capacity. We have been tested the proposed method, on a number of color images (**8 bits/pixel**) with size (**128x128**), to embed an audio message with size (**18.8 KB**). The embedding capacity approximately **110%.** The size of block is (**1x1**). Table (3) gives the

values of **RMSE** and **PSNR** for the restored audio message.

It can be seen from table 3 that the proposed algorithm with generally higher **RMSE** and **PSNR** values. This indicate that the restored audio file is fully or semi to the origin. Here, the similar blocks aren't substituted in order to make the stego-image without distortion.

Also, in the following, the similar blocks can be substituted in order to guarantee best (**full**) restoration for audio message. The table 4 shows the results of **RMSE** and **PSNR** between the cover-images and the stego-images.

It can be seen from table 4 that the proposed algorithm with generally good **RMSE** and **PSNR** values for stego-image. This indicates that all image less or without distortion, and the steganalysis (attacker) can't easily detects the embedded message. This makes him mission more difficult. It can be concluded from this experiment that the increased size doesn't affect on the quality of images and still imperceptibility. You can see the cover-images and stego-images for tables 3 and 4 in appendix (B).

3-3: Explain the relation between block size and key length

In this experiment we will explain the previous notes about the relation between the block size and the length of secret key. First, the audio file that used in experiment 3.1 has been embedded in some color images that are tested in the same experiment with a block size (2x2). The **RMSE** and **PSNR** values for the restored audio message are given in table 5 without substituting between blocks.

Note from the above table that the values of **RMSE** and **PSNR** for the restored audio have been downgraded when we are comparing them with that in table 1. This indicates that if we using enlarge block size the ratio of errors between the original and restored audio massage was larger than a small block size which used in experiment 3.1. In the following table we explain the results of **RMSE** and **PSNR** between the cover-image and stego-image, also between the origin and restored audio message with substituting between the similar blocks for the same experiment.

We can see from the results in tables 5 and 6, and when it have been compared with the results of tables 1 and 2, that the restored audio massage quality have downgraded. For the length of key sequence her, its approximately quarter than in experiment 3.1. You can see the cover-images and stego-images for tables 5 and 6 in appendix (C).

Now, In the following experiment we have been embedded the audio file that used in experiment 3.2 in some color images that are tested in the same experiment with a block size (2x2). The **RMSE** and **PSNR** values for the restored audio message are given in table 7 without substituting between blocks.

We note from the above table that the values of **RMSE** and **PSNR** for the restored audio have been downgraded when we are comparing them with that in table 3 for experiment 3.2. In the following table we explain the result with

substituting between the similar blocks for the same experiment.

You can see the cover-images and stego-images for tables 7 and 8 in appendix (D). For the length of key sequence her is approximately quarter than in experiment 3.2.The experiment 3.3 support what we were said previously about relation between the key length and block size. We find that, if we have been used a block with large size, the quality of restored message and the stego-image will be downgrad. This is because the large size of block have a large amount of error .Another reason for that as a result to split the cover-image into group of nested blocks, to maximize its capacity by increasing the number of blocks in image, this nested blocks may be affecting on each other.

3-4: Comparison between the proposed method and that in reference [14].

Note the table 9 shown below. The RMSE and PSNR are calculated for stego-image at embedding audio message of size (**135 KB**) in 'maraho.bmp' image with size 512 × 512 using our algorithm. We can see that the RMSE is 0 (meaning stego-image without distortion). If we further look at this result in details and then compare it with the results that produced from the LSB algorithm, which is consider a blocked method with a block size $1\times1^{*}$, that used in reference [14] to hide message with maximum capacity (1043351). We found that the PSNR and RMSE evaluated in [14] is less than our algorithm when using the same cover-image with large embedded capacity. You can see from table 9 that our algorithm performance stills best when we embedded large message in cover-image and the message imperceptible as we can conclude from the high values of PSNR. The cover-image and stego-images for this experiment are illustrated in appendix E.

*:Y. Wang and P. Moulin. Steganalysis of Block-Structured Stegotext. Proceedings of SPIE, Vol. 5306, pp. 477-488, 2004.

4-Conclusions

These paper emphases on applying most the requirements of any success steganography system like (capacity, invisibility, security, and undetectability) and advanced the relation of one to one.

The process of finding the similarity between two blocks give as the ability to hide data its size larger than the cover data. It can using one block to indicate many similar blocks. Thus, we can hide a message its size larger than the size of cover-media and make the size of message less limited in some size. At this point, here is the powerful of the proposed method by increasing the capacity of cover-media and reducing the limits of size that facing most data hiding techniques. We find from experiments 3.1 and 3.2 that the increased size of message have no much effects on the quality of stego-image and still imperceptible. Also, when the embedding stage is completed, the stego-image less distortion or distortion-free depending on the values of **RMSE** and **PSNR** as we see in tables (1,2,3 and 4), respectively. This is because the changes in the values of data of cover-image is not found or not perceptual and the quality of stego-

image still good as we see in appendixes A and B, respectively. These results will reflect on the ability of human visual system. Other, its best or more best when its compared with the results of methods that have been used in the references [14] and [15]. This point will reflect on the steganalysis, and makes the process of analyzing the produced steganography very difficult.For the security requirement, the algorithm produces a sequence of secret key that send independently to increase the difficulty of steganalysis on these stego-images. The receiver can extract the embedded message by using that secret key only. The size of block is also an important issue, because the effect of size will be reflect on the invisible and undetectable requirements and the restoration process. If the size of block is large then the length of sequence of secret key is small and need less computation effort for transmit. From the other hand, the quality of restored audio will be affect comparison with the origin audio because the amount of errors will be increase, and vice versa. The results in tables 5,6,7 and 8 support the previous sentence. You can see the appendixes C and D to be sure and comparing them with the appendixes A and B, respectively. Finally, By using the proposed method, the relation one to one between the embedded and cover data becomes multi to one. So we can hide many blocks in a single block by finding the similarity.

References

[1] D. Artz. Digital Steganography :Hiding Data within Data. IEEE INTERNET COMPUTING, Vol. 5, No. 3, pp. 75-80, MAY/JUNE, 2001.

[2] S. Lyu and H. Farid. Steganalysis Using Higher-Order Image Statistics. IEEE Transactions on Information Forensics and Security, Vol. 1, No. 1, pp. 111-119, March, 2006.

[3] J.A. Memon, K. Khowaja and H. Kazi. Evaluation of Steganography for URDU/ARABIC Text. Journal of Theoretical and Applied Information Technology, Vol. 4, No. 3, March, 2008.

[4] S. Katzenbeisser and F. A. P. Petitcolas. Defining Security in Steganographic Systems. Proceedings of Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, Vol. 4675, pp. 50-56, San Jose, CA, USA, 21-24 January, 2002.

[5] D. Kahn. The history of steganography. Proceedings of the first Workshop on Information Hiding, Lecture Notes In Computer Science, Vol. 1174, pp. 1-5, 30 May – 1 June, Cambridge, UK, 1996.

[6] J. Fridrich. A New Steganographic Method for Palette–Based Images. Proceedings of the IS&TPICS conference, pp. 285-289, April, Savannah, Georgia (1998).

[7] P.Moulin and Y. Wang. New Results on Steganographic Capacity. Proc. Conference on Information sciences and systems, pp. 813-818, Princeton, NJ, March, 2004.

[8] K. Rabah. Steganography –The Art of Hiding Data. Information

Technology Journal 3(3), pp. 245-269 , 2004 .

[9] M. A. B. Younis and A. Janta. A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion. International Journal of computer science and network security, vol.8, no.6, June 2008.

[10] E. Cole. HIDING IN PLAIN SIGHT: Steganography and the Art of Covert Communication. Wiley Publishing, Inc. USA. 2003.

[11] C.C. Chang and H.W. Tseng. A steganographic method for digital images using side match. Pattern Recognition Letters, Vol. 25, pp. 1431-1437, 2004.

[12] X. Luo, F. Liu and P. Lu. A LSB STEGANOGRAPHY APPROACH AGAINST PIXELS SAMPLE PAIRS STEGANALYSIS. International Journal of Innovative Computing, Information and Control, Vol. 3, No. 3, pp. 575-588, June 2007.

[13] N. Cvejic and T. Seppanen. Increasing Robustness of LSB Audio steganography using a Novel Embedding Method. Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04), 2004.

[14] Y. K. Lee and L. H. Chen. High capacity image steganography model. IEEE Proceedings on Vision, Image and Signal Processing, 147(3), pp. 288-294, June 2000.

[15] M. Goljan, J. Fridrich and D. Rui. Distortion-Free Data Embedding for mages. Proceedings of the 4th International Workshop on

Table (1): The results of RMSE and PSNR for the restored audio massage.

Image	RMSE (audio)	PSNR (audio)	Max error
lenna	0.097	103.248	1
baboon	0.22	98.341	2
tree	0.153	101.497	1

Table 2: The results of RMSE and PSNR for the stego-images when substituting the blocks

Image	RMSE (image)	PSNR (image)	Max error
lenna	0.017	83.285	1
baboon	0.033	77.722	2
tree	0.023	80.733	1

Table 3: The results of RMSE and PSNR for the restored audio massage.

Image	RMSE (audio)	PSNR (audio)	Max error
lenna	0.057	109.855	1
baboon	0.363	93.820	2
tree	0.109	104.250	1

Table 4: The results of RMSE and PSNR for the stego-images when substitutes the blocks.

Image	RMSE (image)	PSNR (image)	Max error
lenna	0.014	85.504	1
baboon	0.032	77.971	2
tree	0.019	82.493	1

Table 5: The results of RMSE and PSNR for the restored audio massage that with a block size(2x2).

Image	RMSE (audio)	PSNR (audio)	Max error
lenna	39.862	55.677	121
baboon	29.818	55.689	103
Tree	30.144	55.595	163

Table 6: The results of RMSE and PSNR for the restored audio massage and stego-images with a block size(2x2).

Cover Image	Stego-image		Restored audio	
	RMSE	PSNR	RMSE	PSNR
lenna	1.823	42.914	30.393	55.523
baboon	1.752	43.262	30.415	55.517
Tree	1.545	44.352	30.282	55.555

Table 7: The results of RMSE and PSNR for the restored audio massage

Image	RMSE (audio)	PSNR (audio)	Max error
lenna	27.277	56.291	178
baboon	25.943	56.726	197
Tree	25.516	56.870	240

Table 8: The results of RMSE and PSNR for the restored audio massage and stego-images with a block size (2x2).

Cover Image	Stego-image		Restored audio	
	RMSE	PSNR	RMSE	PSNR
lenna	1.386	45.294	26.116	56.668
Baboon	1.389	45.280	25.993	56.709
Tree	1.150	46.750	26.161	56.654

Table 9: comparison between the proposed method and that used in the reference [14] with a block size (1×1).

Embedded method	RMSE (stego-image)	PSNR (stego-image)
modified LSB in reference [10]	6.02	32.57
Proposed Method with block size (1×1)	0	#*
Proposed Method with block size (2×2)	0.521	53.799

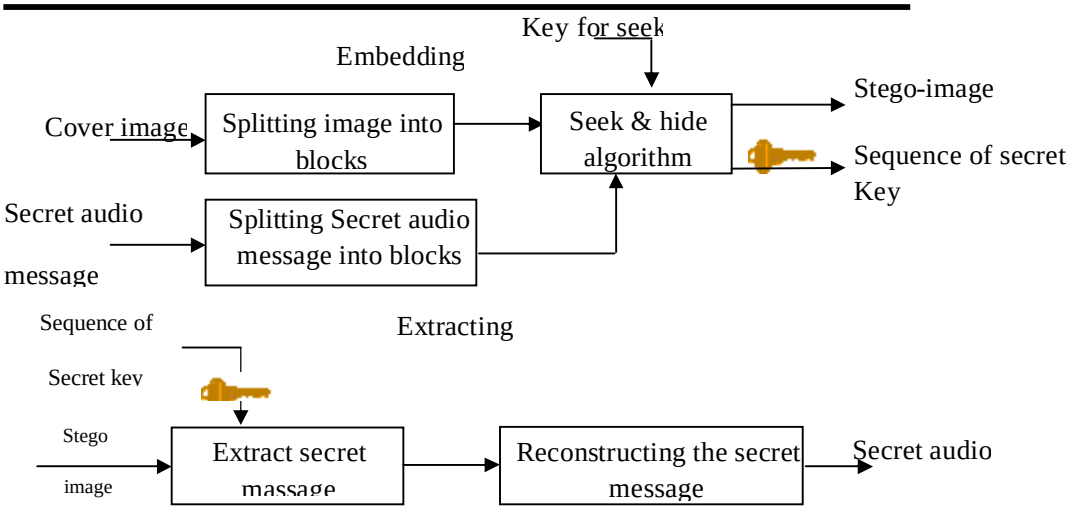
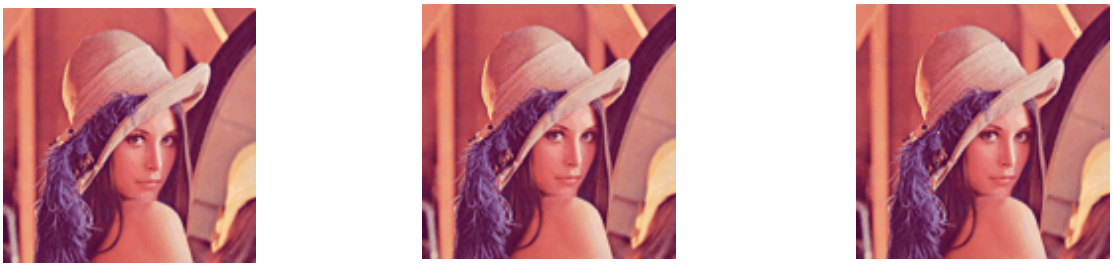


Figure (1): Block diagram of proposed audio embedding and extracting algorithm

Appendix A



(a) (b) (c)

Figure (2): Lenna image (a) cover-image, (b) stego-image without substitution, (c) stego-image with substitution

(a) (b) (c)

Figure (3): baboon image (a) cover-image, (b) stego-image without substitution, (c) stego-image with substitution

(a) (b) (c)

Figure (4): Tree image (a) cover-image, (b) stego-image without substitution, (c) stego-image with substitution

Appendix B

(a) (b) (c)

Figure (5): lenna image (a) cover–image, (b) stego-image without substitution, (c) stego-image with substitution

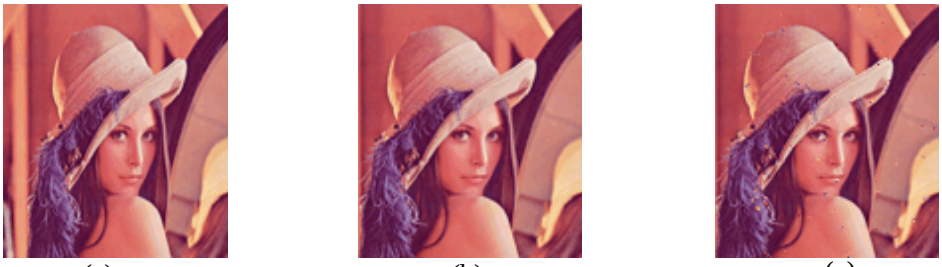
(a) (b) (c)

Figure (6): baboon image (a) cover-image, (b) stego-image without substitution, (c) stego-image with substitution

(a) (b) (c)

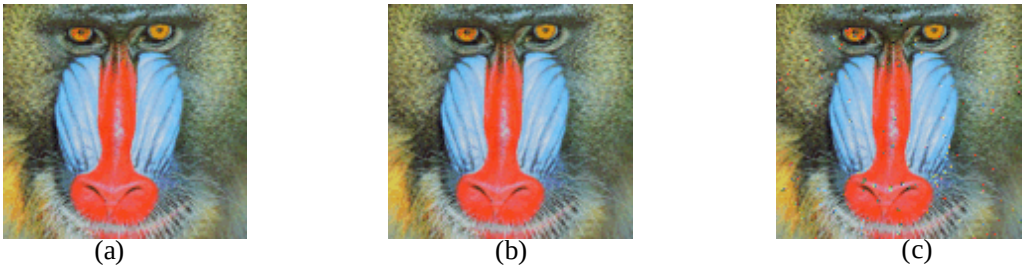
Figure (7): tree image (a) cover–image, (b) stego-image without substitution, (c) stego-image with substitution

Appendix C



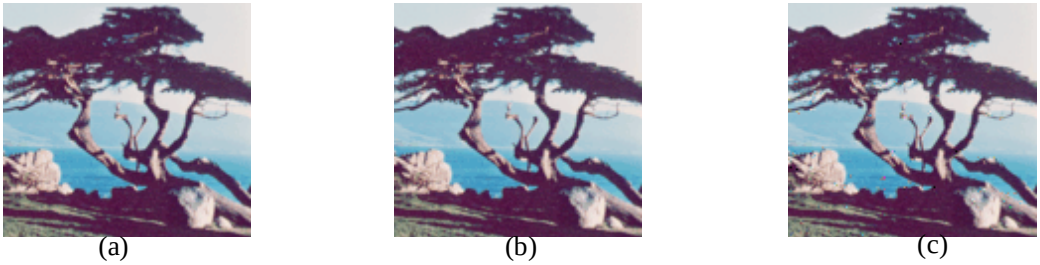
(a) (b) (c)

Figure (8): lenna image with a block size 2x2 (a) cover–image, (b) stego-image without substitution, (c) stego-image with substitution



(a) (b) (c)

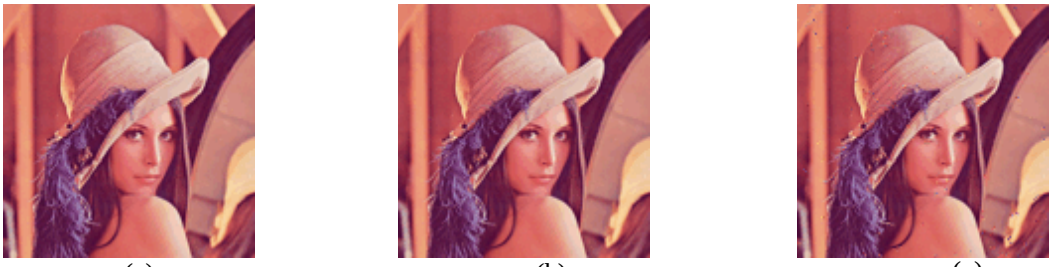
Figure (9): baboon image with a block size 2x2 (a) cover–image, (b) stego-image without substitution, (c) stego-image with substitution



(a) (b) (c)

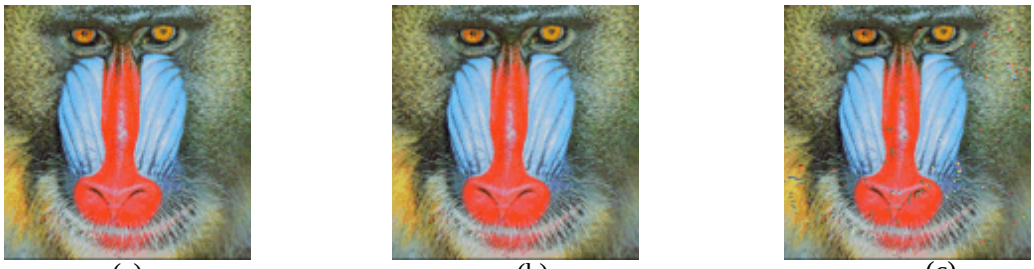
Figure (10): tree image with a block size 2x2 (a) cover–image, (b) stego-image without substitution, (c) stego-image with substitution

Appendix D



(a) (b) (c)

Figure (11): lenna image with a block size 2x2 (a) cover–image, (b) stego-image without substitution, (c) stego-image with substitution



(a) (b) (c)

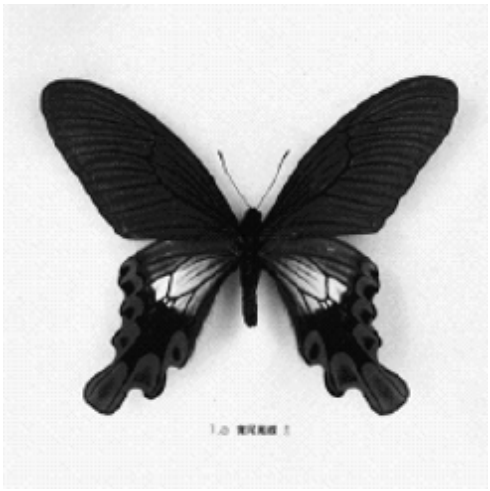
Figure (12): baboon image with a block size 2x2 (a) cover–image, (b) stego-image without substitution, (c) stego-image with substitution

(a) (b) (c)

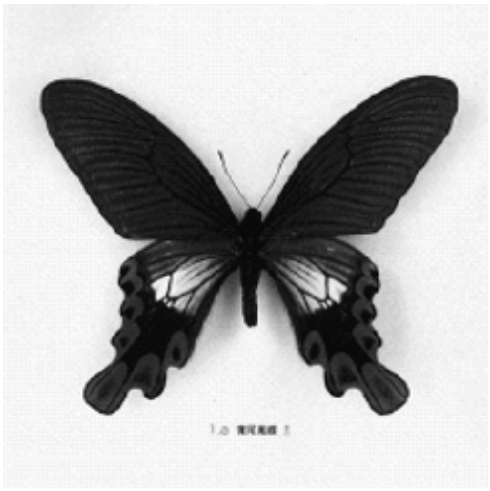
Figure (13): tree image with a block size 2x2 (a) cover-image, (b) stego-image without substitution, (c) stego-image with substitution

Appendix E

(a)



(b)



(c)

Figure (14): maraho image (512×512) (a) cover-image, (b) stego-image with block size 1×1 and (c) stego-image with block size 2×2.