University of Thi-Qar Journal Vol.14 No.3 SEP 2019
Web Site: https://jutq.utq.edu.iq/index.php/main
Email: utj@utq.edu.iq

Image Steganography Technique by Using MSUSAN Algorithm

https://doi.org/10.32792/utq/utj/vol14/4/11

Zainab Fadhil Yaseen
University Of Thi-Qar
Email: 0111821@student.uotechnology.edu.iq
Abdulamir A. Karim
University Of Technology
Email: 110004@uotechnology.edu.iq

Abstract

Nowadays, the protection of secret data, which is being sent during transmission channel, has become one of the most important challenges in the information security. Therefore, the using of multimedia technology to provide data protection is needed. Hence, one of the most common data security methods used is image steganography. This paper applied "Modified Smallest Univalue Segment Assimilating Nucleus" (MSUSAN) algorithm to detect the interest points, which it are used to steganography, so that the embedding process in the area containing the edges or corners is less susceptible to discovery because the human eye is not sensitive to the change of edges. So when the nucleus is a candidate corner, the block detected as a rough block. Whereas the nucleus isn't a candidate corner, the block detected as smooth block. The least significant bit ("LSB") technique is used to hide 3 bits in the rough block while 2 bits are hidden in the smooth block. Therefore, this method is of high efficiency in terms of payload rate, "Peak Signal Noise Ratio"(PSNR) and "Mean Square Error"(MSE) which gives average PSNR of 54.25 and average MSE of 0.25 when hiding secret image of size "128*128" (131,072 bits) in different cover image of size 512*512.In spite of hiding the largest number of secret bits up to 546506 bits, which is approximately secret image of size 261 * 261 , the PSNR is still above 46 and the MSE is still less than 1.4 . This shows that the quality of the proposed technique in this paper is very good

Keywords— hiding image, LSB Method, secret image, cover image, steganography and SUSAN.

تقنية إخفاء الصورة باستخدام خوارزمية SUSAN المحدثة

الخلاصة

في الوقت الحاضر ، أصبحت حماية البيانات السرية ، التي يتم إرسالها أثناء قناة الإرسال، واحدة من أهم التحديات في أمن المعلومات. لذلك ، يلزم استخدام تقنية الوسائط المتعددة لتوفير حماية البيانات. وبالتالي، فإن أحد أساليب حماية البيانات الأكثر شيوعًا المستخدمة هي إخفاء المعلومات. هذه الورقة استخدمت خوارزمية SUSAN المعدلة (MSUSAN) للكشف عن النقاط المهمة ، والتي يتم استخدامها في إخفاء المعلومات ، بحيث تكون عملية التضمين في المنطقة التي تحتوي على الحواف أو الزوايا أقل عرضة للاكتشاف لأن العين البشرية غير حساسة لتغيير الحواف. لذلك عندما تكون النواة زاوية مرشحة، يتم اكتشاف البلوك على أنه بلوك خشن. في حين أن النواة ليست زاوية مرشحة ، يتم اكتشاف البلوك على أنه بلوك ناعم. تستخدم تقنية ("LSB") لإخفاء 3 بتات في البلوك الخشن بينما تخفى 2 بت في البلوك الناعم. لذلك ، تتميز هذه الطريقة بكفاءة عالية من حيث معدل PSNR ، MSE الذي يعطي متوسط PSNR يبلغ 54.25 ومتوسط MSE يبلغ 0.25 عند إخفاء الصورة السرية بحجم 128 * 128 (131،072 بت) في صورة غلاف مختلفة بحجم 512 * 512.و على الرغم من إخفاء أكبر عدد من وحدات البت السرية تصل حتى 546506 بت ، وهي صورة سرية تقريبًا بحجم 261 * 261 ، لا يزال PSNR أعلى من 46 ولا يزال MSE أقل من 1.4. هذا يدل على أن جودة التقنية المقترحة في هذه الورقة جيدة جدا.

الكلمات المفتاحية: اخفاء الصور,تقنيةLSB, الاخفاء,SUSAN, الصور السرية وصور الغلاف

1. Introduction

Information security has become very important in communication technology to transmit different data such as video, audio, text and image safely [1]. The protection of the secret data against illegal person has been necessary while transmitting it over network. So, data hiding is become the popular methods to embed secret data in another file such as image[2]. The image that is used to hide data is called cover_image while the image, which holds the hidden data, is named stego_image [3]. Although the pixels of cover image have been modified to embed secret data, the hidden data should be restored perfectly from cover image[4]. Furthermore, the variance between the "cover image" and the "stego image" should be insensible [5].

Image steganography has many techniques such as “spatial domain technique”, “transform domain technique”, etc. in the “transform domain”. The cover_image is being transformed into frequency domain before hiding process. However, in the “spatial domain”, the secret information has been embedded directly in cover_image without transformation[6]. Least Significant Bit (LSB) is the most common method used in spatial domain which provides good performance in payload[7].

The performance of image steganography can be specified by three features: imperceptibility, payload, and strength. The first feature means the ability of embedding data in an unsuspicious way with less distortion. The second feature represents the Capacity of cover image for embedding data. Moreover, the third feature means the capability to protect the embedding data and retrieve it without doing any changes[8].

When the change in edge area is less discoverable by human visual observation, this concept is exploited to hide more bits in edge area and fewer bits in smooth area[9]. There are many edge detectors algorithms that are used to detect the edge pixels. However, the fastest and the better algorithm is “Smallest Univalue Segment Assimilating Nucleus” (SUSAN). SUSAN edge operator has been used to detect the enhanced edge area [10].

In steganography, there is a trade-off between the payload and PSNR because increasing the hidden bits in the cover image can cause more distortion in the stego_image and vice versa. In this method, Susan algorithm has been applied to detect interested points. In addition, more bits have been hidden in the edge points and their around neighbors while fewer bits have been hidden in the smooth areas. This leads to hide secret data in all pixel of the cover image resulting in an increasing in the number of hidden bits while maintaining the quality and imperceptibility of the stego_image. That means both the payload and PSNR are relatively balanced. On the other hand, in order to increase the protection of the secret image, the 4 LSB and the 4 MSB of each pixel have been swapped to obtain an ambiguous secret image.

2. Related Work

There are many researchers, who have developed many techniques that used in image steganography, especially the use of important points such as edges in the hiding process to improve the quality of stego image. For example, below some of the research which are related to the proposed method:

Al-Dmour H. and Al-Ani A. presented a paper in data hiding by using edge detection technique and coding. The cover image has been divided into non_overlaping blocks of size 3*3. Then the canny edge detector was applied only on the corner of block to determine if the block is edge or smooth. Therefore, 3 bits are hidden in pixels except corner pixels when the block is edge. Also XOR coding is used to reduce the distortion in stego_image. The PSNR of this method is 45.50 and the MSE is 1.833 when embedding rate is 70%[11].

Shen Sh. Y., et al. Proposed a method of data embedding based on Exploiting Modification Direction and interpolation. The 256 intensity color was divided into 6 ranges which each range has different length that decide the number of hidden bits. The cover image has been divided into non_overlap blocks of size 3*3.then the interpolation between the corners of the block was computed in order to calculate the difference between the exact pixel and its interpolation. Accordingly, the deference is checked in any range, and was belonging to select the suitable number of hidden bits. In other words, more secret bits are hidden in the pixel when the difference with its neighbors was high. The result was when hiding 499647 bits in baboon image gave PSNR of 36.1260.[12].

Gaurav K. and Ghanekar U. Proposed a method of image steganography by using edge detection technique. The cover image was modified by takeing just 4 MSB of each pixel to construct modified cover image. Then Dilation operation has been applied on modified cover image to locate the pixels that are around edge pixels which are detected by canny edge detector. Thus, secret image has been hidden in four LSB. The embedding capacity has been changed based on threshold of canny operator. When the capacity payload is 0.1, The PSNR is 57.2413 with 0.1227 MSE.[13].

3. Smallest Univalue Segment Assimilation Nucleus (SUSAN) Detection Algorithm

Smith and Brady proposed SUSAN algorithm in 1997 for corner and edge detection. This method is depended on nonlinear technique by using circular masks [14]. The efficiency of SUSAN algorithm is very high in which all types of corners can be detected by using it [15].

A circular mask is used to test the nucleus which is the center of mask. The nucleus is compared with its neighbors around it, as show in equation 1.

$$c(r, r_0) = \begin{cases} 1 & if\ |I(r) - I(r_0)| \le t \\ 0 & if\ |I(r) - I(r_0)| > t \end{cases} \qquad (1)$$

Where $I(r_0)$ is center of window (nucleus), I(r) is the brightness of neighbors at r, t is the threshold of brightness difference and c is the output.

Then the number of neighbor pixels having similar intensity value to the nucleus is determined by equation 2.

$$n(r_0) = \sum_{r \in c(r_0)} c(r, r_0) \qquad (2)$$

Where n represent the area of "Univalue Segment Assimilation Nucleus"(USAN).

Then n is compared with a geometric threshold for detecting the edge and corners by equation 3.

$$R(r_0) = \begin{cases} g - n(r_0) & if\ n(r_0) < g \\ 0 & otherwise \end{cases} \qquad (3)$$

Where g is named the geometric threshold

The corner is detected at the points where the function R(r_0) by its local maxima. This is a clear formulation of the SUSAN principle. The smallest USAN area gives the greatest value of R (r_0) that is crucial for the detection[16][17][18].

4. Image Quality Evaluation:

There are many of quality measurements used to evaluate the quality of image after hiding process. The most widely measurements used are MSE, PSNR and payload rate.

a.Mean Square Error (MSE)

It is used to compare the variances between cover_image and stego_image after hiding process. As long as there is a decreasing in MSE, the efficiency of hiding process is also increased at the same time. Equation (4) is used to calculate it [19].

$$\text{MSE} = \frac{1}{AB}\sum_{x=1}^{A}\sum_{y=1}^{B}[I(x,y) - I'(x,y)] \qquad (4)$$

Where A and B are the number of rows and columns of image, I(x,y),I'(x,y) represented the cover_image and stego_image pixel value respectably.

b. Peak Signal Noise Ratio (PSNR)

It is the quality of stego_image compared with cover_image. When the PSNR is high then the quality of stego image is good. Equation (5) is used to calculate it.

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right) \qquad (5)$$

c. Payload Rate

Payload rate is the maximum number of which can be hidden bits in cover image. The increase of payload value can lead to increase hide efficiency with keep a high value of PSNR as possible[20].

5. Proposed Method

In this paper , steganography technique is proposed by applying intersted points detector process. The change in edge or corner points is less discoverable by human_visual_perception. This concept is exploited to hide more bits in interested point and its neighbors. MSUSAN is used as an interested point detector on cover image. The proposed method has two phases.

6.1. Hiding Phase

This phase contains three stages:

Candidate Corner Detection Stage

"Modified Smallest Univalue Segment Assimilating Nucleus" (MSUSAN) is proposed in this work in order to determine whether the 3*3 block under consideration is a rough or smooth block. MSUSAN operator uses 3×3 sliding window which are convoluted in non_overlapping manner on the cover image to obtain MSUSAN image. The center of block (nucleus) is compared with the neighbors around it, using equation (1) with threshold value t=20. The number of neighbor pixels having similar intensity value to the nucleus is determined by n using equation 2. Then n is compared with a geometric threshold (g) for detecting the candidate corners by equation 6.

$$\text{nucleus} = \begin{cases} 255 & if\ n(r) < g \\ 0 & if\ n(r) \geq g \end{cases} \tag{6}$$

Where g=4 and 255 mean the nucleus is candidate corner

The nucleus of each block is tested to detect a rough block and a smooth block. When the nucleus is a candidate corner, the block detected as a rough block. Whereas the nucleus isn't a candidate corner, the block detected as smooth block. Figure 1, illustrate the rough block in which the red pixels are rough blocks.

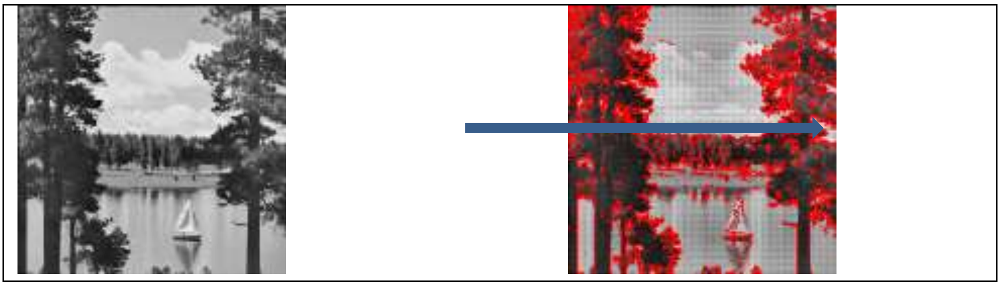

Figure 1: MSUSAN image

Secret Image Security Stage

The secret image must being secured enough before hiding it. Therefor it is being changed into ununderstood image by swapping 4 LSB with 4 MSB for each pixel as show in figure (2). This stage makes the secret image ambiguous, which can lead to increase the protection of the secret image. That depends on the increase of ambiguity. Algorithm 1 is used in this stage.

1	0	1	1	0	0	1	0
MSB				LSB			

→

0	0	1	0	1	0	1	1
MSB				LSB			

Figure 2: Secret image after swapping

Algorithm_1: swapping Algorithm

In: image
Out: swapping image

Start
Step1: for i= 0 to width of image
Step2: for j= 0 to height of image
Step3: convert pixel (i,j) to binary number
Step 4: swap the first 4^{th} with last 4^{th} of the binary number.
Step 5: convert the binary number to decimal number to set the pixel (i,j).
End.

Hiding Stage

The cover image and MSUSAN image have been convoluted in a non_overlapping manner by 3*3 sliding block. Firstly the block must be determined if it's rough or smooth depending on the corresponding block in MSUSAN image. The status of the blocks, whether rough or smooth, has been stored in a way that will be clarified later, since the process of extraction of the secret image depends on the status of the blocks.

The first pixel of block is used as an indicator to the next three blocks sequentially. That means there is one indicator pixel for each three blocks. The 3 LSB of the indicator pixel is used to store the status, whether rough or smooth, of current block and next two blocks. When the block is rough then embed (1) while when the block is smooth then embed (0). The sixth bit of indicator pixels is used to store the status of current block, while the seventh bit is used to store the status of second block. In addition, the eighth bit is used to store to the status of third block. Figure (3)illustrate the indicator process

The embedding process depends on the status of blocks. For example, when the block is rough, 3 bits of secret image has been embedding in 3 LSB of each pixel in this block except the indicator pixel. However, when the block is smooth, 2 bits of secret image has been embedding in 2 LSB of each pixel in this block except the indicator pixel. In the other words, 3 bits are hidden in rough block while 2 bits are hidden in smooth block. Figure (4)illustrate the Hiding stage and Algorithm 2 is used in hiding stage.

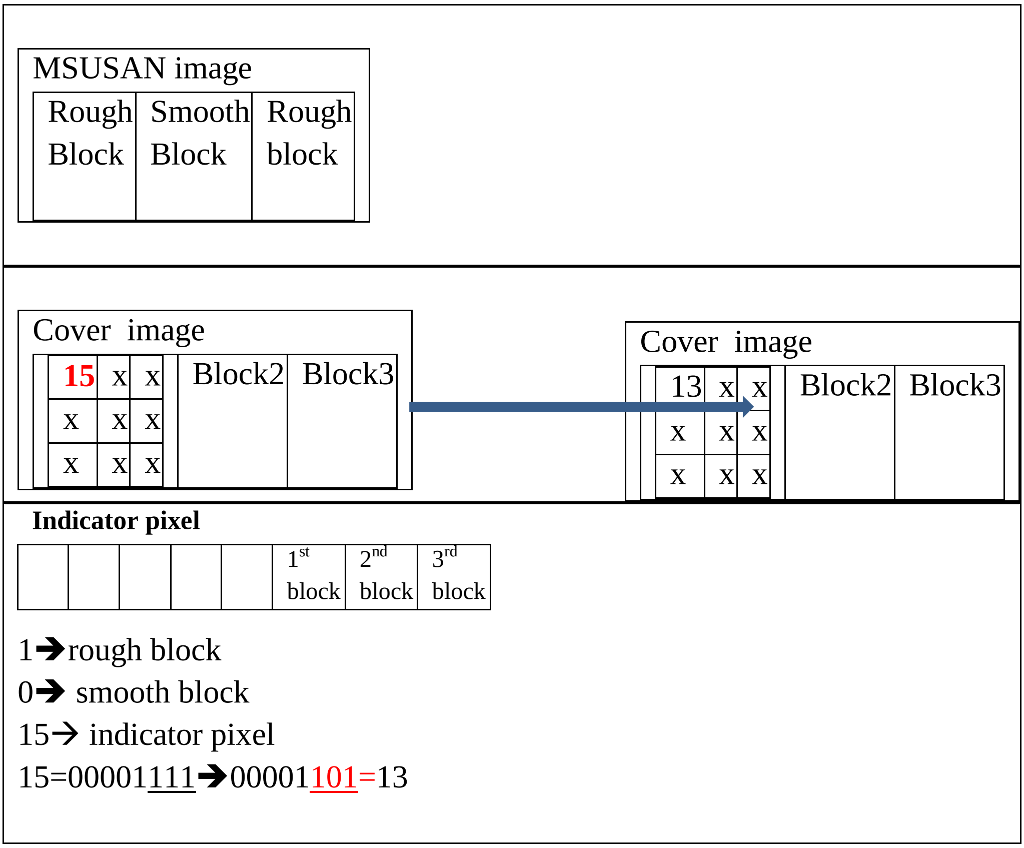

Figure 3: indicator process

Cover_image	Stego_image

15	200	5	250	100	5
60	2	0	120	116	10
10	8	100	50	110	25

10	202	7	253	98	6
60	2	3	123	114	11
11	9	101	51	106	26

Secret bits

101100101111010110101011001**1010011011010010**

Based on MSUSAN operator: the first block is smooth , the second is rough and the third is smooth

0 =smooth block

1=rough block

First block
15=
00001111=00001**010**=10(indicator pixel)
200=11001000=11001010=202
5=00000101=00000**11**=**7**
60=00111100=00111100=60
2=00000010=00000010=2
0=00000000=00000011=3
10=00001010=00001011=11
8=00001000=00001001=9
100=01100100=01100101=101

Second block
250=11111010=11111**101**=253
100=01100100=01100010=98
5=00000101=00000110=6
120=01111000=01111011=123
116=01110100=01110**010**=114
10=00001010=00001**011**=11
50=00110010=00110**011**=51
110=01101110=01101**010**=106
25=00011001=00011**010**=26

Figure 4: example of embedding process

Algorithm_2: hiding_Algorithm
In: cover_image and secret_image **Out**: stego_image

Start

Step1: Creating the MSUSAN image.

1.1 Apply MSUSAN detectors on cover image with threshold t=20 & g=4 to obtain MSUSAN image. So that each nucleus of all 3*3 blocks is indicated either a candidate corner, or not.

1.2 Set rough block when the nucleus is a candidate corner (255) and set smooth block when the nucleus isn't a candidate corner (0).

Step2: Creating ambiguous secret image

2.1 swap 4 LSB with 4 MSB for each pixel in secret image to increase the security.

Step3: : Indicate the cover image block status

3.1 Apply 3*3 non overlapping sliding window on cover image and it is correspond MSUSAN image.

3.2 The 3 LSB of first pixel of block is used as indicator to the next three blocks sequentially (in which one indicator pixel for each three blocks).

3.3 If the block is rough then set its corresponding bit to 1

Else if the block is smooth then set its corresponding bit to 0(as show in figure 3).

Step 4: Embedding secret image into cover image.

4.1 Apply 3*3 non overlapping sliding window on cover image.

4.2 If the block is rough then embed 3 bits of secret image in the 3 LSB of each block pixels

Else embed 2 bits in the 2 LSB of each block pixels as show in figure 4(except the indicator pixel).

4.3 Repeat 4.2 for all cover blocks.

End.

6.2 Extraction Phase

The extraction phase is the contrary of embedding phase. Stego_image has been convoluted in a non_overlapping manner by 3*3 sliding block.

As explained in the process of hiding stage, there is one indicator pixel for every three blocks.

It is selected the first pixel in the block (indicator pixel) and extracted 3 LSB to check the status (whether rough or smooth) of next three blocks sequencialy.

The sixth bit of indicator pixels is used to indicate the status of current block, and the seventh bit is used to indicate the status of the second block as well as the eighth bit is also used to indicate the status of the third block. If the bit is equal to one, the block is rough. If, however, the bit is zero, then the block is smooth.

Moreover, 3 bits are extracted from 3 LSB of each pixel in the rough block except the indicator. In contrast, 2 bits are extracted from 2 LSB of each pixel in the smooth block except the indicator. After the ambiguous secret image has been constructed from the extraction bits; the 4 LSB has been swapped with 4 MSB for each pixel in ambiguous secret image to get the secret image. Therefore, Algorithm_3 is used in extraction phase.

Algorithm_3: extraction_ Algorithm
In: stego_image **Out**: secret_image

Start

Step1: Apply 3*3 non overlapping sliding window on stego-image.

Step 2: determine the rough|smooth block in stego image

2.1 select the 3 LSB from first pixel (indicator pixel) to check the status (whether rough or smooth) of next three blocks (6^{th} bit indicate to the current block, 7^{th} bit indicate to the next block and 8^{th} indicate to the third block).

2.2 If the bit is equal (1) then its corresponding block is rough

Else if the bit is equal (0) then its corresponding block is smooth.

Step 3: extracting ambiguous secret image

3.1 If the block is rough then extract 3 bit from 3 LSB from each pixel except the indicator.

3.2 Else If the block is smooth then extract 2 bit from 2 LSB from each pixel except the indicator.

Step 4:obtion secret image

4.1 swap 4 LSB with 4 MSB for each pixel in the ambiguous secret image to create secret image.

End.

6. Results And Analysis

The proposed method is being evaluated by many quality metrics which are PSNR, payload and MSE. Five cover image of size 512*512 are being used to hide different secret image of different size as show in figure 5.

Table 1shows the result of hiding maximum payload in five cover image by using the proposed method. Results show high payload with better PSNR and less MSE. The average capacity is 517696.6 bits with 47.84 PSNR and 1.08 MSE.

Table 2 shows the result of hiding different secret image in Lena cover image by using the proposed method. Results show high PSNR with minimum MSE.

Table 3 shows the result of hiding secret image of size 128*128 in five cover image. Although the PSNR of all cover images is high with less MSE, however Lena cover image gives higher PSNR with minimum MSE. The average PSNR is 54.25 with 0.25 MSE.

The result of proposed method has been compared with other methods such as method shown in tables 4-6.

Table 4 shows the comparison of proposed method with other methods based on deferent capacity bits and its PSNR by using Lena cover image. It is clear that the proposed method results are the best.

Table 5 shows the result of comparison proposed method with other methods based on maximum embedding bits with its PSNR by using Lena and Pepper cover image. The proposed method result gives the maximum embedding bits.

Table 6 shows the result of comparison proposed method with other methods based on embedding rates (payload) with its PSNR and MSE by using baboon cover image. The result of proposed method gives higher PSNR with minimum MSE.

Pepper image	**Lena image**	**Boat image**	**Baboon image**	**Houses image**

Figure 5: cover images

Table 1 : the result of maximum payload with PSNR in 512*512 cover image

Cover image	**Capacity bits**	**PSNR**	**MSE**	**Payload(bbp)**
Pepper	497654	48.765	0.86	1.898
Lena	505547	48.25	0.97	1.928
Boat	512143	48.026	1.02	1.95
Baboon	526633	47.466	1.16	2.008
houses	546506	46.694	1.39	2.084

average	517696	47.84	1.08	1.974

Table 2: PSNR with different capacity bits in Lena cover image

Capacity bits	1056	8192	24200	45000	73728	122880
PSNR	76.28	67.109	62.35	59.63	57.43	55.06
MSE	0.001	0.01	0.03	0.07	0.11	0.2

Table 3: The result of embedding secret image of size 128*128(131072 bits) in different cover image

Cover image	**Lena**	**Baboon**	**Pepper**	**Boat**	**houses**	**Average**
PSNR	55.06	53.19	54.87	54.31	53.8	54.25
MSE	0.2	0.31	0.21	0.24	0.27	0.25

Table 4: Comparison of proposed method with other methods based on deferent capacity bits and PSNR.

Capacity bits	**Method name**	**PSNR**
7296	Mostafa [8]	63.86
	Proposed method	67.78
1024	Tohari [2]	71.13
	Hendro [1]	69.74
	Proposed method	76.04
10000	Peng [5]	60.47
	Xiaolong [4]	59.86
	Proposed method	66.11
16569	Hendro[1]	56.88
	Pascal[6]	48.27
	Proposed method	64

Table 5: Comparison proposed method with other methods based on maximum embedding bits

Cover image / Method name	**Lena**		**Pepper**	
	maximum capacity(bits)	**PSNR**	**maximum capacity(bits)**	**PSNR**
Hong [3]	47,549	49.98	34,758	49.87

Shen [9]	402,485	42.46	401,088	42.68
Chakraborty[20]	-----------	---------	38,657	50.29
Shen [12]	441,972	40.89	442,711	39.99
Proposed method	505,547	48.25	497,654	48.76

Table 6: Comparison proposed method with other methods based on embedding rates (payload) in baboon cover image

Payload rate	**Method name**	**PSNR**	**MSE**
0.1	Aldamor[11]	53.53	0.28
	Kumar [13]	57.24	0.12
	Proposed method	60.21	0.06
0.25	Aldamor [11]	49.72	0.69
	Kumar [13]	53.44	0.29
	Proposed method	55.87	0.16
0.4	Aldamor [11]	47.38	1.07
0.45	Kumar [13]	51.06	0.5
	Proposed method	53.36	0.29
0.6	Aldamor [11]	46.17	1.57
0.65	Kumar [13]	49.52	0.72
	Proposed method	51.85	0.42

7. Conclusion

The proposed method has been used MSUSAN algorithm to detect the rough block and smooth block. When the nucleus is a candidate corner, the block detected as a rough block. Whereas the nucleus isn't a candidate corner, the block detected as smooth block. For more protection, the secret image has been modified to be ununderstood image by swapping the 4 LSB with the 4 MSB of each pixel. By using LSB technique, 3 secret bits are hidden in the rough block while 2 bits are hidden in the smooth block. Results show that hiding 1056 bits in Lina cover image, gives PSNR of 76.28 and MSE of 0.001. Also the maximum capacity bits of pepper cover_image are 497654 bits and payload rate of 1.898 gives PSNR of 48.765 with MSE of 0.86. Besides, the PSNR still above 46 even when hiding maximum secret image and that is a good indicator that we preserve the security.

When it is compared the result of the proposed method with other state of the methods, the proposed method has achieved high performance in term of imperceptibility (high PSNR), high capacity.

Reference

[1] H. E. Prabowo and T. Ahmad, "Enhancement Of Pixel Value Ordering Based Data Hiding By Row Block Partition," *J. Ilmu Komput. dan Inf.*, vol. 11, no. 2, pp. 77–85, 2018.

[2] H. E. Prabowo and T. Ahmad, "Adaptive Pixel Value Grouping for Protecting Secret Data in Public Computer Networks.," *JCM*, vol. 13, no. 6, pp. 325–332, 2018.

[3] W. Hong and T. S. Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism," *Journal of Visual Communication and Image Representation*, vol. 22, no. 2. pp. 131–140, 2011.

[4] X. Li, J. Li, B. Li, and B. Yang, "High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion," *Signal Processing*, vol. 93, no. 1. pp. 198–205, 2013.

[5] F. Peng, X. Li, and B. Yang, "Improved PVO-based reversible data hiding," *Digit. Signal Process.*, vol. 25, pp. 255–265, 2014.

[6] P. Maniriho and T. Ahmad, "Enhancing the Capability of Data Hiding Method Based on Reduced Difference Expansion," *Eng. Lett.*, vol. 26, no. 1, pp. 45–55, 2018.

[7] J. Bai, C. C. Chang, T. S. Nguyen, C. Zhu, and Y. Liu, "A high payload steganographic algorithm based on edge detection," *Displays*, vol. 46. pp. 42–51, 2017.

[8] M. Cem kasapbaşi and W. Elmasry, "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check," *Sadhana - Academy Proceedings in Engineering Sciences*, vol. 43, no. 5. 2018.

[9] S.-Y. Shen and L.-H. Huang, "A data hiding scheme using pixel value differencing and improving exploiting modification directions," *Comput. Secur.*, vol. 48, pp. 131–141, 2015.

[10] M. H. Shokhan and A. M. Khitam, "Biometric identification system by lip shape," *Int. J. Adv. Comput. Res.*, vol. 5, no. 18, p.

19, 2015.

[11] H. Al-Dmour and A. Al-Ani, “A steganography embedding method based on edge identification and XOR coding,” *Expert Syst. Appl.*, vol. 46, pp. 293–306, 2016.

[12] S. Shen, L. Huang, and S. Yu, “A novel adaptive data hiding based on improved EMD and interpolation,” *Multimed. Tools Appl.*, vol. 77, no. 10, pp. 12563–12579, 2018.

[13] K. Gaurav and U. Ghanekar, “Image steganography based on Canny edge detection, dilation operator and hybrid coding,” *Journal of Information Security and Applications*, vol. 41. pp. 41–51, 2018.

[14] D. Tulpan, N. Belacel, F. Famili, and K. Ellis, “Experimental evaluation of four feature detection methods for close range and distant airborne targets for Unmanned Aircraft Systems applications,” *2014 International Conference on Unmanned Aircraft Systems, ICUAS 2014 - Conference Proceedings*. pp. 1267–1273, 2014.

[15] H. Y. et al. Jin, Lee; Ong, Say Leong; Ng, “Jin 2013.Pdf,” *Journal of Membrane Science journal*, vol. 427. pp. 250–258, 2013.

[16] P. Dahal, D. Peng, Y. Yang, and H. Sharif, “A resource-efficient approach to steganography in mobile systems,” *2016 International Wireless Communications and Mobile Computing Conference, IWCMC 2016*. pp. 150–157, 2016.

[17] M. Dixit and S. Silakari, “A Hybrid Approach of Face Recognition Using Bezier Curve,” *Int. J. Adv. Sci. Technol.*, vol. 71, pp. 41–48, 2014.

[18] S. T. Pathan, S. S. Waghmare, P. P. Khadse, P. P. Shukla, and S. A. Wawre, “A survey paper on a novel approach for image classification based on susan low level image processing algorithm from real time video,” *Int. J. Sci. Technol. Res.*, vol. 3, no. 2, pp. 201–205, 2014.

[19] Y. Inan, “Assesment of the Image Distortion in Using Various Bit Lengths of Steganographic LSB,” in *ITM Web of Conferences*, 2018, vol. 22, p. 1026.

[20] S. Chakraborty, A. S. Jalal, and C. Bhatnagar, “LSB based non

blind predictive edge adaptive image steganography," *Multimed. Tools Appl.*, vol. 76, no. 6, pp. 7973–7987, 2017.