Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

A Review of Image Steganography Techniques

Sura I. Mohammed Ali [1]

1. Department of mathematics & computer applications, Collage of science ,Al-Muthanna University. Al-Muthanna,Iraq.
suraibraheem@mu.edu.iq

Article Information
Submission date: 14/11/ 2020
Acceptance date: 27/12/ 2020
Publication date: 31/ 12/ 2020

Abstract

Image steganography is one in techniques of securing data as a cover image. In the other hand, since secret communications and development of multimedia contents, stenography of the techniques reflect important roles. In based are reflected stegnography system, the quality of stego image and the capacity of the cover image are important side of the image, evaluate performance and comparison of techniques are depending on these parameters in steganography system. There are existing embedding techniques that aim to protect information, and a higher bit embedding rate is an important challenge in designing a steganographic system. This paper highlights a literature review of the classification spatial domain (beads on pixel value) approach of image steganography; include, (i) LSB steganography, (ii) PVD based steganography, (iii)GLM based steganography, (iv) PPM based steganography. The goal of this paper is to supply a comprehensive summary of existing works in terms of ideals, and to highlight the strong and weak points of current techniques.

Keywords: Information Hiding, Steganography Techniques, Spatial Domain, Cover image, Visual Quality.

1. Introduction

Term of steganography is the method and technology of hiding data in approaches that prohibit revelation. The secret text in cryptography is transformed into cipher text, while the secret text in steganography stays the identical, but it is hiding in another layout of data[1]. To achieve security, a number of techniques based on any type of the cover object are presented. For instance: an image is an approach of hiding the secret image into the cover image and the cover image likes to be an original image, an image is a carrier that hides the secret information[2]. Audio object is applied to hide a secret message through the manipulation of binary sequence of sound files. Another type is video object that is streamed images and sounds together. The video object holds huge data to hide its, and a text file mentions the information that is covered up in image files. The main components of steganography require, cover of an object, secret information, and steganography algorithm [3].Images are considered the best cover objects for hiding information because they contain a large amount of redundant bits[4]. The image carrying secret information called stego image. A process of image stenography approaches is being a spatial domain and a transformational domain. All the existing techniques have their strong and weak aspects specifically in factors of payload capacity (maximum message size that embedded in bits of stego image), security and performance represented by (Mean Squared Error (MSE) and the Peak Signal-to-Noise Ratio (PSNR) who achieves better fineness of the image. Spatial

Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

domain and Transform domain are popular approaches in image steganography; spatial domain is more popular because of readiness in hiding and extraction approach [2]. In figure 1diagram of image steganography, where the embedding process must achieved strength factors: embedding capacity(Payload), maintaining the visual qualtiy of stego image, with higher un-detectability which makes it hard to be attacked by others.

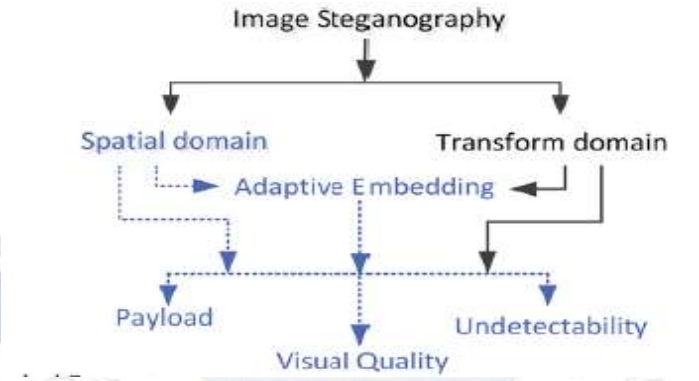

Figure .1 Image stenographic diagrams

This paper focuses a few of spatial domain steganography approaches and describes various popular algorithms of image steganography.

2. Spatial Domain Steganography: A brief review

Spatial domain steganography has been yet researched widely [5]. It is popular mainly because its strength of supplying space for large payload of information[1]. Least Significant Bit (LSB), PVD, Histogram shifting, and Pixel are methods of steganography spatial domains as figure 2.

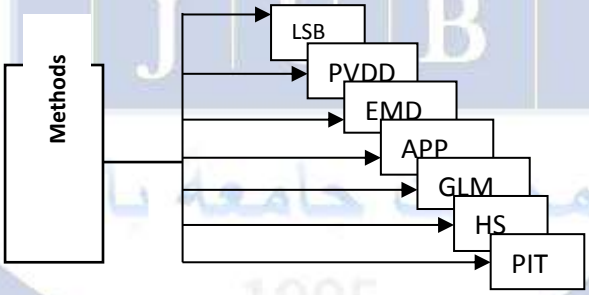

Figure.2 Methods of Stenographic spatial domains

In spatial methods, not changed in image quality using any algorithm and huge capacity of data can be stored. The combination of methods based on LSB is covered in this section. The several common methods used by this domain are as follows.

2.1 Least Significant Bit (LSB) based methods

It is most a broadly strategy for achievement steganography. This technique works by replacing selected 2 bits of LBS pixels or more in the cover image with original text "message" bits. In the spatial domain, the LSB technique, with image processed a part of hidden data can get missing [5]. Figure 3 shows example of LSB method.

Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

Figure.3: Embedding Mechanism Using 1-bit LSB

2.2 Pixel Value Difference (PVD)

PVD method is one of the most important algorithms used for data hiding. This method splits up an image into blocks of 2pixels in a zig-zag manner. The disparity of values for 2 pixels is the reason for embedding. High performance in visual quality, payload and impedance of steganalysis attacks, these features are supplied by PVD method[6]. Multi Directions (MD), Multi-Pixel Difference (MPD), PVD, PVD with LSB, Modulus Function (MF) and Side matching are the classes of PVD. Many studies proposed in the literature by PVD method.

2.3 Exploiting Modification Direction (EMD)

It keeps up the high fineness of cover images [7]. This method divides the image with a set of n pixels into equivalent groups((g1, g2… gn).) .

A pixel in each group is modified one gray scale value at most to hide a secret digit in a (2n+1)-ary notational system.

The embedding allowed one to be added or subtracted from a specific pixel withi n the group. To embed secret digit (d) into pixel group, value of extraction function f is calculated by using equation (1)

$$f(p1, p2, p3,\ldots pn) = \sum_{i=1}^{n}(pi \times i) \bmod (2n + 1)$$

If $f \neq d$, then only one of the pixels from the pixel group has to be incremented or decremented by one. If $f = d$, then there is no need to change any pixel and the process continues until no secret digit is remaining.

2.4 Pixel Pair Matching (PPM)

It worked with a pixel capable (x,y) and (x' ,y') is selected. Pixel capable (x,y) is refer to as coordinate and searching coordinate (x' ,y') in the neighborhood set of this pixel pair as indicated by a given message digit. A pixel in each set is adjusted for the gray scale value to hide a secret number in a (2n+1)-ary notational system [8].

2.5 Gray Level Modification (GLM) based methods

The gray level values of the image pixels adjusted as per a numerical capacity to represent binary information [9]. Every pixel appears as for odd or even value that is prepared in manner to perform binary information..

Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

2.6 Histogram based methods

It is normally utilized steganographic method and viewed as a functional, histogram based on embedded schemes and next stages. The histogram is created through partial classes of data set into equal-size cases. The numbers of points of every case are checked edge based methods[10].

2.7 Pixel/Block indicator base methods

Pixel/Block indicator based information embedding inserting plans using RGB images as cover media. A color image includes 3 bytes (red, green and blue)channel, one of them channels is utilized as an indication while the remainder of channels are utilized as information channels.

3. Literature Review

Several of the existing steganographic techniques discussed in this section. In [3] authors introduced an adjusted image steganography that depends on LSB technique. Their proposed is dependent on using 2 pixels of the cover image to concealing six message bits, the first pixel is covered (3 bits) of the first message bits and the second pixel is covered (3 bits) of last message bits. Through the application of LSBraille algorithm is to make each byte in the secret message in binary format as appeared in figure 4 below.

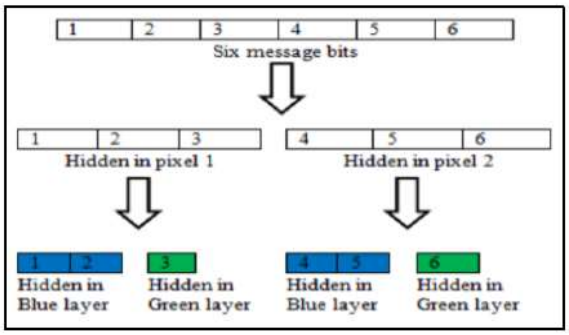

Figure4: The Secret Message Bits

On their method, Red layer, Blue layer and Green layer were of the split result of the original image. Second and third bits of least significant bit (LSB) of the blue layer are utilized for embedding information, while one binary bit of green layer is used for embedding, this process applying by XOR Gate, as follows equations:

"B1 XOR B2=N2 …… (1) "

"B2 XOR B3=N3 ……. (2) "

Where, B is a byte of the Blue layer, (B1, B2, and B3) refers to First, Second and Third layer of LSB respectively. Outputs (N2, N3) are equal to two secret data bits; no change in the pixel. If bits of message are not quite the same as any of those outputs, single bit of cover image pixels changed only. This changed may be in one of the bits (B1, B2 and B3) of least significant bit.

Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

In [11] the authors present another technique for embedding secret message in images. Their proposed hiding 9 bits of massage in a single pixel of cover image, only 2 bits of each component is changed. A digital image consists of three components R, G, and B, 3 bits of one component message hidden. In this method, four bits of each component of LSB used as circuit to convert pixel of cover image into stego as shown in figure5.

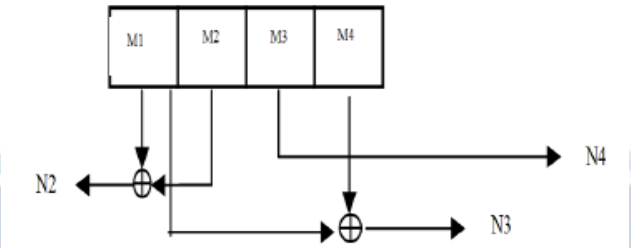

Figure 5: Circuit Converts Cover to Stego Bits

Where (M1, …, Mi) ∈ LSB of one component, i represent the number of bits. N4 represents a third bit. When entering bits of the component, in XOR gate are resulted it of N2, N3. The component unchanged if outputs N2, N3 and N4 are equal to message embedded bits. The two bits of each component are changed if embedded bits are different from one of these outputs. The process embedded is used only even columns of pixels, which gives strengthen and security for this method.
In [12] the authors proposed Pixel Value Modification (PVM) method for hiding a secret message in digital images. Three color planes (red, green, and blue) of the image are using. Embedding procedure of proposed as steps;

Step 1: Each color is a separate component and obtains matrix M×N (1st pixel of the red, 1st pixel of the green, 1st pixel of the blue and so on for all pixels) separated. All three components used for data embedded.
Step 2: secret data d is represented into 3 values of (0, 1, 2) that hidden in 3 colors.
Step3: g1, g2, ..., gn. Values of Pixel indicted as group of matrix. gr_i,gg_i,gb_i represented Decimal value of Red pixel, Green pixel, Blue pixel respectively,
f is studied by Eq. (1) for each color.
$f=(g1,g2\ ,g2\ ,\ldots\ldots gn)=\Sigma=1 gri\ ni\ mod\ 3$
Three cases of f:
Case 1: if f= d, refer no changed gir='gir

Case 2: if f≠d and f < d, then 'gri= (gri +1) refer new changed
Case 3: if f ≠d & f > d, then 'gir= (gri -1) refer new changed.

Step 4: A pixel for PVM of embedded including
0≤ gi ≤250 of cover image.
Step5: Repeat step 3,4 for g & b matrix of cover image.
Step 6: combination rgb plane of secret data from rgb plane of stego image. Figure 6 shows Example on PVM method.

Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

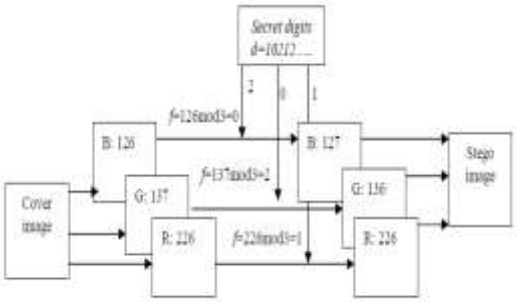

Figure 6: Example PVM method

In [9] a stenographic algorithm based on Gray Level Modification (GLM) technique is presented. The process of embedded data implementations based on select a set of pixels according to an arbitrary function g (x, y) as a bit stream. Set of pixel has an odd number referring to gray level value and another set have an even number. For example, bit stream 1001010101, the first bit would allocate with the first pixel that selected in the image. Increment the gray level value of the pixel by one unit when gray level value is odd, making it even by represented 0 and to represent 1 of pixel by decrementing its gray level value by one for satisfying the condition of being odd or even. Figure 7 shows Gray Level Modification

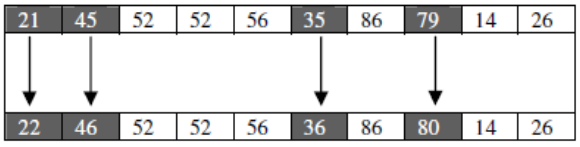

Figure7: Gray Level Modification (GLM)

Shaded pixels would represent adds while unshaded pixels would represent evens. The bit stream 1001010101 can now be represented as shown in Figure 8.

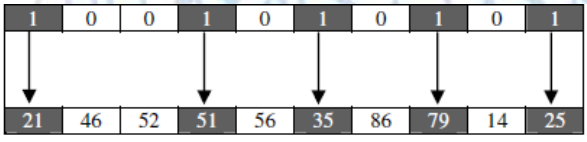

Figure 8: Changed Bit Streams

In [4] proposed a data embedding method based on Pixel Pair Matching (PPM). The pixel pair is the exchange of the searched coordinate to disguise the digit. A cycle of embedding dependent on assume the cover image is of size M×N, S is the message bits to be covered up and the size of S is |S|. For embedded all message bits, should be initial calculates the minimum B such that. At this point, a message digit covered up into sets of pixels consecutively, to achieve a superior image quality, those users' choices digits in any notational system for data embedding, through providing more compact neighborhood sets. In [13] is proposed pixel indicator technique (PIT)

Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

technique using RGB image pixels. The process of selected indicator is in series manner. One of the channels uses two bits of LSB as an indicator of secret data existence. Its selected first of 8 bytes of the image utilized to store of embedded message, and used to recognize of the indicator channel sequence as displayed in table1.

Table 1: Indicator Channel Sequence

Indicator Channel	Channel 1	Channel 2
00	No hidden data	No hidden data
01	No hidden data	2bits of hidden data
10	2bits of hidden data	No hidden data
11	2bits of hidden data	2bits of hidden data

The primary level is indicator chocking, while channels that embedded data are second level. Is possible six indicators are obtained from the length of the message (N), for example, if N is even; channel R, is indicated, leaving of G or B depending on the equality bit of N, if N is a prime number, Chanel B is considered as the indicator leaving R and G for data covering up. If the N value neither is even nor prime, "else" row in table 2 chosen, choosing the indicator channels (G, B and R) are for secret data retention. The primary level is indicator chocking, while channels that embedded data are second level. Is possible six indicators are obtained from the length of the message (N), for example, if N is even; channel R, is indicator leaving of

G or B depending on the equality bit of N, if N is a prime number, Chanel B is considered as the indicator leaving R and G for data covering up. If the N value neither is even nor prime, "else" row in table 2 is chosen, choosing the indicator channels (G, B and R) are for secret data retention. Table 3 explains advantages and disadvantage of Image Steganography Techniques in Spatial Domain.

Table 2: Indicator Channel Sequence

Type of length (N) of secret message	I Level Selection Select indicator channel, first element of sequence	II Level Selection Binary N parity-bit	
		Odd Parity	Even Parity
Even	R	GB	BG
Prime	B	RG	GR
Else	G	RB	BR

Journal of University of Babylon for Pure and Applied Sciences, Vol. (28), No. (3): 2020
Online ISSN: 2312-8135, Print ISSN: 1992-0652

Table 3: A Review of Image Steganography Techniques in Spatial Domain

Approach	Reference	Algorithm	Advantages	Disadvantages
LSB-based	" A Modified image Steganography Method based on LSB Technique"	LSB-XOR Gate	• Improved slightly of performance of LSB stenographic technique. • Improved visual quality (PSNR). • Good capacity of hiding data	• Limited evolution(capacity only).
LSB-based	"A Youthful Procedure for Spatial Domain Steganography"	LSB-XOR Gate	• Higher security because only few pixels are used	Security should be evaluated
PVD-based	"Color Image Steganography based on Pixel Value Modification Method Using Modulus Function"	PVD-PVM	• More secret data Hiding	High pixel modification ratio
GLM-based	"Grey Level Modification Steganography for Secret Communication"	GLM	• Complexity time O(n) • High data hiding capacity	Limited evolution
PPM-based	"A Novel Data Embedding Method Using Adaptive Pixel Pair Matching"	PPM-APPM	• More compact neighborhood sets • Lower distortion for payloads	Bounded security (<0.5) SPAM

4. Conclusion

A literature review of steganographic approaches of spatial domain has introduced in this paper. The existing embedding approaches in spatial domain were substantive and discussing the methodology of these approaches. Depending on the proposed algorithms, all the aforementioned approaches had strengths and limitations. An image steganography approach should higher implanting payload, high quality, and high security, however ,there is no existence of steganography approach in reality that include these features.

Conflict of interests.

There are non-conflicts of interest.

References

[1] S. I. M. Ali, M. G. Ali, and L. A. Z. Qudr, "PDA: A private domains approach for improved msb steganography image," Period. Eng. Nat. Sci., vol. 7, no. 3, 2019.

[2] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, and K. H. Jung, "Image steganography in spatial domain: A survey," in Signal Processing: Image Communication, Jul. 2018, vol. 65, pp. 46–66, doi: 10.1016/j.image.2018.03.012.

[3] M. A. Saleh, "Image Steganography Techniques - A Review Paper," IJARCCE, vol. 7, no. 9, pp. 52–58, Sep. 2018, doi: 10.17148/ijarcce.2018.7910.

[4] K. Muhammad, J. Ahmad, H. Farman, and M. Zubair, "A Novel Image Steganographic Approach for Hiding Text in Color Images using HSI Color Model."

[5] M. M. Hussain, M. M. Hussain, S. Zulfiqar, and A. Bhutto, "A Survey of Image Steganography Techniques," 2013.

[6] et al. HUSSAIN, Mehdi, "Pixel value differencing steganography techniques: Analysis and open challenge.," in 2015 IEEE International Conference on Consumer Electronics-Taiwan. IEEE, 2015, pp. 21-22.

[7] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," IEEE Commun. Lett., vol. 10, no. 11, pp. 781–783, 2006, doi: 10.1109/LCOMM.2006.060863.

[8] W. Hong and T. S. Chen, "A novel data embedding method using adaptive pixel pair matching," IEEE Trans. Inf. Forensics Secur., vol. 7, no. 1 PART 2, pp. 176–184, 2012, doi: 10.1109/TIFS.2011.2155062.

[9] V. M. Potdar and E. Chang, "Grey level modification steganography for secret communication," in 2nd IEEE International Conference on Industrial Informatics, INDIN'04, 2004, pp. 223–228, doi: 10.1109/indin.2004.1417333.

[10] P. Daniel, R. Raju, and G. Neelima, "Image Segmentation by using Histogram Thresholding," IJCSET, vol. 2, no. 1, pp. 776–779.

[11] S. Arya Raj and T. Soumya, "A youthful procedure for spatial domain steganography," Proc. - 2013 3rd Int. Conf. Adv. Comput. Commun. ICACC 2013, pp. 300–303, 2013, doi: 10.1109/ICACC.2013.63.

[12] V. Nagaraj, V. Vijayalakshmi, and G. Zayaraz, "Color Image Steganography based on Pixel Value Modification Method Using Modulus Function," IERI Procedia, vol. 4, pp. 17–24, 2013, doi: 10.1016/j.ieri.2013.11.004.

[13] A. A. A. Gutub, "Pixel indicator technique for RGB image steganography," J. Emerg. Technol. Web Intell., vol. 2, no. 1, pp. 56–64, Feb. 2010, doi: 10.4304/jetwi.2.1.56-64.

الخلاصة

اخفاء الصور هو أحد تقنيات تأمين البيانات كصورة غلاف. من ناحية أخرى ، نظرًا لأن الاتصالات السرية وتطوير محتويات الوسائط المتعددة ، يعكس الاختزال للتقنيات أدوارًا مهمة. تعد جودة صورة الغلاف " stego"وقدرة صورة الغلاف جانبًا مهمًا في نظامstegnography ، ويعتمد تقييم الأداء ومقارنة التقنيات على هذه المعلمات في نظام إخفاء المعلومات. هناك تقنيات تضمين موجودة تهدف إلى حماية المعلومات ، ومعدل تضمين البت الأعلى يمثل تحديًا مهمًا في تصميم نظام إخفاء المعلومات. تسلط هذه الورقة الضوء على مراجعة الأدبيات لنهج المجال المكاني للتصنيف (الاعتماد على قيمة البكسل) لإخفاء الصور ؛ و شمل ، (1) إخفاء العلومات باستخدام طريقة LSB ، (2)إخفاء المعلومات باستخدام طريقة PVD ، (3)إخفاء المعلومات باستخدام طريقة GLM ، (4) إخفاء المعلومات باستخدام طريقة PPM الهدف من هذه الورقة هو توفير ملخص شامل للأعمال الموجودة من حيث الهدف ، وتسليط الضوء على نقاط القوة والضعف في التقنيات الحالية.

الكلمات الدالة: إخفاء المعلومات، تقنيات إخفاء المعلومات، المجال المكاني، صورة الغلاف، الجودة المرئية.