ARTICLE

JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)

Vol.30; No.4.| 2022

Information Hiding Method For Gray Images Using Motif Patterns

Elaf Ali Abbood[1*] and Rafeef Mozher Ketran [2]
1* Computer Department, Science College for Women, University of Babylon
wsci.elaf.ali@uobabylon.edu.iq, Hilla, Iraq
2 Computer Department, Science College for Women, University of Babylon
wsci.rafeef.ketran@uobabylon.edu.iq, Hilla, Iraq
***Corresponding author email**: wsci.elaf.ali@uobabylon.edu.iq; mobile: 07725963555

طريقة لاخفاء المعلومات للصورة الرمادية باستخدام نماذج الزخارف

ايلاف علي عبود*[1]، رفيف مظهر كطران [2]
*1 كلية العلوم للبنات، جامعة بابل، wsci.elaf.ali@uobabylon.edu.iq الحلة، العراق
2 كلية العلوم للبنات، جامعة بابل، wsci.rafeef.ketran@uobabylon.edu.iq الحلة، العراق

Received:	29/ 7/2022	Accepted:	25 /9 /2022	Published:	31/12/2022

ABSTRACT

Information hiding is one of multimedia security tasks need to develop and update in Continuously. Thus, the researchers work in this field and interest in developing and improving the information hiding techniques. In this paper, a new method for develop least significant bits (LSB) method is introduced. The method includes a schema for hiding two bits of secret text in each pixel (least and penultimate bits of pixel) in gray image considering motif Z, U, N, and C patterns. The method is implemented on different standard images with size 512*512 and hide different secret text lengths. The experimental and results show the efficiency of method that hide two bits in each pixel compare with the traditional LSB method that hide one bit of data in each pixel of image. The results show that the proposed method produces a good accuracy of stego image near to the original LSB method in terms of PSNR accuracy metric.

Key words:
Information hiding, motif patterns, LSB, Gray image

الخلاصة

إخفاء المعلومات هي واحدة من مهام أمان الوسائط المتعددة التي تحتاج إلى تطويرها وتحديثها باستمرار. وبالتالي ، يعمل الباحثون في هذا المجال ويهتمون بتطوير وتحسين تقنيات إخفاء المعلومات. في هذا البحث ، يتم تقديم طريقة جديدة لتطوير طريقة البتات الاقل اهمية (LSB). تتضمن الطريقة مخططا لإخفاء بتين من النص السري في كل بكسل (البتات الأخيرة وقبل الأخيرة من البكسل) في صورة رمادية مع مراعاة أنماط الزخارف Z و U و N و C. يتم تنفيذ هذه الطريقة على صور قياسية مختلفة بحجم 512 * 512 وإخفاء أطوال نصية سرية مختلفة. تظهر التجربة والنتائج كفاءة الطريقة التي تخفي بتين في كل بكسل مقارنة مع طريقة LSB التقليدية التي تخفي بت واحد من البيانات في كل بكسل من الصورة. أظهرت النتائج أن الطريقة المقترحة تنتج دقة جيدة لصورة stego تقترب من طريقة LSB الأصلية من حيث مقياس دقة PSNR.

الكلمات المفتاحية:

اخفاء المعلومات، نماذج الزخارف، LSB، PSNR

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

INTRODUCTION

Because to the fast development at the field of modernistic communications and information technology, which made the process of data flow faster and easier [1 and 2]. So, data transmission process is unreliable, can be tampered with, copied, alter its integrity, and allows access to malicious attacks, authorization, and eavesdropping. Therefore, one of the most important challenges is to prevent the confidentiality of important information [3], whether for preservation or transmission over the network. Hiding information is one of the methods of steganography that works to maintain the confidentiality of data [4]. As well as, it one of the modern methods that keep something secret and find the best place to hide something away from others and at the same time it does not affect where the thing is saved. This is called "*Steganography*". The word Steganography comes of the Greek, whom literally means “hidden writing” or “covered” and which contains broad aggregates of secret means of communication that conceal the existence of this message [5].

Because of such fast growth for network technologies and emergence of cutting-edge devices like cloud, fog, edge, SDN, big data, Internet of Things (IoT), deep learning, etc. Such development has led up to increased security concerns, such as, unauthorized reproduction, modification, deletion, etc., where is considered Internet is an open medium, in addition to the presence of many strong multimedia processing material. Thus, protecting privacy of multimedia data has be imperative requirement in the field of multimedia security. So, steganography is the main approach to block multimedia data of unauthorized access, utilize and privacy violation [6].

In multimedia files, information hiding goal to include a large number of confidential data records in them, this as audio, static and dynamic images, and video [7]. In a computer science, an image is a set of numbers, and these numbers representing the intensity of light at different points or pixels. These pixels shape the image raster data [8]. When Steganography is used with digital images, image files are typically 8-bit and 24-bit-per-pixel. Therefore, digital images are more flexible when used with steganography. There are many different ways to hide information inside images. Messages can be inserted directly, as you shall purely encode every piece of information in the image. Further complex coding can become done to include the message only in the "noisy" areas of the image that shall entice less attention. in addition to, we might randomly scatter the message all over the cover photo [9].

The most common ways to hide information in photos is the Least significant bit (LSB). The Least significant bit (LSB) is popular and easy way, used to include information in a graphic image file. In computing and other related fields, binary numbers are used so that the least significant bit is especially important when it comes to transferring binary numbers. So, the least significant bit is the bit farthest to the right and holds the lowest value in a multi-bit binary number [9]. So, the Least significant bit (LSB) depends on changing the least significant bit (the eighth bit) for a few or all of the bytes within the image to part of the secret message [10]. The distinguishing feature for LSB inputs is that data can be hidden in the least and second to lowest bits, yet the human eye will not be able to notice it [9].

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

In computational biology, the search for data motifs has been adapted as a means of finding recurring patterns through sequential time series [11]. The advantage of motifs in other patterns matching techniques is that the style does not require a priori templates or examples of sequences. Instead, motifs search finds the most frequent, non-trivial, and mutually exclusive K-repetition patterns present in the data series [12].

Usually, patterned texture is observed in many everyday items where it is in the form of periodic structures such as nets, chains, engraved metal, heated windows and other materials important for safety. The patterned texture is composed of lattice, the basic unit of its composition, which is found by design. And to manufacture the patterned texture is by applying the appropriate analog rules for that network. Practically, when manufacturing and working on lattice repetition, it causes various types of defects to appear. Traditionally, patterned texture is checked after it has been manufactured by man, and it is refused if the number of flaws exceeds the threshold limit. In addition, the defect detection system not only reduces employment cost but also ensures high quality production in industrial automation and safety system [13].

Image quality definition is a property about an image that measures the degradation of a processed image by comparing it with an ideal image. In most imaging systems, humans are the observers and users of them, and therefore self-assessment of image quality is considered a reliable method. As well as, in real-time applications, the use for the subjective method is limited by its complexity and onerousness in implementing it. In recent years, objective methods have been widely used to assess image quality. In this work, we will consider measures of image quality PSNR (peak signal to noise ratio) is one of the most frequently used metric parameters [14]. PSNR is a signal processing measurement who compares a given signal received or processed with its original source signal. This comparison allows us to determine how well the processed signal fulfills the original, which, also, allows us to identify potential noise or distortions in the signal. Therefore, PSNR represents a direct relationship to the signal before and after the degradation process [15].

In this paper, a new method of LSB method implementation is proposed. The method adopts motif patterns as a schema for hiding secret text bits in last and penultimate bits of each pixel in a cover image. The method is applied on many three standard images and different lengths of secret text streams. The rest of paper organized as follow: Section 2 presents the related works and literature review. Section 3 introduces the proposed method and its steps in details. Section 4 shows the experimental results when applying the method on different images and secret text lengths compared with tradition LSB method in terms of PSNR metric. Section 5 introduces the conclusions and future works to develop the method idea.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Related Works

Sumathi CP et al. in [16] introduced various statistical algorithms were used in order to change statistical elements of the digital file for statistical information hiding techniques. Spread spectrum communication is also a common way to hide information as well, as it the hides and retrieves messages of greater long within the digital image that preserve the original image size and dynamic range, whilst the jamming process includes changing the signal that carries the information and then making comparisons with the content the original mediator with later.

In [17], a difference expansion (DE) widening technique has been proposed, it is a lossless technique to help integrate data within cover images in high-quality, high-capacity ways. Therefore, this method relied on exploration the redundancies in digital images in order that take advantage of the excess information in capacity increase as well reducing the distortion. Then the difference of adjacent pixel values was calculated in order that obtain DE, and to determine the embedding region use the Segmented Least Significant Bit (SLSB) method, the native values for that area and payload were combined the same time. The method has been included for the native values in order to obtain accurate image recovery and reduce image distortion. The techniques used in that work lossless compression technique before the merging process on order that solution the large amount for embedded data (payload and original values). PSNR technology demonstrated best for lower payload size.

Luo H et al. [18] introduced a technique based on the mediator principle to strengthen the impregnation ability and specific image quality. The method scans the image for the corresponding High-link pixels, in order that obtain a histogram of difference. Given the average of the integer number of selected blocks, a multilevel transformation of the embedding stage graph was used. Based on the relevant method, the measured masses were grouped and distributed into four classes. Thus, the objective for this process is maintain the computed average through the embedding phase.

Tao J et al. [19] proposed a framework for hidden JPEG compression when it is transmitted through a secret communication channel. First, the original version of the compressed channel was obtained, and by using the steganography JPEG method, embedded confidential data was obtained through the compressed image channel, and a stego image was produced after the transmission process.

In [20], a new approach to hiding information without including (SWE) has been worked. In the method, the secret data is mapped into the noise vector, the neural network model of the generators are trained, and the image swatch is created based on the vector. The model extractor has proven to be successful in extracting image information by other neurons in the network after training.

In [21], the concept of image color channel angular shifting in data security is illustrated. In this paper, LSB Steganography technology was used to hide confidential data in color image with the help of red, green, and blue RGB channels. The inline message is extracted by shaping the same angular transformation on the receiving side of the stego image.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Methodology

This paper introduces a method for information hiding for hide text data in cover gray image using a new form of applying LSB method. The method includes applying Z, U, N, and C motif pattern in each consecutive four vertical group of pixels and then uses the same patterns in next five vertical pixels for hiding data and so on. Figure (1) illustrates the block diagram of the proposed method. Like in LSB method, the data bits are hides in images pixels; each bit is hides in one pixel. Whereas the images we used in our experiments are gray images, each pixel consumes one byte of cover image. As explain in Figure (2), data bits are hides in the least and penultimate significant bits of the cover image pixels in the sequence. That mean, less information of the cover image is missing, thus, more secure method and less distortion of it.

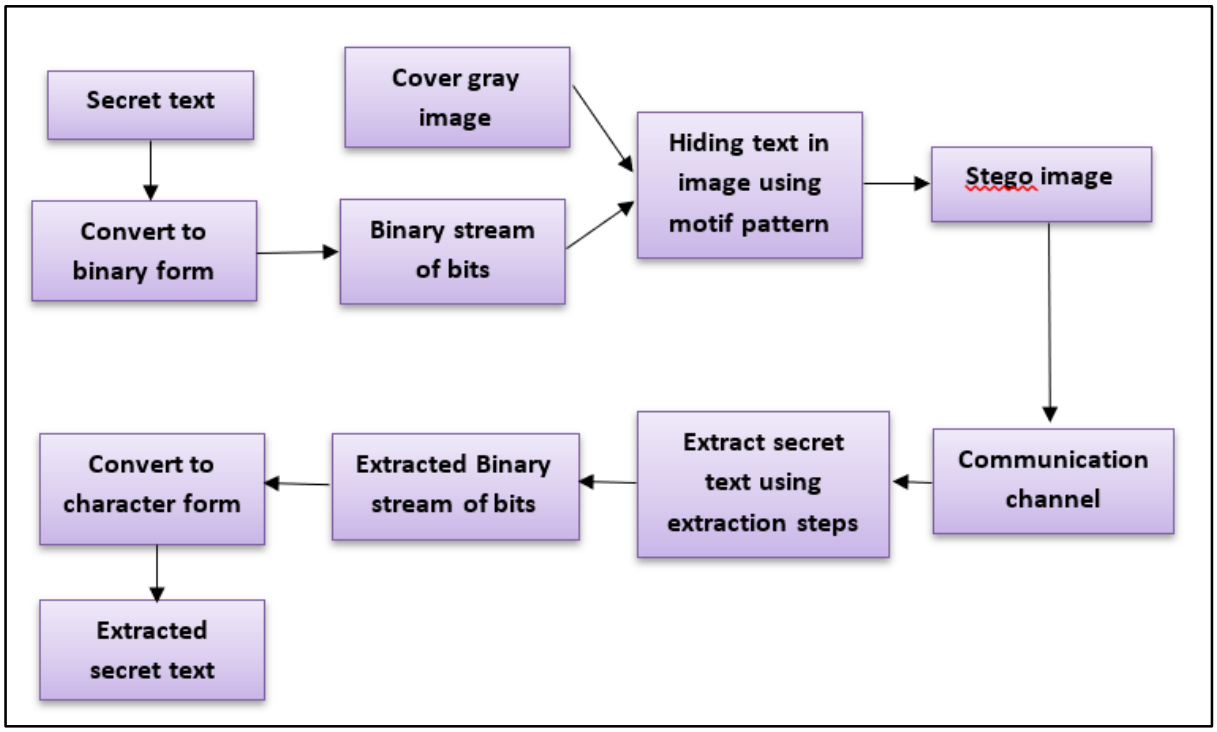

Figure (1) Block diagram of proposed LSB method

The proposed method is motivated form the original LSB method just changes the location of hiding bit in cover byte. The changes in hiding patterns increase the powerful of the method and get more efficiency and robustness against the intriguers and attacks.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

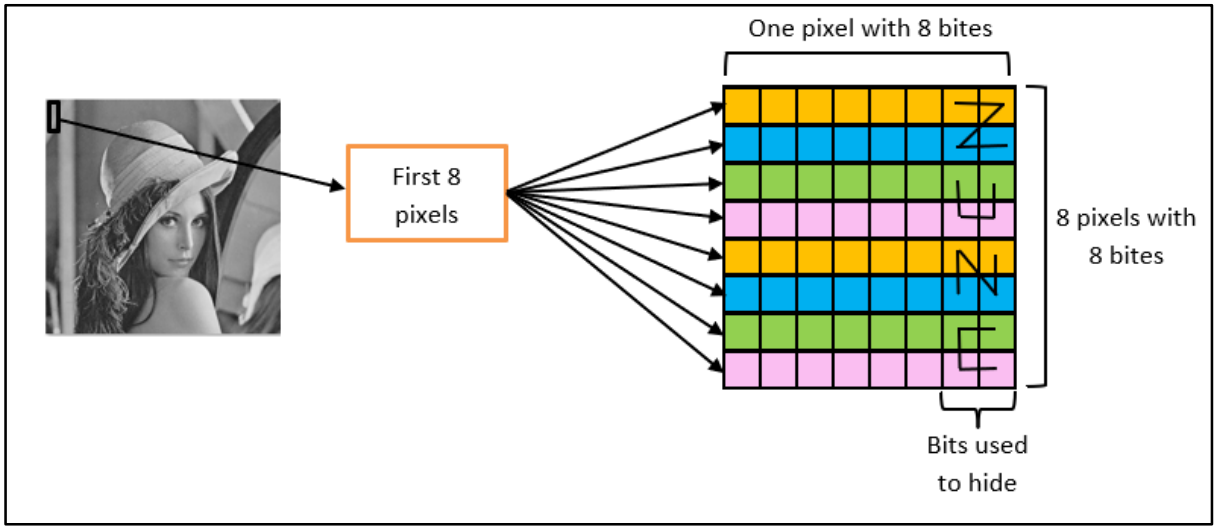

Figure (2) First 8 pixels and method to hide secret text bits in least and penultimate bits in each pixel using Z, U, N, and C patterns

The proposed method includes the following steps to hide text:

1. Read the secret text characters.
2. Convert the text characters to binary form.
3. Scan the cover image from top to down and from left to right.
4. Change the least and penultimate bits of two pixels on top of each other with a secret text bit considering Z, U, N, and C motif patterns, respectively.
5. Continue until hide all text bits.

The extraction steps of secret text are illustrated in Figure (2) and explained in the following steps:

1. Scan the stego image from top to down and from left to right.
2. Extract a secret text bit from the least and penultimate bits of two pixels on top of each other considering Z, U, N, and C motif patterns, respectively.
3. Continue until extract all text bits.
4. Convert the text binary form and return to characters.

Results and Discussions

To evaluate the method presented in this paper, Peak Signal-to-Noise Ratio (PSNR) is used between the original and stego images. PSNR is a statistical metric used to measure the accuracy of the stego image using the Eq. (1) [15]:

$$PSNR = 10log_{10}\left(\frac{255^2}{\frac{1}{MN\sum i\sum j(yij-xij))^2}}\right), \qquad (1)$$

Where, M and N are the images dimessions, xij and yij are original and stego images pixels, respectively.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

The experimental performed in this paper includes applying the proposed method on many standard images and using many lengths of secret text. Table (1) illustrates a comparison between original LSB method and proposed hiding method in terms of PSNR between original and stego image using standard Lena, Baboon, and Goldhill images with 512*512 pixels and secret text lengths 4000, 15000, and 30000 bits.

Table (1) Comparison in terms of PSNR between proposed method (hide two bits in each pixel) and original LSB (hide one bit in each pixel) using different images and different secret text lengths

Cover image 512*512	Secret text 4000 bits		Secret text 15000 bits		Secret text 30000 bits	
	Original LSB / hide one bit in each pixel (dB)	Proposed method / hide two bits in each pixel (dB)	Original LSB/ hide one bit in each pixel (dB)	Proposed method / hide two bits in each pixel (dB)	Original LSB/ hide one bit in each pixel (dB)	Proposed method / hide two bits in each pixel (dB)
Lena	60.04112	45.4452	55.3422	40.1123	45.7888	32.4412
Baboon	61.5466	46.6673	56.2221	41.5655	45.9811	33.1169
Goldhill	59.8992	44.7764	54.6677	39.9666	44.5267	33.7743

As illustrated in table (1), the secret text is hide in a part of the cover image and the accuracy of resulted stego image is mostly good and near to the accuracy of stego image resulted from the original LSB method.

Conclusions

This paper presents a new implementation of LSB hiding method using motif patterns. These types of patterns are diverse and strange and therefore it increases the accuracy and strength of the method against the attackers and intriguers when send and receive the image in communication media. The method is applied on different standard images with to hide different lengths of secret text comparing with original LSB method. The resulted accuracy shows how a convergence of two methods although the methods varies and complexity increases. The complexity of the proposed method increases its power and sobriety against attackers. As a future idea, there are many motif patterns can used to diverse the method and make it more difficult.

Conflict of interests.

There are non-conflicts of interest.

References

[1] Nashat D, Mamdouh L. An efficient steganographic technique for hiding data. J Egypt Math Soc 2019;27:1–14.
[2] Shafiq M, Tian Z, Bashir AK, Cengiz K, Tahir A. SoftSystem: smart edge computing device selection method for IoT based on soft set technique. Comput 2020;2020.
[3] Kadhim IJ, Premaratne P, Vial PJ, Halloran B. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing

2019;335:299–326.
[4] Wang X, Feng L, Zhao H. Fast image encryption algorithm based on parallel computing system. Inf Sci (Ny) 2019;486:340–58.
[5] Ja'far AMAA. Audio Hiding In Audio Files by Using Low-Bit Encoding. Informatics Inst Postgrad Stud M Sc Thesis, Baghdad, Iraq 2003.
[6] Singh S, Jung K-H. Special issue on emerging technologies for information hiding and forensics in multimedia systems. Multimed Tools Appl 2022:1–8.
[7] Khan AA, Shaikh AA, Cheikhrouhou O, Laghari AA, Rashid M, Shafiq M. IMG-forensics: Multimedia-enabled information hiding investigation using convolutional neural network. IET Image Process 2021.
[8] RĂDESCU R, Gliga R. An Introduction to Steganography. UPB Sci Bull C Electr Eng 2004;64:17–24.
[9] Thampi, Sabu M. Information hiding techniques: a tutorial review. arXiv preprint arXiv:0802.3746 , 2008.
[10] Gupta S, Goyal A, Bhushan B. Information hiding using least significant bit steganography and cryptography. Int J Mod Educ Comput Sci 2012;4:27.
[11] Wang JTL, Shapiro BA, Shasha D. Pattern discovery in biomolecular data: tools, techniques, and applications. Oxford University Press; 1999.
[12] Apostolico A, Parida L, Rombo SE. Motif patterns in 2D. Theor Comput Sci 2008;390:40–55.
[13] Liu L, Choi GPT, Mahadevan L. Wallpaper group kirigami. Proc R Soc A 2021;477:20210161.
[14] Memon F, Unar MA, Memon S. Image quality assessment for performance evaluation of focus measure operators. Mehran Univ Res J Eng Technol 2015;34:379–86.
[15] Fardo FA, Conforto VH, de Oliveira FC, Rodrigues PS. A formal evaluation of PSNR as quality measurement parameter for image segmentation algorithms. ArXiv Prepr ArXiv160507116 2016.
[16] Sumathi CP, Santanam T, Umamaheswari G. A study of various steganographic techniques used for information hiding. ArXiv Prepr ArXiv14015561 2014.
[17] Li X, Li J, Li B, Yang B. High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion. Signal Processing 2013;93:198–205.
[18] Luo H, Yu F-X, Chen H, Huang Z-L, Li H, Wang P-H. Reversible data hiding based on block median preservation. Inf Sci (Ny) 2011;181:308–28.
[19] Tao J, Li S, Zhang X, Wang Z. Towards robust image steganography. IEEE Trans Circuits Syst Video Technol 2018;29:594–600.
[20] Hu D, Wang L, Jiang W, Zheng S, Li B. A novel image steganography method via deep convolutional generative adversarial networks. IEEE Access 2018;6:38303–14.
[21] Rajput GG, Chavan R. A novel approach for image steganography based on LSB technique. Proc Int Conf Comput Data Anal, 2017, p. 167–70.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com