Using Digital Image as a Cover of Information Hiding: Review Paper

Ahmed saadi Abdullah 1 and Qasim Mohammed Hussein2

(1) Computer science department - computer science and mathematics – tikrit university- Iraq
(2) Tikrit University, College of Petroleum & Minerals Engineering
Salah Adin, Iraq
albashaahmed1985@gmail.com kassimalshamry@yahoo.com

Abstract
One of the most important topics that concern many researchers is how to make information that has a high degree of confidentiality hidden and not accessible except by the people who have the authority to view it, images are one of the most important multimedia that can be used as a cover to include the data, because the image contains how much a huge amount of data that can include confidential information in it, as well as the image is one of the most multimedia that is sent and received thus that the process of messaging with pictures does not arouse suspicion, this research provided a detailed study of a group of articles that used the image as a cover in the inclusion of information Confidentiality, and focus was on the most important domains of strength in each article. Articles were studied from 2013 to 2020 that were published at the containers of Scopes, and Google Scholar.

Key words: Steganography, Metric, PSNR, MSE, Q-factor, K-factor.

1. Introduction

The steganography techniques make use to invisible communication on unsecure channel, by hiding the existence of secret information inside other digital media from a third party so that intruders can't detect the communication[1]. Many types of digital media were used as a cover such as text, image, audio and video [2]. The images were widely used as a cover-up to hide secret information because containing huge data amounts, and altering some bits values don't effect on image perceptibility, although there are some limitations in some types of images, such as images generated using Julia Set[3], the nature and type of images and the steganography techniques play a major role in determining the robust of the steganography system[1]. The secret data may be expressed in different forms[4].
A system in steganography consists of three elements: the secret message, cover media that uses to hides the secret message within it, and the stego-cover that is the cover after embedding the secret information within it [3], as shown in Figure 1. The embedded data in the cover must be imperceptible to the observer[1,3]. This imperceptibility can be indicated by comparing the original image and its counterpart with embedded data to determine if their visual or aural are the same, or can be expressed by mathematical relationships between and the stego cover the original cover[3].

Steganography techniques may be implementing infrequency domain or spatial domain. In the frequency domain techniques, some transformations are used to transform the cover media before hiding the secret message within it. Whereas, in the spatial domain techniques, the secret data embed directly within the cover without any preprocessing[3].

The digital image is 2-dimension array of numbers that represent light intensities at various points, picture elements (called pixels) [5]. Many types of image are available such as binary, gray, color and multispectral images. For example, in RGB color image, each pixel contains 24-bit binary number, 8-bit for each color[5,6].
2. Evaluating the steganography techniques metrics

The researcher proposed a variety of steganography techniques and approaches; each one has its limitations and advantages. A number of metrics have been used to measure and evaluate the efficiency of the proposed techniques and approaches, which most of them focused on amount of effect of hidden data on the cover imperceptibility. Some of these metrics are[7,8]:

1. **Mean Square Error (MSE)**: it uses to measure the distortion in the cover after hiding the data within. Its equation is[5,7]:

   \[ MSE = \frac{1}{R \times C} \sum_{a=1}^{R} \sum_{b=1}^{C} (O_{image}(a, b) - S_{image}(a, b))^2 \]  

   Where \((R, C)\) represents the number of rows and the number of columns of the image, \(O_{image}\) is the original image before hiding the information in it, and \(S_{image}\) is the cover image after hiding the secret data within it.

2. **Peak Signal to Noise Ratio (PSNR)**: it use to measure the quality between the original cover and the stego-cover in the hiding process after the hiding data. The equation (2) is used to calculate the PSNR[5,7].

   \[ PSNR = 10 \times \log_{10} \left( \frac{R^2}{MSE} \right) \]  

   Where \(R\) is the maximum value of the byte, or pixel, for 8-bit it is 255.
3. The signal-to-noise ratio (SNR) is used to quantify how much a signal has been distorted by a noise, the higher SNR ratio shows the less obtrusive the background noise. The equation (3) is used to calculate the SNR metric[7].

\[
SNR = 10 \times \log_{10} \frac{\sum_{i=1}^{n} \sum_{j=1}^{m} o_{image}(a, b)^2}{\sum_{a=1}^{n} \sum_{b=1}^{m} (O_{image}(a, b) - S_{image}(a, b))^2} \quad \text{... (3)}
\]

4. Entropy: It is a statistical measure of randomness amount that presents in the cover. It calculated using equation (4)[7].

\[
Entropy = - \sum_{i=1}^{n} P_i \log P_i \quad \text{... (4)}
\]

5. Normalized cross correlation (NCC): This metric is used to measure the degree of similarity (or dissimilarity) between the original cover and stego cover, equation (5) is used to calculate it[7].

\[
NCC = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} O_{image}(a, b) S_{image}(a, b)}{\sum_{i=1}^{N} \sum_{j=1}^{M} (O_{image}(a, b))^2} \quad \text{... (5)}
\]

Where \(o_{image}(a, b)\) is the Original cover and \(S_{image}(a, b)\) is the stego cover.

6. Correlation (CORR)

\[
CORR = \frac{\sum_{a} \sum_{b} (o_{image}(a, b) - \overline{o_{image}(a, b)})(s_{image}(a, b) - \overline{s_{image}(a, b)})}{\sqrt{\sum_{a} \sum_{b} (o_{image}(a, b) - \overline{o_{image}(a, b)})^2} \sqrt{\sum_{a} \sum_{b} (s_{image}(a, b) - \overline{s_{image}(a, b)})^2}} \quad \text{... (6)}
\]

Where \(o_{image}(a, b)\) is the original image data average, \(S_{image}(a, b)\) is the average of image data after hiding process[9].

7. Q – factor: it measure the number of changed cover bits as a result of hiding process taking in the account the total number of secret data that will be hidden in the cover media, equation (7) is used to find it[7].

\[
Q – factor = \frac{\text{number of changing in cover bits}}{\text{number of secret text bits}} \quad \text{... (7)}
\]

Where the Q-factor has small, difference between original and stego cover is small, best efficient of the steganography algorithm where the values of the Q-factor = 0.
8. K-factor: it uses to measure the effecting of changing cover bits on the quality of the original cover depending on bits locations within their bytes. The k-factor can be calculated using equation (8)[7].

\[ k - \text{factor} = \frac{\sum_{i=1}^{n} wb_i}{\text{Total size of secret data (in bits)}} \quad \ldots (8) \]

Where n is the number of changed bits in the stego cover through hiding process, wb is the weight of the changed bit in bytes of stego cover.

The value of k-factor is minimum where its value is zero. whereas the maximum its value for each location in the byte is \((n*2^L)/m\). L is the number of changed bit within the cover, m is the number of secret text bits and n is the location of changed bit within the byte, \(0 \leq L \leq 7\)[7].

4. Critical Analysis

| Ref. | Type of image | Domain | Color spaces | Num. layer used | Used (AI) algorithm | Secret massage | Advantage | Disadvantage |
|------|---------------|--------|--------------|-----------------|-------------------|----------------|-----------|--------------|
| [1]  | Color         | Spatial | HSV          | One             | No                | Text           | Its dependence on a color layer is difficult to hide, and its dependence on a method not widely used | The amount of data that can be hidden is small |
| [2][4] | Color         | Spatial | RGB          | Three           | Yes               | Text           | The use of AI algorithms | Upon arriving at the required |
| [23] |               |        |              |                 |                   |                |                        |                          |
| Reference | Methodology | Spatial | RGB | Image Processing | User Input | Description |
|-----------|-------------|---------|-----|-----------------|------------|-------------|
| [26]      |             |         |     |                 |            | in choosing a user's pixel for concealment means randomly generated high scores to hide information. |
| [6][15]   |             | color   | Spatial | RGB | Three | No | Text | pixel, the confidential data will be revealed for its dependence on the LSB algorithm. |
| [18][36]  |             |         |       |                 |            | Relying on the least significant bit in secreting. |
| [39][40]  |             |         |       |                 |            | The method depends on the nature of the image, because the embedding depends on the attribute of cover image. |
| [41][46]  |             |         |       |                 |            | Reliance on conversion parameters gives strength to counting the discovery of hidden places. |
| [51]      |             |         |       |                 |            | Places that can be used for concealment will be few. |
| [9][10]   |             |         |       |                 |            | Using more than one bit per pixel means that you can. |
| [35][42]  |             |         |       |                 |            | Using a widely known method, which is. |
| [12]  | color | Spatial | RGB | Three | No   | image | hide a large number of data | dependence on a LSB method |
|-------|-------|---------|-----|-------|------|-------|-----------------------------|-----------------------------|
| [13][33] | Gray, color | Spatial | Gray.RGB,RG B | One,Three | No   | Image,Text,Text | The use of AES encryption method makes it difficult to know the meaning of the hidden text after its discovery |
| [37]  | color | Spatial | RGB | One,Three | No   | Text | Use two locations per pixel, which increases places that can be used to hide data | Using a widely known method, which is dependence on a LSB method |
| [14]  | Color | Spatial | RGB | One | No   | Text | The use of a color scheme other than the known system of the image | Using a widely known method, which is dependence on a LSB |
| [16][34] | Color | Spatial | RGB | Three | No   | Text,Text,Image | Dependence on some digital image processing techniques | Using a widely known method, which is dependence |

| [38][54] | Color | Spatial | RGB | Three | No   | Text,Text,Image | Dependence on some digital image processing techniques | Using a widely known method, which is dependence |
| No  | Color | Spatial | Transformation | LSB | Text |
|-----|-------|---------|----------------|-----|------|
| 1   | Color | Spatial | YUV,YIQ        | Two | No   |
|     |       |         |                |     | Text |
|     | [17],[22] |       | Use a color scheme other than the original image color scheme |
| 2   | Color | Spatial | RGB            | Three | No |
|     |       |         |                |     | image |
|     | [19] |       | Convert the image to be hidden to grayscale to reduce the number of bits |
| 3   | Gray  | Spatial | Gray           | One  | No   |
|     |       |         |                |     | Text |
|     | [20] |       | Depend on a method, rely on hiding the secret message bits with the cover bits, so there will be no change to the cover image |
| 4   | Color | Spatial | RGB            | Three | No |
|     |       |         |                |     | image |
|     | [21] |       | Use XoR twice with the red and using a widely known method |

To increase the efficiency of information hiding on a LSB.
| Reference | Color | Spatial | Type | No. | Medium | Methodology |
|-----------|-------|---------|------|-----|--------|-------------|
| [25]      | Color | Spatial | RGB  | Three | No     | Text        |
|           |       |         |      |       |        | green layer bits and use the blue layer to hide |
|           |       |         |      |       |        | method, which is dependence on a LSB |
| [27]      | Color | Spatial | RGB  | Three | No     | Audio      |
|           |       |         |      |       |        | Hide is not in consecutive pixels |
|           |       |         |      |       |        | Using a widely known method, which is dependence on a LSB |
| [28][47] | Color | Spatial | Color| Three | No     | Image, Text |
|           |       |         |      |       |        | Bits with the highest influence on Pascal were used in the inclusion process |
|           |       |         |      |       |        | If there is too much inclusion data, this will affect the cover and reveal it |
| [50]      | Gray  | Spatial | Gray | One  | No     | Text       |
|           |       |         |      |       |        | The embedding process depends on the Mosaic Image configuration |
|           |       |         |      |       |        | Re-hidden data is a complex process |
| [31] | Color | Spatial | RGB | Three | No | Text |
|------|-------|---------|-----|-------|----|------|
|      |       |         |     |       |    | It distributes the secret text to the three color layers thus increasing the area of the cover that can be used to hide |
|      |       |         |     |       |    | Using a widely known method, which is dependence on a LSB |

| [32] | Gray | Spatial | Gray | One  | No | Audio |
|------|------|---------|------|------|----|-------|
|      |      |         |      |      |    | It depends on some features of low impact fingerprint images |
|      |      |         |      |      |    | Big data cannot be hidden |

| [50] | Gray | Spatial | Gray | One  | No | Text |
|------|------|---------|------|------|----|------|
|      |      |         |      |      |    | Relying on the function of random number generation in choosing the locations of pixels that are hidden |
|      |      |         |      |      |    | Using a widely known method, which is dependence on a LSB |

5. Result And Conclusion

After studying the articles that have been analyzed in detail, the following is adopted for us, as shown in Figure 1-7.
Figure (1): Measurement criteria

Figure (2): Color spaces of cover image

Figure (3): Using AI algorithm
Figure (4): number of layers used as a cover in color space

Figure (5): type of secret information

Figure (6): type of cover image
Through Table (1) and Figures (1-7), it turns out that relying on the color image as a cover is more used than using other types (white and black, the image with a grayscale) because the amount of information that contains the color image is more than the information provided by other types. And the black and white image is considered one of the least used types of cover as a cover, because any change in this image can be clear and the number of data represented by this type of image is few, in addition to that it is clear that the dependence on the color image of type (RGB), as well as it becomes clear that the dependence on the three layers of colors is the most used to increase the information that confidential data can be included in it, as well as it turns out that the most used criteria in measurement is (psnr) because it is considered one of the criteria that clearly gives the amount of change that got the image cover, in addition to that it is clear that dependence on artificial intelligence algorithms is few, but most often, encryption algorithms are used for the data to be included, but the most types of confidential data that can be included are texts because the size of the texts is less than the size of the sound or image, therefore, the smaller the size of the confidential data, the more secret the inclusion process.

Reference:

1. Ahmed S. Abdullah," Text Hiding Based On Hue Content In Hsv Color Space ", International Journal Of Emerging Trends & Technology In Computer Science (Ijettcs), Volume 4, Issue 2, March-April 2015.
2. HazimNoman Abed, Noor HasanHassoon, Ahmed Luay Ahmed, Ismael SalihAlbayaty “Hiding Information in an Image Based on Bats Algorithm”, Iraqi Journal of Information Technology, volume 8, issue 2, 2018.
3. Nada Qasim Mohammed, Qasim Mohammed Hussein, Mohammed Sh. Ahmed."Suitability of Using Julia Set Images as a Cover for Hiding Information", 
Al-Mansour International Conference on New Trends in Computing, Communication, and Information Technology, IEEE Xplore, 2018.

4. Omar YounisAbdulhameed, "Hiding a Secret Information in Image Using Gravitational Search Algorithm", Diyala Journal For Pure Science, volume 14, issue 1, 2018.

5. KI Al-Saif, AS Abdullah, "Color image enhancement based on contourlet transform coefficients", Australian Journal of Basic and Applied Sciences, 2013

6. Ahmed Saadi Abdullah, "Improving Message Embedding By Using Some Attributes Of Color Image", Raf. J. of Comp. & Math's., Vol. 13, No.2, 2019.

7. Qasim Mohammed Hussein, "New Metrics for Steganography Algorithm Quality", International Journal of Advanced Science and Technology, Vol. 29, No.02,(2020).

8. Qasim Mohammed Hussein, Hiding Message in Color Image Using Auto Key Generator, 3rd International Conference on Advanced Computer Science Applications and Technologies, Amman, Jordan, 2014.

9. Khalil Ibrahim Alsaif, Meaad M. Salih, "Contourlet Transformation For Text Hiding In Hsv Color Image", International Journal Of Computer Networks And Communications Security, Vol. 1, No.4, September 2013.

10. Amer A. Al-Lehiebe, "Ciphered Text Hiding in an Image using RSA algorithm", J. Of College Of Education For Women, volume 26, issue 3, 2015.

11. Abdullah H. Muhammad, "Hiding the Text in Image of Variable Size", Diyala Journal For Pure Science, Volume: 11 Issue: 2 Pages: 44-55, 2015.

12. AymenMudheher Badr, Mohamed laythtalal and GhassanSabehc, "Image in Image Steganography based on modified Advanced Encryption Standard and Lest Significant Bit Algorithms", Journal of University of Babylon for Pure and Applied Sciences, Vol.(26), No.(8): 2018.

13. KamaldeepJoshi, Swati Gill, and RajkumarYadav, "A New Method of Image Steganography Using 7th Bit of a Pixel asIndicator by Introducing the Successive Temporary Pixel in theGray Scale Image", Journal of Computer Networks and Communications, 2018.

14. Khan Muhammad, Jamil Ahmad, Haleem Farman and Muhammad Zubair, "A Novel Image Steganographic Approach for Hiding Text in Color Images Using HSI Color Model", Middle-East Journal of Scientific Research 22 (5), 2014: 647-654, 2014.

15. DeepaliSingla and Dr. MamtaJuneja, "New Information Hiding Technique usingFeatures of Image", JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE, VOL. 6, NO. 2, MAY 2014.

16. MamtaJuneja and Parvinder Singh Sandhu, "A New Approach for Information Security using an Improved Steganography Technique", J Inf Process Syst, Vol.9, No.3, September 2013

17. Suhaila Mohammed, Shaymaa Ahmed, Ghusoon Mohammed, and DhuhaAbduljabbar, "Block-based Image Steganography for Text Hiding Using YUV Color Model and Secret Key Cryptography Methods", Australian Journal of Basic and Applied Sciences, 11(7) May 2017.
18. AzalHabeeb,” A NEW METHOD FOR HIDING TEXT IN A DIGITAL IMAGE”, JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY, Vol. 55 No. 2, 2020.

19. Allen Tom , Anu V Thomas , Jerin Jose , Maria, P. Darsana,“Hiding Host Image using a Cover Image”, International Journal of Engineering Research & Technology, 2015.

20. Hussein L. Hussein, Ahmed A. Abbass,, Sinan A. Naji, Salam Al-augby and Jasim H. Lafta,”Hiding text in gray image using mapping technique,“ IOP Conf. Series: Journal of Physics, 2018

21. Hamid Mohammed Farhan , Zena Ahmed Alwan , ”Improved method using a two Exclusive-OR to binary image in RGB color image steganography”, International Journal of Engineering & Technology, 2018.

22. Ali Nasser Hussaina, Entidhar Mhawes Zghairb, ”Efficient Text Message Hidden Technique Using YIQ Model”, JOURNAL OF MADEMAT ALELEM COLLEGE , Volume: 9 Issue: 1 Pages: 217-228 , 2017.

23. Omar Younis Abdulkhameed. “Hiding A Secret Watermark In Image Using Intelligent Water Drops Algorithm”, Diyala Journal For Pure Science , volume 13 , issue 2 , 2017.

24. Dr. Yossra H. Ali Ahmed Y. Yousif Tayseer A. Atia , “Distributed AMELSB Replacement Method For Text Hiding”, “, Iraqi Journal of Information Technology, volume 2 , issue 2 , 2018.

25. Falih Hassan owaid,”INFORMATION HIDING USING STAGAEROGRAPHS SYSTEM USING LSB-TECHNIQUE”, Journal of Baghdad College of Economic sciences University, Issue: 38 Pages: 376-394, 2015.

26. Kartik Sharma , Ashutosh Aggarwal, Tanay Singhania, Deepak Gupta, Ashish Khanna, “Hiding Data in Images Using Cryptography and Deep Neural Network”, Journal of Artificial Intelligence and Systems, 2019.

27. B. Geetha Vani L. K Sathya Suneetha S. Susmitha,” Embedding Audio in Image for Hiding Information Using MSB Technique”, Volume 6, Issue 6, June 2016

28. Deepesh Rawat, Vijaya Bhandar, “A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image”, International Journal of Computer Applications, Volume 64– No.20, February 2013.

29. Kanar M. Sami, “Embedding Data In Personal Image By Using Mosaic Image”, Journal of Education and Science, Vol. 28, No.4, 2019.

30. Sabah A. Gitaffa,” IMPLEMENTATION OF HIDING SECURED FINGERPRINT IN FACE IMAGE FOR BIOMETRIC APPLICATIONS”, Vol. 20, No.1, January 2016.

31. Jinan N. Shehab  , Haraa Raheem Hatem  , Omar Abdul Kareem Mahmood,”HIDING (1-8) MULTIMEDIA FILES IN ONE COLOR IMAGE”, Diyala Journal of Engineering Sciences, Vol. 10, No. 3, September 2017.

32. Tawfiq A. Al-Asadi,” Sound file hiding in fingerprint image”, Journal of University of Babylon, 2013.
33. Zainb Bakar Dahoos, “Hide Encoded Text Within the Image by Using the Third Least Significant Bit”, Journal of University of Thi-Qar Vol.9 No.4 Dec. 2014.
34. Arun Kumar Singh, Juhi Singh, Dr. Harsh Vikram Singh, “Steganography in Images Using LSB Technique”, International Journal of Latest Trends in Engineering and Technology, 2015.
35. Srikanth. V, “Secret Image Hiding in an Enhanced Steganography Approach using IWT”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 5, Issue 4, April 2016.
36. Karthikeyan B, Asha S, Poojasree B, “Gray Code Based Data Hiding in an Image using LSB Embedding Technique”, Volume-8, Issue-1, May 2019.
37. Ashwini Palimkar, Dr. S. H. Patil, “Using SBR Algorithm To Hide The Data Into The JPEG Image”, International Journal of Security (IJS), Volume (8), Issue (2), 2014.
38. Alyaa Hasan Zwiad, “Proposal Compression Algorithm to Hide Multiple Text Images Based on Bit Plane Slicing”, Iraqi Journal of Information Technology. V.8 N.4, 2018.
39. Ali Fattah Dakhil, “Steganography: Applying LSB Algorithm to Hide Text in Image”, Journal of Al-Qadisiyah for computer science and mathematics Vol.9 No.1 Year 2017.
40. Wejdan A. Amer, “Efficient text in image hiding method based on LSB method principle”, Iraqi Journal of Science, Vol. 57, No.2, 2016.
41. Hayder I. Hendi, Shaker K. Ali, “PROPOSED METHOD OF INFORMATION HIDING IN IMAGE”, Journal of Kufa for Mathematics and Computer, Vol. 2, No. 1, May 2014.
42. Jamila Harbi S, “New Method of Image Hiding”, Iraqi Journal of Information Technology, Vol. 6 No. 2, May 2014.
43. Qasim Mohammed Hussein, Ahmed Saadi Abdullah, Nada Qasim Mohammed, “The Efficiency Of Color Models Layers At Color Images As Cover In Text Hiding”, Tikrit Journal Of Pure Science, Vol. 21, No. 1, Pp. 130–139, 2016
44. Rajaa Ahmed Ali, Muntadher Khamees Mustafa, Ali A. Alani, “Hiding Information Using Circular Distribution”, Journal of College of Education, No. 1, 2015.
45. ZEYAD SAFAA YOUNUS ALSAFFAWI, “Image Steganography by Using Exploiting Modification Direction and Knight Tour Algorithm”, Journal of Al-Qadisiyah for Computer Science and Mathematics, Volume 8, Issue 1, 2016.
46. Ahmed Kadem Hamed Al-Saedi, “A method to hide text in image”, Journal of Missan Researches, Vol (12), No (24), 2016.
47. Rawsam A. Hasan and Israa M. Alwan, “Image Steganography Algorithm with Minimizing Distortion In Cover Image”, Al- Mustansiriyah J. Sci. Vol. 24, No 3, 2013.
48. Asmaa Abdul-Razzaq Al-qaisi, “Audio Hiding in Color Image Using SLT Schemes”, Iraqi Journal of Science, Vol. 57, No.3, 2016.
49. Yossra Hussain Ali, Hussein Jaeiz Mankhi, "Hiding and Encryption of Secret Image Using Secret Sharing Scheme", Iraqi Journal of Science, Vol. 57, No. 4, 2016.
50. Elaf Ali Abbood, Rusul Mohammed Neamah, Shaymaa Abdulkadhm, "Text in Image Hiding using Developed LSB and Random Method", International Journal of Electrical and Computer Engineering, Vol. 8, No. 4, August 2018.
51. Geeta D. Rote, Dr. A. M. Patil, "Steganography with Cryptography Technique For Data Hiding", International Journal of Science and Research, 2013.
52. Abdelfatah A. Tamimi, Ayman M. Abdalla, Omaima Al-Allaf, "Hiding an Image inside another Image using Variable-Rate Steganography", International Journal of Advanced Computer Science and Applications, Vol. 4, No. 10, 2013.
53. ISRAA S. AHMED, "Hiding Secret Text in Image Using RC2 and Serpent Algorithm", Journal of The Iraqi University, 2018.
54. Haraa R. Hatem, "Hiding 9 Gray Images In RGB Image and Using Filters For Noise Removing", Engineering and Technology Journal, Vol. 36, Part A, No. 11, 2018.