

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/347083013>

Modified Least Significant Bit Technique for Securing Medical Images

Chapter · November 2020

DOI: 10.1007/978-3-030-63396-7_37

CITATIONS

6

READS

61

4 authors:



Roseline Ogundokun
Landmark University

174 PUBLICATIONS 1,548 CITATIONS

[SEE PROFILE](#)



Oluwakemi Christiana Abikoye
University of Ilorin

108 PUBLICATIONS 559 CITATIONS

[SEE PROFILE](#)



Sanjay Misra
Institute for Energy Technology

817 PUBLICATIONS 8,621 CITATIONS

[SEE PROFILE](#)



Awotunde J. Bamidele
University of Ilorin

180 PUBLICATIONS 1,665 CITATIONS

[SEE PROFILE](#)



Modified Least Significant Bit Technique for Securing Medical Images

Roseline Oluwaseun Ogundokun¹ ,
Oluwakemi Christiana Abikoye² , Sanjay Misra³,
and Joseph Bamidele Awotunde² 

¹ Department of Computer Science, Landmark University,
Omu Aran, Kwara State, Nigeria
ogundokun.roseline@lmu.edu.ng

² Department of Computer Science, University of Ilorin, Ilorin,
Kwara State, Nigeria

³ Department of Electrical and Information Engineering, Covenant University,
Ota, Ogun State, Nigeria

Abstract. The confidentiality and safety of patient records is a significant concern for medical professionals. So protections must be placed to guarantee that illegal individuals do not have access to medical images (Patient's description). Hence, the objective of this study is to secure digital medical images being transmitted over the internet from being accessed by an intruder. The study, therefore, proposed a modified Least Significant Bit (LSB) algorithm implemented on a MATLAB 2018a programming environment, and the proposed system was compared with the existing system using three performance metrics which are PSNR, MSE and SSIM. The result showed that the proposed approach outperformed the current standard methods by producing a more robust, high capacity, and highly imperceptible stego image. The comparative analysis conducted also showed that the PSNR value is higher, and MSE value is lower when compared with existing systems. It was concluded that the projected technique accomplishes excellently in making the medical image transmitted to be more secured, robust, and invisible, thereby making the communication to be unnoticeable by an intruder or attacker.

Keywords: Steganography · Medical image · Least significant bit · PSNR · MSE · SSIM

1 Introduction

These days, the growing of information technology, particularly systems such as mobile communication, the computer network, and digital interactive program applications, has unlocked innovative possibilities for steganography and concealing procedures for information [1]. Data security has been a critical topic in recent years as a product of the massive developments in information technologies as well as the tremendous rise in computer networks used by data transmission and receiving [2, 28]. Researchers then concentrated on developing data security systems, and experiments

were carried out to refine existing strategies and introduce new ones to secure data from hackers [3]. Cryptography is a tool used to confirm the details of a message by scrambling the message in such a way that nobody can decode apart from the individual who has the undisclosed password. It also a means of ensuring that messages were not altered throughout the communication cycle. Many methods for encoding and decoding messages to secure them have been developed, nevertheless with the emergence of the internet, these methods became inefficient [3]. New techniques were, therefore, necessary to resolve this problem, and this led to the advent of the principle of steganography [4–6].

Steganography refers to know-how and the ability to hide messages or any communication between the source and the destination of the undisclosed message via an electronic channel transferring the message [7–10]. The term (steganography) arising out of (steganos) denoting (concealed) and (graph) denoting (script) denotes (hidden writing) [11, 12]. Steganography is a way of covering coded communications in a plain concealment medium such as stegograms so that the presence of the hidden messages would not be revealed to an accidental observer [13–17, 49, 50]. Using steganographic strategies, material that is perceptually and statistically undetectable can be contained inside images, audio, video documents, or text. The electronic object is the utmost well-known concealment medium because of its extreme level of verbosity [18, 19]. The equivalent technique could be utilized in video steganography to entrench a communication into all the video edges [20, 21]. Audio steganography integrates the message as noise in a concealment acoustic medium at a rate of recurrence that is below the normal listening range [22]. It's discovered that steganography disguises the presence of hidden communication, equating steganography with cryptography [23], while cryptography masks the meaning of the hidden communication [1].

Therefore, the objective of this study is to secure digital medical images being transmitted over the internet or an electronic medium from being accessed by an intruder. The study, therefore, proposed a modified Least Significant Bit algorithm implemented on a MATLAB 2018a programming environment and submitted to conduct a comparative analysis of the developed system with the existing system using three performance metrics which are PSNR, MSE and SSIM.

The remaining part of the paper are prearranged as follows: Sect. 2 discussed the related research works, Sect. 3 described the proposed method for this study, the datasets used for the implementation of the system and the stages with the algorithms utilized for performance, Sect. 4 discussed the results obtained from the implementation of the system, and this also showed the interfaces of the performance. The qualitative evaluation metrics used for the developed system analysis and the comparative analysis of the developed system with previous researches were discussed in Sect. 5. This investigation was concluded in Sect. 6.

2 Related Works

Several studies have investigated the various Steganography image approaches utilized to conceal messages in concealment objects [24–27]. The critical problem of communication concealing methods is to embed the most significant volume of communication in the cover object while maintaining consistency, including the reliability and power of the system in challenging hackers with electronic attacks. Several techniques and methods have been proposed to mask image data due to the immense number of visual imageries on the internet and as well as the straightforwardness of managing imageries in a concealment procedure [29–31].

To this end, scholars have tried to use new methods to deal with the accelerated evolution of concealing strategies to obtain specific outcomes. Researchers recently concentrated on enhancing the hiding mechanism in images by utilizing diverse approaches, for instance, LSB.

The LSB structure is prevalent plus is the utilization of Images to conceal data. This approaches the concealment medium specifically by modifying the least essential bit size to insert the details about the undisclosed communication and make it very difficult to identify the evolving mechanism in the medium from the people's eyes. Hence, it a robust technique to add hidden knowledge by effecting imperceptible changes in the cover object [32, 33].

[34] proposed the Manipulating Alteration Path approach where the image was divided into multiple clusters comprising n pixels to inject the undisclosed file into $(2n + 1)$ -ary encryption. The amount of a particular pixel within a category was raised or decreased by one during the insertion phase. Their method's drawback is the reduced concealment object features because the group size had two pixels.

[35] proposed a structure to develop the so-called EMD process (IEMD). Compared to the standard EMD approach, this system collected a significant volume of data without compromising the concealment object features. This process transformed the undisclosed communication into an undisclosed digit in an 8-ary encrypting structure and inserted all secret communication into a collection of two pixels.

[36] proposed a system for improving the conventional EMD approach by embedding secret messages in all pixels using every pixel in the image. The entrenched material in the picture was duplicated when contrasted with the traditional method in the process. Utilizing the approach overpowered the detrimental features of the EMD system plus integrated the best volume of facts as long as maintaining the image characteristics.

[37] proposed an Opt EMD structure to what end the association amid the number of pixels (n) in the whole cluster with the number of payloads contained in the image was used to minimize the image distortion. This scheme achieved high efficiency, but the volume of the payload was affected.

[38] introduced a scheme using the methods of encoding Huffman, affine cypher, and Knight Tour. The undisclosed communication was scrambled and compacted in the procedure utilizing affine encryption and Huffman encoding, after that the new message was entrenched into a concealment object using LSB and Knight's tour approaches.

The item was translated into the colour space of YCbCr, and the undisclosed communication was inserted in the Cb part.

[39] brought forward a system utilizing better techniques for coding EMD and Huffman. This approach compacts the mystery message using Huffman coding; after that, the mystery cypher was encoded in an image utilizing the EMD approach, whereas the collection of pixels used for entrenching was divided into two subcategories of 2 and 3 pixels successively to maximize the payload beyond effecting the concealment object characteristics.

[40] implemented a data hiding structure that would calculate the sum of the I structure contained in the image utilizing the EMD process. The undisclosed message in this scheme was represented using (cn-ary). Then, utilizing C of diverse approaches to change its rate after that the set of (n) pixels was used to enclose the undisclosed communication in it.

[41] recommended a structure utilizing the LZW technique to minimize the magnitude of undisclosed details and raise the payload then use the Knight tour system as well as EMD structure to incorporate new knowledge into the concealment picture.

[42] set out a framework for developing the EMD process. The picture was separated into n pixels in the scheme and was utilized to implant 2kn-ary figures in the core section. The technique of Image Steganography was proposed by combining the methods of cryptography and steganography in this investigation. First, Vigenere cypher and Huffman encrypting were used to scramble and compact undisclosed communication. This means preserving the details and raising the size of the unknown communication for integration into the concealment picture utilizing the EMD procedure. Using the Knight tour scheme and arbitrary function, it was then enhanced to improve robustness and reliability by selecting the wedges and clusters used to enclose the secret communication into a particular pixel. This as well helps to maintain the stego-picture consistency and brought it nearer to the camera cover.

To ensure internet stability, [43] established a new LSB replacement scheme using stego-key guidance. The system's payload and imperceptibility were models as a search issue for optimization. Finally, using a messy map, the critical information was arbitrarily inserted into the cover image. The recovery of classified information requires all procedures being reversed. The technique got 44.09db and 0.97 respectively as PSNR and SSIM.

[48] recommended image steganography established on integrated files plus inverted bit LSB replacement. The research intended to deliver three layers of security moderately than entrenching the file's bit straight forward into the concealment object. The pixels were engendered arbitrarily via a pseudo-random number generator after the undisclosed communication is concealed inside the concealment object utilizing an inverted LSB approach.

The findings from the review show that the standard LSB steganography has mostly been used for hiding information, and it has shown that it had some limitation of perceptibility, distortion, the cover image is not robust.

3 Material and Method

3.1 Proposed Method

The need to develop reliable mechanisms for transmitting and receiving information through a contact channel is a significant issue. An innovative method is anticipated to cover the medical image by changing the LSB steganography approach to mask a considerable volume of records and given the accuracy of stego-images succeeding incorporating the medical image into the file. This provides an extreme degree of confidentiality in concealing the details inside the cover picture and through the method's intensity in the digital occurrence situation. Such elements are confrontations facing the technique of hiding messages in photographs.

The stages of the projected method comprise

Embedding Procedure: The medical image is entrenched within the concealment object by utilizing a modified LSB procedure called Circular Shift LSB and gives an output called stego image which is an image hiding the medical image in it.

Extraction Process: The stego image is detached out of the stego image using the modified LSB procedure called the Circular Shift algorithm.

3.2 Materials

Data Availability.

The medical images which are mammogram images exploit in this investigation are openly obtainable at mini-MIAS: <http://peipa.essex.ac.uk/pix/mias/>.

Sample Medical Images.

Figure 1 displays the sample medical images, which are a mammogram used for the testing of the developed system.

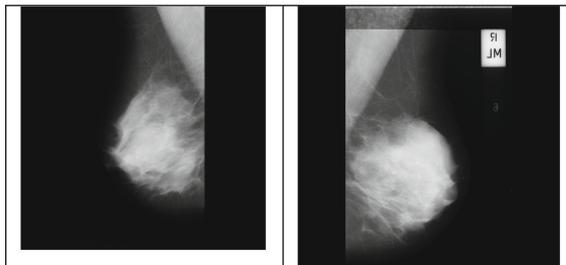


Fig. 1. Sample medical image

3.3 Proposed Method Algorithms

Embedding Algorithm

Input: Medical image, Cover object, Stego key

Output: Stego image

Phase 1: Enter the medical image and the stego key

Phase 2: Read the given message of the medical image

Step 3: Change the pictures to ASCII arrangement

Phase 4: Embed the ASCII format into the cover image using the modified LSB algorithm called Circular Shift Method

Phase 5: Produce a stego image

Extracting Algorithm

Input: Stego image, Stego key

Output: Medical image, Cover image

Phase 1: Enter the stego image and the stego key

Phase 2: Read given stego image

Phase 3: Change the picture to ASCII arrangement

Phase 4: Extract the ASCII format from the stego image utilizing the projected system algorithm called Circular Shift Method

Phase 5: Produce the medical image and the initial cover image

4 Results and Discussion

The study exploits the use of MATLAB for the implementation of the proposed technique, the system also employed medical images for the testing of the system. The following interfaces display the results from the performance of the developed system.

4.1 Embedding Phase of the System

Figure 2 shows the proposed system interface for the secured medical information system.

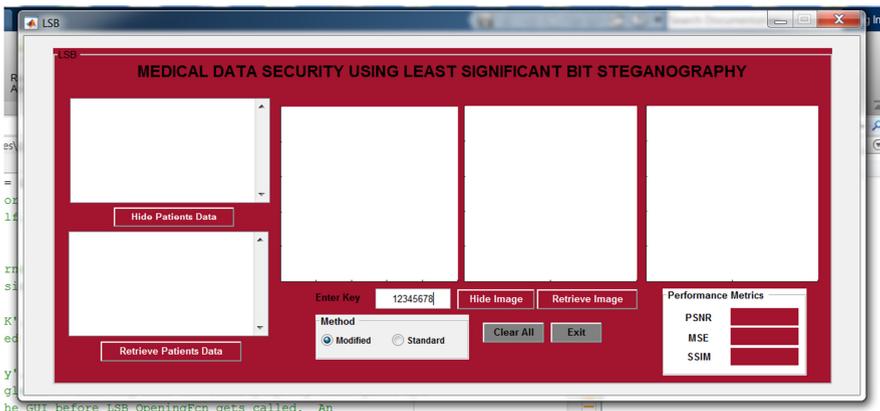


Fig. 2. The interface of the system

Figure 3 displays the interface showing the procedure of the embedding technique.

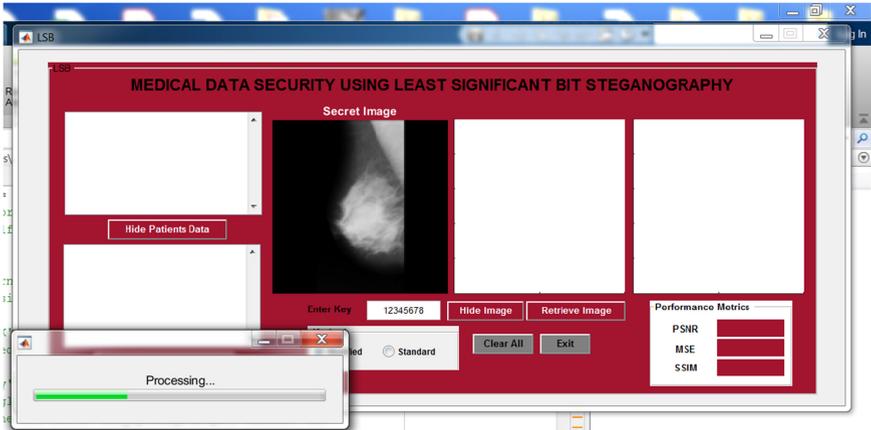


Fig. 3. Embedding process in progress

Figure 4 shows the interface displaying the result of the embedding stage of the system. This demonstrates the initial concealment object and the steganographic image (that is object hiding the patient’s information).



Fig. 4. The interface of embedding result

4.2 Extracting Phase of the System

Figure 5 displays the extraction phase for the scheme, and here the stego key for access to the secured patient information is entered.

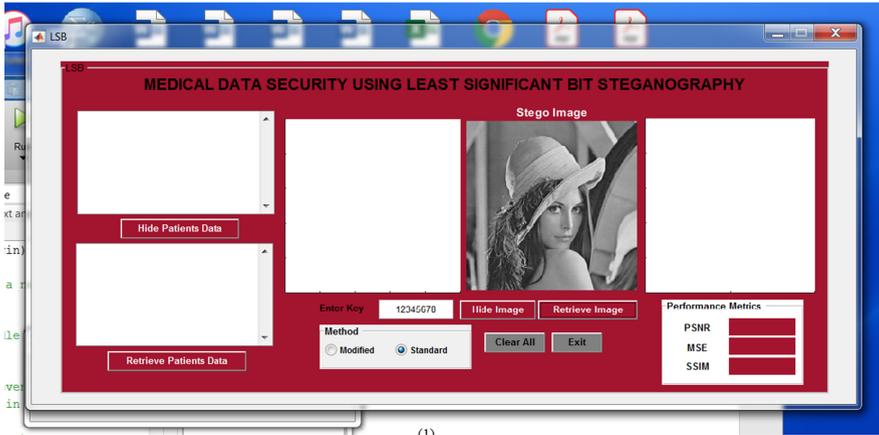


Fig. 5. The interface of the extraction phase

Figure 6 shows the folder from where the saved stego image is being stored and picked for extraction.



Fig. 6. The interface of folder having the message sent

Figure 7 displays the extraction phase of the projected scheme, and the confidential information is shown on the retrieve message and also the initial cover message.

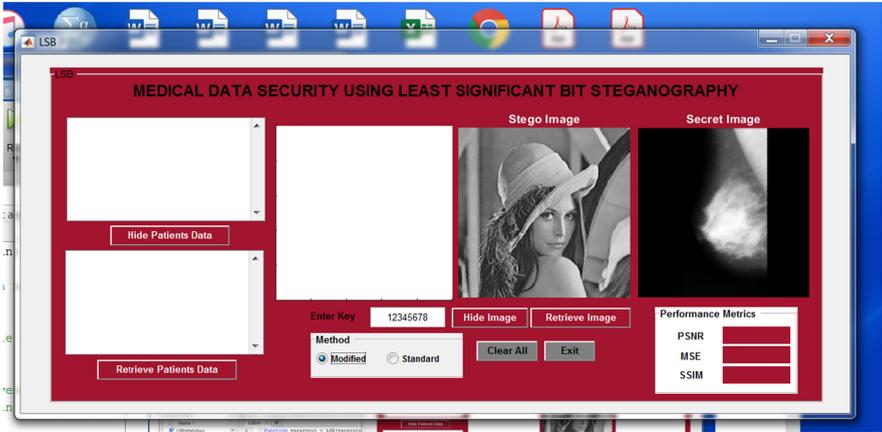


Fig. 7. The interface of the extraction phase

5 Qualitative Evaluation Metric

Mean square error (MSE), peak signal-to-noise ratio (PSNR), normalization of cross-correlation (NCC), structural similarity index (SSIM), plus histogram are generally utilized to assess the characteristics of stego-images virtually [44]. In this investigation, the authors used three out of the metrics; for instance, the MSE, PSNR, and SSIM.

Mean Square Error (MSE).

This tests the quality of a stego image by determining the variation amid the concealment object and the stego image [45].

$$MSE = \frac{1}{mn} \sum_0^{m-1} \sum_0^{n-1} c - s^2 \quad (1)$$

m and n are the entered images number of rows and columns correspondingly, C is the cover-object while S is the stego-image.

Peak Signal to Noise Ratio (PSNR).

The PSNR calculates the rate at which the encoded information in the decibel (dB) variable distorts a stego-image as a result. A more excellent PSNR value represents the advanced stego-image efficiency and is measured as [46].

$$PSNR = 10 \log \left(\frac{255^2}{MSE} \right) \quad (2)$$

Where 255 is the utmost pixel value in both stego-image plus concealment object.

Structural Similarity Index (SSIM).

SSIM contrasts two equivalent pictures using their configurations to values ranging from -1 to 1. The closest the SSIM is to 1 the. The resemblance between the two images given and is determined [47].

5.1 Comparative Evaluation

Three qualitative evaluation metrics were used for the comparative analysis with previous researches, and these were used in comparing with two earlier pieces of research which are Younus & Hussain, 2019, and Bhardwaj & Sharma, 2016.

Table 1. Comparative analysis of the developed system with previous works

Methods	Payload	PSNR value	MSE value	SSIM value
Younus & Hussain [2]	32.768 bytes	58.12	—	—
Bhardwaj & Sharma [48]	24.964 bytes	51.98	0.2499	—
Proposed System	32.768 bytes	82.35	0.0744	0.99

Table 1 illustrates the values of PSNR, MSE, and SSIM for Younus & Hussain, (2019), Bhardwaj & Sharma, (2016), and the proposed system. It displays the value of payload, PNSR value, MSE value, and SSIM. Consequently, it was deduced that the PSNR value is higher than 30 which is 82.35 and the MSE value is increased with 0.0744, which signifies that the suggested approach is ideal at entrenching the medical image inside the concealment object by implanting a considerable quantity of medical images within it and maintaining the concealment object quality. The SSIM value is similar to 1, which means that the stego image is the same as the initial concealment image of good quality.

6 Conclusion

The critical aim of steganography techniques is to hide a vast volume of details within an image without compromising the appearance of the picture. The robustness and reliability of these systems also offer protection against cyber threats. For this study, an innovative technique was recommended, which is the circular shift (Modified LSB) steganography technique to mask the medical image within cover images. The proposed scheme was tested utilizing PSNR, MSE, and SSIM to determine the consistency and utilizing the embedding degree to exam the payload. The analytical findings indicate that the suggested scheme's efficiency and payload are higher than conventional approaches. Furthermore, the protection and robustness of the presented process were considered to be satisfactory in the face of electronic attacks. The system can be checked in future works by producing other electronic threats, and other techniques can be used for random selection as well.

References

1. Attaby, A.A., Ahmed, M.F.M.M., Alsammak, A.K.: Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3. *Ain Shams Eng. J.* **9**, 1965–1974 (2018). <https://doi.org/10.1016/j.asej.2017.02.003>
2. Younus Z.S., Hussain, M.K.: Image steganography using exploiting modification direction for compressed, encrypted data. *Journal of King Saud University–Computer and Information Sciences*, an article in press (2019). <https://doi.org/10.1016/j.jksuci.2019.04.008>
3. Morkel, T., Eloff, J., Olivier, M.: An overview of image steganography. In: *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)*, Sandston, South Africa (2005)
4. Rehman, A., Alqahtani, S., Altameem, A., Saba, T.: Virtual machine security challenges: case studies. *Int. J. Mach. Learn. Cybern.* **5**(5), 729–742 (2013). <https://doi.org/10.1007/s13042-013-0166-4>
5. Kumar, V., Kumar, D.: Performance evaluation of modified colour image steganography using discrete wavelet transform. *J. Intell. Syst.* (2017). <https://doi.org/10.1515/jisys-2017-0134>
6. Younus, Z.S., Younus, G.T.: Video steganography using knight tour algorithm and LSB method for encrypted data. *J. Intell. Syst.* (2019) <https://doi.org/10.1515/jisys-2018-0225>
7. Habibi, M., Karimi, R., Nosrati, M.: Using SFLA and LSB for text message steganography in 24-bit RGB colour images. *Int. J. Eng.* **2**(3), 68–75 (2013)
8. Tejeshwar, G.: Colour image steganography using LZW compression and fisher-yates shuffle algorithm. *Int. J. Innovative Res. Dev.* **3**(6), 54–61 (2014)
9. Ranjani, J.J.: Data hiding using pseudo magic squares for embedding high payload in digital images. *Multimedia Tools Appl.* **76**(3), 3715–3729 (2016). <https://doi.org/10.1007/s11042-016-3974-1>
10. Taha, A., Hammad, A., Selim, M.: A high capacity algorithm for information hiding in Arabic text. *Journal of King Saud University*, pp. 1–8 (2018) <https://doi.org/10.1016/j.jksuci.2018.07.007>
11. Kalra, M., Singh, P.: EMD techniques of image steganography a comparative study. *Int. J. Technol. Explor. Learn.* **3**(2), 385–390 (2014)
12. Hashim, M., Rahim, M.: Image steganography based on odd/even pixels distribution scheme and two parameters random function. *J. Theor. Appl. Inf. Technol.* **95**(22), 5977–5986 (2017)
13. Christiana, A.O., Oluwatobi, A.N., Victory, G.A., Oluwaseun, O.R.: A secured one time password authentication technique using (3, 3) visual cryptography scheme. *J. Phys. Conf. Ser.* **1299**(1), 012059 (2019)
14. Marvel, Jr, Boncelet, C., Retter, C.: Spread spectrum image steganography. *IEEE Trans. Image Process.* **8**, 1075–83 (1999)
15. Akande, N.O., Abikoye, C.O., Adebisi, M.O., Kayode, A.A., Adegun, A.A., Ogundokun, R. O.: Electronic medical information encryption using modified blowfish algorithm. In: Misra, S. (ed.) *ICCSA 2019. LNCS*, vol. 11623, pp. 166–179. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-24308-1_14
16. Memon N, Chandramouli R. Analysis of LSB based image steganography techniques. In: *Proceedings of IEEE ICIP* (2001)
17. Abikoye, O.C., Ojo, U.A., Awotunde, J.B., Ogundokun, R.O.: A safe and secured iris template using steganography and cryptography. *Multimedia Tools and Appl.* **79**(31), 23483–23506 (2020). <https://doi.org/10.1007/s11042-020-08971-x>

18. Marvel, Jr, Boncelet, C., Retter, C.: Spread spectrum image steganography. *IEEE Trans. Image Process.* **8** 1075–83 (1999)
19. Memon N, Chandramouli R.: Analysis of LSB based image steganography techniques. In: *Proceedings of IEEE ICIP* (2001)
20. Morimoto, N., Bender, W., Gruhl, D., Lu, A.: Techniques for data hiding. *IBM Syst. J.* **35**, 313–316 (1996)
21. Doerr, G., Dugelay, J.L.: Security pitfalls of frame-by-frame approaches to video watermarking. *IEEE Trans. Signal Process. Suppl. Secure. Media* **52**, 2955–2964 (2004)
22. Gopalan K.: Audio steganography using bit modification. In: *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '03)*, vol. 2 (6), pp. 421–24 (2003)
23. Anderson, R., Petitcolas, F.: On the limits of steganography. *IEEE J. Select Areas Commun. (J-SAC)* **16**, 474–481 (1998)
24. Kutade, P., Bhalotra, P.: A survey on various approaches of image steganography. *Int. J. Comput. Appl.* **109**(3), 1–5 (2015)
25. Prajapati, H., Chitaliya, N.: Secure and robust dual image steganography: a survey. *Int. J. Innovative Res. Comput. Commun. Eng.* **3**(1), 534–542 (2015)
26. Kalaivanan, S., Ananth, V., Manikandan, T.: A survey on digital image steganography. *Int. J. Emerg. Trends Technol. Comput. Sci.* **4**(1), 30–33 (2015)
27. Hussain, M., Hussain, M.: A survey of image steganography techniques. *Int. J. Adv. Sci. Technol* **54**, 113–124 (2013)
28. Idakwo, M.A., Muazu, M.B., Adedokun, E.A., Sadiq, B.O.: An extensive survey of digital image steganography: state of the art. *J. Sci. Technol. Edu.* **8**(2), 40–54 (2020)
29. Chang, C., Tai, W., Chen, K.: Improvements in EMD embedding for large payloads. In: *Third International Conference on International Information Hiding and Multimedia Signal Processing (IIH-MSP 2007)*, pp. 473–476. *ACM* (2007)
30. Cheddad, A., Condell, J., Curran, K., McKeivitt, P.: Digital image steganography: survey and analysis of current methods. *Signal Process.* **90**, 727–752 (2010). <https://doi.org/10.1016/j.sigpro.2009.08.010>
31. Maniriho, P., Ahmad, T.: Information hiding scheme for digital images using difference expansion and modulus function. *J. King Saud Univ.-Comput. Inf. Sci.* 1–13 (2018). <https://doi.org/10.1016/j.jksuci.2018.01.011>
32. Chan, C., Cheng, L.: Hiding data in images by simple LSB substitution. *Pattern Recogn.* **37**, 469–474 (2004). <https://doi.org/10.1016/j.patcog.2003.08.007>
33. Shjul, A., Kulkarni, U.: A secure skin tone based steganography using wavelet transform. *Int. J. Comput. Theory Eng.* **3**(1), 16–22 (2011)
34. Zhang, X., Wang, S.: Efficient stenographic embedding by exploiting modification direction. *IEEE Commun. Lett.* **10**(11), 781–783 (2006). <https://doi.org/10.1109/LCOMM.2006.060863>
35. Lee, C., Wang, Y., Chang, C.: A steganography method with high capacity by improving exploiting modification direction. In: *IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP)*, pp. 497–500. (2007) <https://doi.org/10.1109/IIH-MSP.2007.62>
36. Jung, K., Yoo, K.: Improved exploiting modification direction method by modulus operation. *Int. J. Signal Process. Image Process. Pattern.* **2**(1), 79–87 (2009)
37. Lin, K., Hong, W., Chen, J., Chen, T., Chiang, W., n et al. Data hiding by exploiting the modification direction technique using optimal pixel grouping. In: *IEEE 2010 2nd International Conference on Education Technology and Computer (ICETC)* (2010). <https://doi.org/10.1109/ICETC.2010.5529581>

38. Mohsin, A.T.: A New Steganography Technique Using Knight's Tour Algorithm, Affine Cipher, And Huffman Coding (Master Thesis). Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia (2013)
39. Ahmad, A., Sulong, G., Rehman, A., Alkawaz, M., Saba, T.: Data hiding based on improved exploiting modification direction method and Huffman coding. *J. Intell. Syst.* **23**(4), 451–459 (2014). <https://doi.org/10.1515/jisys-2014-0007>
40. Lee, C., Chang, C., Pai, P., Liu, C.: Adjustment hiding method based on exploiting modification direction. *Int. J. Netw. Secur.* **17**(5), 607–618 (2015)
41. Alsaffawi, Z.S.Y.: Image steganography by using exploiting modification direction and knight tour algorithm. *J. Al-Qadissiya Comput. Sci. Math.* **8**(1), 1–11 (2016)
42. Saha, S., Ghosal, S., Chakraborty, A., Dhargupta, S., Sarkar, R., Mandal, J.: Improved exploiting modification direction-based steganography using dynamic weightage array. *Electron. Lett.* **54**(8), 498–500 (2018). <https://doi.org/10.1049/el.2017.3336>
43. Walia, G.S., Makhija, S., Singh, K., Sharma, K.: Robust stego-key directed LSB substitution scheme based upon the cuckoo search and chaotic map. *Optik* **170**, 106–124 (2018)
44. Preishuber, M., Hütter, T., Katzenbeisser, S., Uhl, A.: Depreciating motivation and empirical security analysis of chaos-based image and video encryption. *IEEE Trans. Inf. Forensics Secur.* **13**(9), 2137–2150 (2018)
45. Atawneh, S., Almomani, A., Al Bazar, H., Sumari, P., Gupta, B.: Secure and imperceptible digital image steganographic algorithm based on diamond encoding in the DWT domain. *Multimedia Tools Appl.* **76**(18), 18451–18472 (2017). <https://doi.org/10.1007/s11042-016-3930-0>
46. Wang, Z., Zhang, X., Yin, Z.: Joint cover-selection and payload allocation by steganographic distortion optimization. *IEEE Signal Process. Lett.* **25**(10), 1530–1534 (2018)
47. Kumar, V., Kumar, D.: A modified DWT-based image steganography technique. *Multimedia Tools Appl.* **77**(11), 13279–13308 (2017). <https://doi.org/10.1007/s11042-017-4947-8>
48. Bhardwaj, R., Sharma, V.: Image steganography based on complemented message and inverted bit LSB substitution. *Procedia Comput. Sci.* **93**, 832–838 (2016). <https://doi.org/10.1016/j.procs.2016.07.245>
49. Christiana, A.O., Oluwatobi, A.N., Victory, G.A., Oluwaseun, O.R.: A secured one time password authentication technique using (3, 3) visual cryptography scheme. In: *Journal of Physics: Conference Series*, vol. 1299, no. 1, p. 012059, IOP Publishing (2019)
50. Abikoye, O.C., Akande, N.O., Garuba, A.V., Ogundokun, R.O.: A secured one time password authentication technique using (3, 3) visual cryptography scheme (2019)