Hindawi
International Journal of Digital Multimedia Broadcasting
Volume 2021, Article ID 8827055, 8 pages
https://doi.org/10.1155/2021/8827055

Research Article

A Safe and Secured Medical Textual Information Using an Improved LSB Image Steganography

Roseline Oluwaseun Ogundokun[1] **and Oluwakemi Christiana Abikoye**[2]

[1]*Department of Computer Science, Landmark University Omu Aran, Nigeria*
[2]*Department of Computer Science, University of Ilorin, Kwara State, Nigeria*

Correspondence should be addressed to Roseline Oluwaseun Ogundokun; ogundokun.roseline@lmu.edu.ng

Received 4 August 2020; Revised 27 February 2021; Accepted 17 March 2021; Published 27 March 2021

Academic Editor: Marco Roccetti

Safe conveyance of medical data across unsecured networks nowadays is an essential issue in telemedicine. With the exponential growth of multimedia technologies and connected networks, modern healthcare is a huge step ahead. Authentication of a diagnostic image obtained from a specialist at a remote location which is from the sender is one of the most challenging tasks in an automated healthcare setup. Intruders were found to be able to efficiently exploit securely transmitted messages from previous literature since the algorithms were not efficient enough leading to distortion of information. Therefore, this study proposed a modified least significant bit (LSB) technique capable of protecting and hiding medical data to solve the crucial authentication issue. The application was executed and established by utilizing MATLAB 2018a, and it used a logical bit shift operation for execution. The investigational outcomes established that the proposed technique can entrench medical information without leaving a perceptible falsification in the stego image. The result of this implementation shows that the modified LSB image steganography outperformed the standard LSB technique with a higher PSNR value and lower MSE value when compared with previous research works. The number of shifts was added as a new performance metric for the proposed system. The study concluded that the proposed secured medical information system was evidenced to be proficient in secreting medical information and creating undetectable stego images with slight entrenching falsifications when likened to other prevailing approaches.

1. Introduction

The advancement of information and communication technologies in recent ages has made the delivery of digital information further relevant. It is necessary for various divisions, for instance, government, education, banking, and healthcare, where the Internet has to turn out to be the bedrock for data exchange and distribution [1–5]. The medical industries mainly use the internet to promote remote sharing between hospitals and clinics of digital medical information and to provide patients with e-health facilities [6, 7]. Access to medical records allows patient data to be shared between multiple physicians and provides successful remote diagnosis [7–11]. For the detection and management of several ailments [7, 12–14], digital medical images are necessary and, thus, it is highly critical to ensure safe recording, retrieval, and review of medical information without breaching the Code of Ethics for Health Information Practitioners. The Hospital Information System (HIS) and the Patient Archiving and Communication System (PACS) form the basis of the Digital Imaging and Communication in Medicine (DICOM) standard for digital hospital systems [15–18]. DICOM has been the world standard for treating, preserving, publishing, and distributing medical imaging and related information since its establishment in 1993 [19]. It specifies the format for medical images that can be shared for therapeutic use with the data required. DICOM was first implemented without consideration for network security or privacy safety [17, 18, 20]. Several strategies for preserving diagnostic photographs and health data have recently been

implemented [6, 21, 22]. These approaches rely on encryption or information hiding techniques for secure communication.

Information hiding is the technique of inserting information into another medium for safe transfer. It has a broad variety of features, including copyright enforcement, tamper detection, and hidden data transfer [23]. In general, according to the purposes for which information hiding is used, information hiding techniques can be divided into two, and they are steganography and watermarking. Steganography is the practice of hiding the presence of a hidden message inside other media, for instance, text, image, audio, and video without causing unintended awareness and at the same time attaining a high entrenching potential [21] while watermarking approaches are employed to validate the identification and validity of the digital image holders by inserting distinct material such as a signature into the host medium [24]. There has been a surge of interest in incorporating these techniques like [1, 25–28] in recent years. Based on the domain type, steganography methods can be divided into two: spatial and transform [21, 28, 29]. In the cover image, spatial domain procedures entrench the hidden data directly. On the other hand, transforming domain procedures embed the data after transforming the image of the cover into another domain [30, 31]. Spatial domain algorithms such as LSB take less time to perform and have a higher embedding performance [29, 32].

Therefore, as a result of this research, a steady medical information system based on a modified least significant bit (LSB) algorithm was suggested. The proposed system was introduced in the programming environment of MATLAB 2018a. This functions by moving the LSB of the red (R), green (G), and blue (B) of concealed object pixel components to the given number of times the sender determines. The bits of the undisclosed message would then be substituted for the moving bits.

The remainder of the article is written as follows: Section 2 discussed the related works in this field of study. Section 3 presented the proposed modified LSB image steganography, and both the embedding and extracting algorithms were outlined and discussed. Section 4 addressed the study proposed prototype. Performance analysis of the system was likewise presented, and discussion on this comparative analysis was presented in this section. Lastly, Section 5 concluded the study.

2. Related Works

The most popular spatial steganography approach is the least significant bit (LSB) technique [33, 34]. This LSB technique is proficient in entrenching comparatively huge undisclosed data in a concealment object [35] by substituting the LSBs of the concealment object pixels with the hidden data bits [36, 37]. In the field of medical textual information hiding, several approaches have been suggested for various goals [38–42]. In recent years, different mechanisms of image steganography have been implemented [43–57]. Some of the literature that has utilized image steganography are discussed as thus.

Asad and Shayeb [58] proposed the improvement of the Least Significant Digit (LSD). In this research work, the authors implemented the use of the Least Significant Digit (LSD) Digital Watermark Technique and at the same time, the method of optimizing preference is employed. The exact reliability was not attained through the unsystematic choosing of pixel's value. Optimizing preference lessens the quantity of pixel value that was altered. The digital watermark and digital cover image were in grayscale. The handling domain was in the spatial domain. In 2017, Jung [59] conducted a comparative investigation of information hiding, and the study was based on least significant bit. The diverse implanting proportion had been introduced in numerous varieties of research work. The performance and juxtaposition of image evaluation and histogram evaluation for each one of the pixel layers were conducted in the article. The authors presented that the data hiding approach with individual bpp implanting proportion was strenuous to differentiate between the cover and stego objects. An innovative structure aimed at the rightfulness of optical constituents employing steganography was postulated by Muhammad, Ahmad, Rho, and Baik [60] in 2017. The study made use of the gleaming level surface of contributed representation for concealed records by utilizing Morton scrutinizing the precise least significant bits replacement technique. The undisclosed records were scrambled employing a trio-parallel encoded process preceding implanting, and this led to enhancing an extra steady safety for validation. Al-Shatanawi [61] suggested a generation of a procedure centered upon dual methodologies. These dual methodologies are presented as Distinctive Magnitude Picture Divisions (DMPD) as well as Amended Smallest Substantial (ASS) pieces. The DMPD was administered upon protected representation towards inserting undisclosed representation arbitrarily. This procedure interchanged the number of portions in inconsistent means, whereas it delivers little distortion on the concealed representation. Laskar and Hemachandran [62] recommended a technique in information hiding. In the study, records are implanted within the reddish level surface of the representation, and the constituent is chosen utilizing an arbitrary integer originator. It is nearly not possible to observe the alteration in the concealment image. To single out the pixel locations, a stego password was employed to root the artificial arbitrary figure originator. The authors' objectives focused on shooting up the confidentiality of the communication and lessen misrepresentation proportion or level. Jung [63] recommended powerful magnitude files obscuring the structure. The recommended structure applies the component rate distinguishing along with smallest important part substitution concurrently in the consistent item level towards expanding the entrenching competence. The empirical outcomes indicated that the recommended structure retained 32.61 dB on moderate once the entrenching competence attained 1,052,641 parts. Hence, the recommended structure ensured sturdiness supported by entrenching competence in the absence of misrepresentation to the mortal optical technique.

Gutub and Al-Ghamdi [8] postulated multimedia image steganography for optimized counting-based secret sharing. The authors used multimedia image-based steganography

methods to store the optimized shares that are providing comparisons for proofed remarks. The paper experiments measure the function of the improvements by assuming various hidden sharing key sizes of 64-bit, 128-bit, and 256-bit to ensure that real differences within the security analysis. The usability of the shares was further enhanced by experimenting with five different image-based steganography techniques to embed each produced share. The findings showed a major enticing impact, making the streamlined counting-based secret sharing scheme a promising approach for security applications for multi-user authentication.

Karakis, Guler, Capraz, and Bilir (2015) proposed an innovative fuzzy logic-based image steganography technique to guarantee medical information safety. The authors proposed to protect patients' records by employing steganographic techniques to merge them into one file format. The electroencephalogram (EEG) was chosen as the concealed information, and MR objects are employed as the concealment object. Furthermore, to the EEG, the message in the image file header is comprised of doctor's statements and patient information.

It was deduced from related works that most systems developed were less robust and lesser quality images produced. Some researchers did not consider the condition of more PSNR and less MSE, and there was distortion in the cover image used in some research thereby giving low qualities of stego image which made it possible for intruders to detect a secured message being communicated. Finally, distortion, robustness, and imperceptibility were not considered in some previous research.

Hence, with all these deductions, the study, therefore, is aimed at solving the problems of imperceptibility, less robustness, distortion, and security by modifying the previous standard LSB steganography techniques which are called the circular shift LSB steganography.

3. Proposed System

The suggested system for this study is modified least significant bit (LSB) image steganography for entrenching and securing medical information.

Figure 1 illustrates the embedding stage of the projected system. The medical information is passed into the modified LSB steganography. The cover image and the medical information are loaded into the system after which the modified LSB is used for the embedding process, and the output is a stego image. Figure 2 displays the extraction stage of the system where the stego image is loaded into the system, and then the modified extraction algorithm is implemented on the stego image given output of the original cover image and secured medical information.

The proposed algorithm employs a key that can be in any length and could contain a mixture of letters, numbers, and symbols. A circular shift function was used to maximize the complexity of the message being covered by moving the coded message bits by several steps at each iteration up to the sum of the password length in an ASCII value. The LSB of the concealment object is replaced in stages up to the appropriate quantity of bits to be substituted. The same

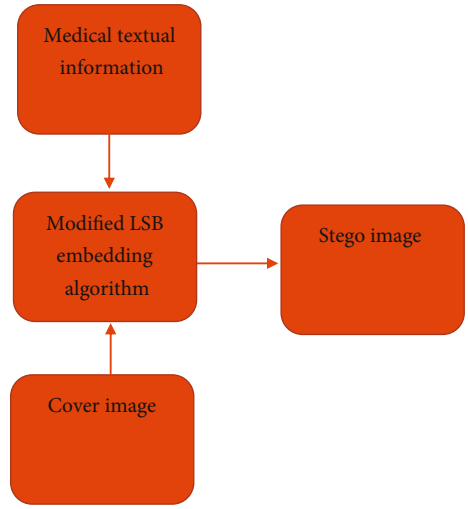

Figure 1: Embedding phase of the projected system.

method is followed to recover the undisclosed code, but by moving the extracted bits to the left by k steps up to the password sum in the ASCII value.

4. Our Prototype

MATLAB was used by the authors to execute the proposed algorithms where two-dimensional cover images were used to implant medical information from the patient. The system often used the text of varying sizes, and it was deduced that it was difficult to discern between the original concealment object and the stego object when the algorithm was applied. The following interfaces show the outcomes of the algorithm's implementation.

4.1. Embedding Phase of the System. The proposed secured medical information system interface is shown in Figure 3.

Figure 4 displays the system interface illustrating the patient's medical information which is in text format and the stego key (known to only the source and recipient) being entered into the system.

The final stage of the embedding phase is shown in Figure 5. This shows the initial cover image and the steganographic image (that is image hiding the patient's information). The PSNR value, MSE value, and the no. of shifts are shown as well.

4.2. Extraction Phase for the System. The interface of the extraction phase is shown in Figure 6. Here, the recipient entered the secret stego key and then have access to the stego image.

The concealed medical information and the initial cover image are revealed after the modified extraction LSB algorithm is implemented as shown in Figure 7.

4.3. Performance Analysis. To evaluate the performance of the proposed system, the authors compared the PSNR and MSE of the modified system with the existing methods. For numerical analysis, the system employed MATLAB and also

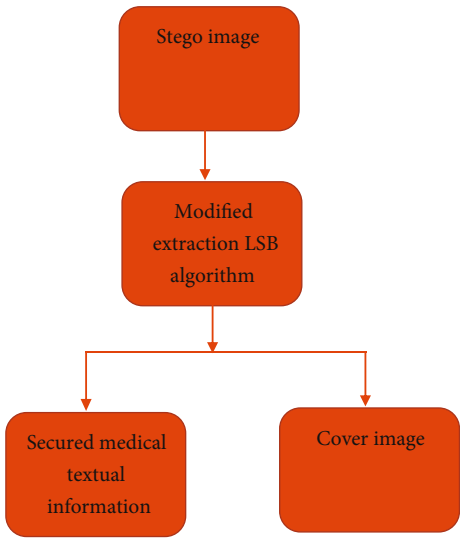

Figure 2: Extraction phase of the projected system.

Cover image read cover image
binMsg read medical information into binary
key read stego key
sum $\sum_{k=0}^{length(key)} key(k)$
while (i=1: length(binMsg))**do**
  for j=1 to sum
  right circular shift(binMsg(j))
  end
% replace lsb of cover image with binMsg
End

Algorithm 1: Embedding stage algorithm.

stego image read LSB of stego image
key read stego key
sum $\sum_{i=0}^{length(key)} key(i)$
while (! End of message)**do**
  for j=1 to sum
  left circular shift(extractedMsg(j))
  end
% extracted message
End

Algorithm 2: Extraction stage algorithm.

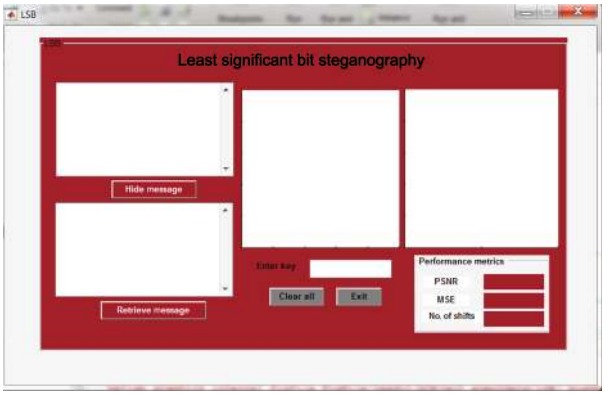

Figure 3: Interface of the system.

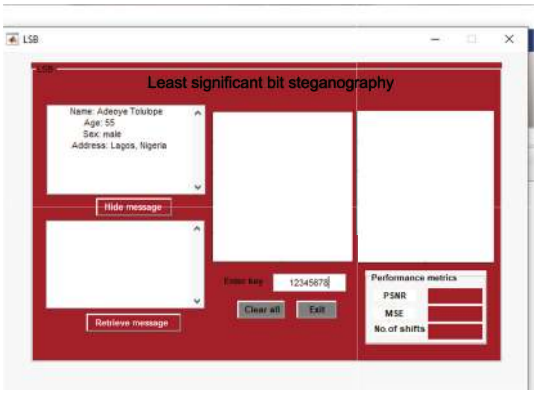

Figure 4: Interface showing text and stego key entered.

Figure 5: Interface of the embedding result.

added the number of LSB shifts as a performance metric. Table 1 shows and describes the evaluation of the projected scheme using PSNR, MSE, and number of shifts as the evaluation metrics. The study evaluates the system by computing the peak signal-to-noise (PSNR) and mean squared error (MSE). The PSNR mathematical equation is shown in Eq. (1) and the MSE in Eq. (2), respectively.

(i) Peak signal-to-noise ratio (PSNR): to avoid suspicion, the quality of the stego image and the cover image must be the same. The difference in quality will be measured using PSNR. The higher the PSNR, the higher the quality of the stego image. PSNR could be calculated using Eq. (1):

$$\text{PSNR} = 10 \log \left(\frac{255^2}{\text{MSE}} \right). \quad (1)$$

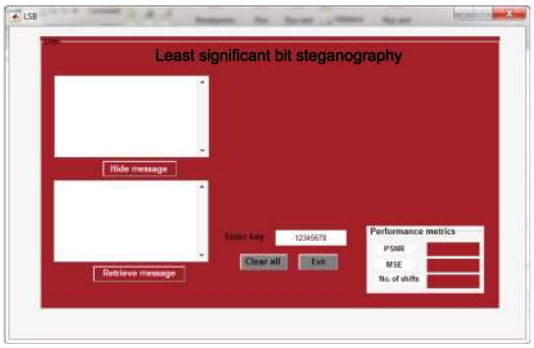

Figure 6: Interface of the extraction phase.

Figure 7: Interface of the extraction phase.

Table 1: Evaluation of the proposed system.

Samples	Number of stego key characters	PSNR	MSE	No. of shifts
1	8	79.1473	0.000791	88410
2	5	80.364	0.000598	32640

(ii) MSE which is the mean square error will be calculated using the equation:

$$\text{MSE} = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|c-s\|^2. \quad (2)$$

5. Discussion

The study performance was evaluated using the two most common steganography performance metrics which are PSNR and MSE. It was noticed that the PSNR for fewer text characters is higher than the text with higher characters. Table 1 shows that a text with 8 characters has a PSNR of 79.147 and MSE of 0.000791, and a text with 5 characters has a PSNR value of 80.364 and an MSE value of 0.000598. Table 2 displays the comparative examination of the projected system with other previous researches. Abd-El-Atty et al. [54] have a PSNR value of 73.27 and did not use MSE for evaluation, and Hashim et al. [12] have a PSNR value of 72.29 and also did not use MSE for their performance evaluation. Setyono and Setiadi [64] got a PSNR value of 63.52 and a MSE value of 0.0289. The proposed system had a PSNR value of 80.36 and an MSE value of 0.00060 which shows that the proposed modified LSB outperformed previous researches as seen in Figure 8. Table 3 shows the parameter values for the proposed system, and it was discovered that the proposed system security level is high, the MSE value is low, PSNR value is high, and it is highly robust and also possessed a high imperceptibility.

Table 2: Comparison with other LSB steganography technique.

Authors	PSNR	MSE
Abd-El-Atty et al. [54]	73.27	—
Hashim et al. [12]	72.29	—
Setyono and Setiadi [64]	63.52	0.0289
The proposed system, 2020	80.36	0.00060

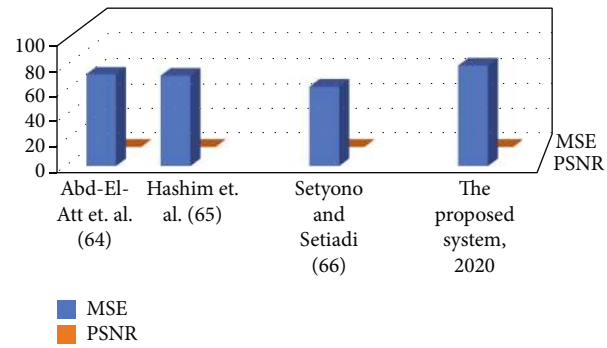

Figure 8: Comparative analysis with previous researches.

Table 3: Parameter values of the proposed method.

Features	Proposed
Security	High
MSE	Low
PSNR	High
Robustness	High
Imperceptibly	High

6. Conclusions

The protection of patient data in the digital medical system is the focus of this research. The research presented an important information entrenching system for maintaining the confidentiality and privacy of patient information by concealing its presence. This study suggested a modified least significant bit image steganography technique. The system was implemented using MATLAB, and two performance metrics were used to evaluate the proposed system which includes PSNR and MSE. The number of shifts was added as well. Investigational findings showed that with a low degree of embedding distortion, the proposed algorithm obtained a high embedding rate and thus offered a reasonable balance between concealment and stego image quality.

Therefore, the proposed secured medical information system is evidenced to be proficient in secreting medical

information and creating undetectable stego images with slight entrenching falsifications when likened to other prevailing approaches.

Data Availability

No data were used to support this study.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Consent

Informed consent was obtained from all individual participants included in the study.

Conflicts of Interest

The author(s) declare(s) that they have no conflicts of interest.

References

[1] M. K. Ramaiya, N. Hemrajani, and A. K. Saxena, "Security improvisation in image steganography using DES," in *2013 3rd IEEE International Advance Computing Conference (IACC)*, pp. 1094–1099, Ghaziabad, India, 2013.

[2] P. Thiyagarajan and G. Aghila, "Reversible dynamic secure steganography for medical image using graph coloring," *Health Policy and Technology*, vol. 2, no. 3, pp. 151–161, 2013.

[3] O. C. Abikoye, U. A. Ojo, J. B. Awotunde, and R. O. Ogundokun, "A safe and secured iris template using steganography and cryptography," *Multimedia Tools and Applications*, vol. 79, no. 31-32, pp. 23483–23506, 2020.

[4] O. N. Akande, O. C. Abikoye, A. A. Kayode, O. T. Aro, and O. R. Ogundokun, "A dynamic round triple data encryption standard cryptographic technique for data security," in *Computational Science and Its Applications – ICCSA 2020. ICCSA 2020*, pp. 487–499, Springer, 2020.

[5] A. Oluwakemi Christiana, A. Noah Oluwatobi, G. Ayomide Victory, and O. Roseline Oluwaseun, "A secured one time password authentication technique using (3, 3) visual cryptography scheme," *Journal of Physics: Conference Series*, vol. 1299, article 012059, 2019.

[6] H. K. Maity and S. P. Maity, "Joint robust and reversible watermarking for medical images," *Procedia Technology*, vol. 6, pp. 275–282, 2012.

[7] M. Kay, J. Santos, and M. Takane, "mHealth: new horizons forhealth through Mobile technologies," *World Health Organization*, vol. 2011, pp. 66–71, 2011.

[8] A. Gutub and M. Al-Ghamdi, "Hiding shares by multimedia image steganography for optimized counting-based secret sharing," *Multimedia Tools and Applications*, vol. 79, no. 11-12, pp. 7951–7985, 2020.

[9] M. Roccetti, G. Delnevo, L. Casini, and P. Salomoni, "A cautionary tale for machine learning design: why we still need human-assisted big data analysis," *Mobile Networks and Applications*, vol. 25, no. 3, pp. 1075–1083, 2020.

[10] M. Chaumont, "Deep learning in steganography and steganalysis," in *Digital Media Steganography*, pp. 321–349, Academic Press, 2020.

[11] S. Mirri, M. Roccetti, and G. Delnevo, "The New York City COVID-19 spread in the 2020 spring: a study on the potential role of particulate using time series analysis and machine learning," *Applied Sciences*, vol. 11, no. 3, p. 1177, 2021.

[12] M. M. Hashim, M. S. Taha, A. H. M. Aman, A. H. A. Hashim, M. S. M. Rahim, and S. Islam, "Securing medical data transmission systems based on integrating algorithm of encryption and steganography," in *2019 7th International Conference on Mechatronics Engineering (ICOM)*, pp. 1–6, Putrajaya, Malaysia, 2019.

[13] A. Ibaida and I. Khalil, "Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems," *IEEE Transactions on Biomedical Engineering*, vol. 60, no. 12, pp. 3322–3330, 2013.

[14] G. Prabakaran, R. Bhavani, and P. S. Rajeswari, "Multi secure and robustness for medical image-based steganography scheme," in *2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT)*, pp. 1188–1193, Nagercoil, India, 2013.

[15] H. K. Lee, H. J. Kim, S. G. Kwon, and J. K. Lee, "ROI Medical Image Watermarking Using DWT and Bit-Plane," in *2005 Asia-Pacific Conference on Communications*, pp. 512–515, Perth, WA, Australia, 2005.

[16] H. Nyeem, W. Boles, and C. Boyd, "A review of medical image watermarking requirements for teleradiology," *Journal of Digital Imaging*, vol. 26, no. 2, pp. 326–343, 2013.

[17] S. Das and M. K. Kundu, "Effective management of medical information through ROI-lossless fragile image watermarking technique," *Computer Methods and Programs in Biomedicine*, vol. 111, no. 3, pp. 662–675, 2013.

[18] O. S. Pianykh, "Brief History of DICOM," in *Digital Imaging and Communications in Medicine (DICOM)*, pp. 19–25, Springer, Berlin, Heidelberg, 2012.

[19] M. Onken, M. Eichelberg, J. Riesmeier, and P. Jensch, "Digital Imaging and Communications in Medicine," in *Biomedical Image Processing*, pp. 427–454, Springer, 2011.

[20] F. Cao, H. K. Huang, and X. Q. Zhou, "Medical image security in a HIPAA mandated PACS environment," *Computerized Medical Imaging and Graphics*, vol. 27, no. 2-3, pp. 185–196, 2003.

[21] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[22] M. Ulutas, G. Ulutas, and V. V. Nabiyev, "Medical image security and EPR hiding using Shamir's secret sharing scheme," *Journal of Systems and Software*, vol. 84, no. 3, pp. 341–353, 2011.

[23] C. H. Yang, "Inverted pattern approach to improve image quality of information hiding by LSB substitution," *Pattern Recognition*, vol. 41, no. 8, pp. 2674–2683, 2008.

[24] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognition*, vol. 34, no. 3, pp. 671–683, 2001.

[25] S. Song, J. Zhang, X. Liao, J. Du, and Q. Wen, "A novel secure communication protocol combining steganography and cryptography," *Process Engineering*, vol. 15, pp. 2767–2772, 2011.

[26] D. Bouslimi, G. Coatrieux, and C. Roux, "A joint encryption/-watermarking algorithm for verifying the reliability of medical

images: application to echographic images," *Computer Methods and Programs in Biomedicine*, vol. 106, no. 1, pp. 47–54, 2012.

[27] P. P. Aung and T. M. Naing, "A novel secure combination technique of steganography and cryptography," *International Journal of Information Technology, Modeling and Computing*, vol. 2, no. 1, pp. 55–62, 2014.

[28] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: a survey," *Computer Science Review*, vol. 13-14, pp. 95–113, 2014.

[29] D. Bandyopadhyay, K. Dasgupta, J. K. Mandal, and P. Dutta, "A novel secure image steganography method based on chaos theory in spatial domain," *International Journal of Security, Privacy and Trust Management*, vol. 3, no. 1, pp. 11–22, 2014.

[30] S. U. Maheswari and D. J. Hemanth, "Frequency domain QR code based image steganography using Fresnelet transform," *AEU - International Journal of Electronics and Communications*, vol. 69, no. 2, pp. 539–544, 2015.

[31] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, "Watermarking techniques used in medical images: a survey," *Journal of Digital Imaging*, vol. 27, no. 6, pp. 714–729, 2014.

[32] M. Ghebleh and A. Kanso, "A robust chaotic algorithm for digital image steganography," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 1898–1907, 2014.

[33] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image steganography techniques: an overview," *International Journal of Computer Science and Security*, vol. 6, no. 3, pp. 168–187, 2012.

[34] T. Morkel, J. H. Eloff, and M. S. Olivier, "An overview of image steganography," *ISSA*, vol. 1, pp. 1–11, 2005.

[35] S. Bansod and G. Bhure, "Data encryption by image steganography," *Int. J. Inform. Comput. Technol. Int. Res. Publ. House*, vol. 4, pp. 453–458, 2014.

[36] M. Juneja and P. S. Sandhu, "An improved LSB based steganography technique for RGB color images," *International Journal of Computer and Communication Engineering*, vol. 2, no. 4, pp. 513–517, 2013.

[37] H. Al-Dmour, A. Al-Ani, and H. Nguyen, "An efficient steganography method for hiding patient confidential information," in *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 222–225, Chicago, IL, USA, 2014.

[38] N. O. Akande, C. O. Abikoye, M. O. Adebiyi, A. A. Kayode, A. A. Adegun, and R. O. Ogundokun, "Electronic medical information encryption using modified blowfish algorithm," in *Computational Science and Its Applications – ICCSA 2019. ICCSA 2019*, pp. 166–179, Springer, 2019.

[39] R. O. Ogundokun, O. C. Abikoye, S. Misra, and J. B. Awotunde, "Modified least significant bit technique for securing medical images," in *Information Systems. EMCIS 2020*, pp. 553–565, Springer, 2020.

[40] R. Karakış, İ. Güler, I. Capraz, and E. Bilir, "A novel fuzzy logic-based image steganography method to ensure medical data security," *Computers in Biology and Medicine*, vol. 67, pp. 172–183, 2015.

[41] G. Delnevo, M. Roccetti, and S. Mirri, "Modeling patients' online medical conversations: a granger causality approach," in *Proceedings of the 2018 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies*, pp. 40–44, Washington, DC, USA, 2018.

[42] G. Delnevo, S. Mirri, L. Monti et al., "Patients reactions to non-invasive and invasive prenatal tests: a machine-based analysis from reddit posts," in *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pp. 980–987, Barcelona, Spain, 2018.

[43] S. M. Karim, M. S. Rahman, and M. I. Hossain, "A New Approach for LSB Based Image Steganography Using Secret Key," in *14th International Conference on Computer and Information Technology (ICCIT 2011)*, pp. 286–291, Dhaka, Bangladesh, 2011.

[44] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 201–214, 2010.

[45] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," in *Proceedings 2001 International Conference on Image Processing (Cat. No.01CH37205)*, pp. 1019–1022, Thessaloniki, Greece, 2001.

[46] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Optics & Laser Technology*, vol. 116, pp. 92–102, 2019.

[47] C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, "Reversible hiding in DCT-based compressed images," *Information Sciences*, vol. 177, no. 13, pp. 2768–2786, 2007.

[48] V. Kumar and D. Kumar, "Performance Evaluation of DWT Based Image Steganography," in *2010 IEEE 2nd International Advance Computing Conference (IACC)*, pp. 223–228, Patiala, India, 2010.

[49] G. Prabakaran and R. Bhavani, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform," in *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, pp. 1096–1100, Nagercoil, India, 2012.

[50] V. Kumar and D. Kumar, "Digital Image Steganography Based on Combination of Dct and Dwt," in *International Conference on Advances in Information and Communication Technologies*, pp. 596–601, Springer, Berlin, Heidelberg, 2010.

[51] B. Feng, W. Lu, and W. Sun, "Secure binary image steganography based on minimizing the distortion on the texture," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 243–255, 2015.

[52] V. Holub and J. Fridrich, "Designing Steganographic Distortion Using Directional Filters," in *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 234–239, Costa Adeje, Spain, 2012.

[53] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security, ACM*, pp. 59–68, Montpellier, France, 2013.

[54] B. Abd-El-Atty, A. A. Abd El-Latif, and M. Amin, "New Quantum Image Steganography Scheme with Hadamard Transformation," in *International Conference on Advanced Intelligent Systems and Informatics*, pp. 342–352, Springer, 2016.

[55] N. Jiang, N. Zhao, and L. Wang, "LSB based quantum image steganography algorithm," *International Journal of Theoretical Physics*, vol. 55, no. 1, pp. 107–123, 2016.

[56] A. A. Abd El-Latif, B. Abd-El-Atty, M. S. Hossain, M. D. A. Rahman, A. Alamri, and B. B. Gupta, "Efficient quantum information hiding for remote medical image sharing," *IEEE Access*, vol. 6, pp. 21075–21083, 2018.

[57] T. J. Zhang, B. Abd-El-Atty, M. Amin, and A. A. A. El-Latif, "QISLSQb: A Quantum Image Steganography Scheme Based on Least Significant Qubit," in *2016 International Conference on Mathematical, Computational and Statistical Sciences and Engineering (MCSSE)*, pp. 40–45, 2016.

[58] N. Masoud and I. Ghazi, "A modification of least significant digit (LSD) digital watermark technique," *International Journal of Computer Applications*, vol. 179, no. 32, pp. 4–6, 2018.

[59] K. Jung, "Performance analysis of LSB-based data hiding techniques," *International Journal of Signal Processing*, vol. 2, pp. 129–132, 2017.

[60] K. Muhammad, J. Ahmad, S. Rho, and S. W. Baik, "Image steganography for authenticity of visual contents in social networks," *Multimedia Tools and Applications*, vol. 76, no. 18, pp. 18985–19004, 2017.

[61] O. M. Al-Shatanawi and N. N. El Emam, "A new image steganography algorithm based on MLSB method with random pixels selection," *International Journal of Network Security & Its Applications*, vol. 7, pp. 37–53, 2015.

[62] S. A. Laskar and K. Hemachandran, "Steganography based on random pixel selection for efficient data hiding," *International Journal of Computer Engineering and Technology*, vol. 4, no. 2, pp. 31–44, 2013.

[63] K.-H. Jung, "Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 127–136, 2018.

[64] A. Setyono and D. R. I. M. Setiadi, "Securing and hiding secret message in image using XOR transposition encryption and LSB method," *Journal of Physics: Conference Series*, vol. 1196, article 012039, 2019.