Efficiency of LSB steganography on medical information

Oluwakemi Christiana Abikoye[1], Roseline Oluwaseun Ogundokun[2]
[1]Department of Computer Science, University of Ilorin, Kwara State, Nigeria
[2]Department of Computer Science, Landmark University Omu Aran, Kwara State, Nigeria

Article Info

Article history:

Received Mar 31, 2020
Revised Mar 10, 2021
Accepted Mar 22, 2021

Keywords:

Information hiding
Least significant bit
Medical information
Security
Steganography

ABSTRACT

The development of the medical field had led to the transformation of communication from paper information into the digital form. Medical information security had become a great concern as the medical field is moving towards the digital world and hence patient information, disease diagnosis and so on are all being stored in the digital image. Therefore, to improve the medical information security, securing of patient information and the increasing requirements for communication to be transferred between patients, client, medical practitioners, and sponsors is essential to be secured. The core aim of this research is to make available a complete knowledge about the research trends on LSB Steganography Technique, which are applied to securing medical information such as text, image, audio, video and graphics and also discuss the efficiency of the LSB technique. The survey findings show that LSB steganography technique is efficient in securing medical information from intruder.

Corresponding Author:

Roseline Oluwaseun Ogundokun
Department of Computer Science
Landmark University
Omu Aran, Kwara State, Nigeria
Email: ogundokun.roseline@lmu.edu.ng

1. INTRODUCTION

Steganography can be described as an art and science of securing information communication where the secret data is hidden in his file and it application areas include communication of data, military, healthcare, voting system and so on. Due to rapid growth of the multimedia and internet, confidential message is commonly stored in digital media and transmitted via the internet [1]-[11]. Steganography is derived from Greek words Stego which means cover and Grafia which denotes writing put together covered writing. Information is hidden in the images in image steganography [12]-[15]. Capacity, security and robustness are the three-different aspect of information hiding that oppose each other [16]-[24]. Some categories of documents hiding methodologies are watermarking, steganography and reversible data hiding (RDH). Watermarking refers to an order of numeral bits positioned in a digital concealment object that recognize the document's patent information [25], [26]. Steganography convert message and also modifies the image in a way that merely the disseminator of the message and the projected receiver would be able to discover the message while being sent [27]-[31]. In RDH, concealment object holds the secret data as well [32]-[34]. Information like patient's personal details, medical history such as past test results and current test reports are the data of a patient that needs to be protected [35]. The methods that can be used to protect patient's information can be categorized into two ways [35].

– Patient's ID with the report shouldn't be incorporated so as to maintain the patient's privacy.

- It will be difficult for an attacker to extract an information when he gains access to the patient’s reports and this will rely on the strength of the steganography algorithm and proper management of the key between the concerned parties such as the medical practitioner and the client

Though these techniques work well, they possess certain limitations also. Hence, it is established in this research that steganography can be used to protect medical information in digital form by embedding the patient’s reports and identification into a cover image and this can only be access by an authorized person that is the person having the confidential stego key.

2. LITERATURE REVIEW

The method used for this research is downloading of many past literatures and the ones relating to this study were reviewed and conclusions were drawn from the survey conducted. The steganography algorithm surveyed here is least significant bit technique (LSB).

2.1. Steganography

Steganography can be described as an art and science of securing information communication where the secret data is hidden in his file and its application areas include communication of data, military, healthcare, voting system and so on [36]. Steganography is derived from Greek words Stego which means cover and Grafia which denotes writing put together covered writing. Information is hidden in the images in image steganography [37]. Capacity, security and robustness are the three-different aspect of information hiding that oppose each other [38]. There are various steganography techniques used based on the information to be hidden is shown in Figure 1.

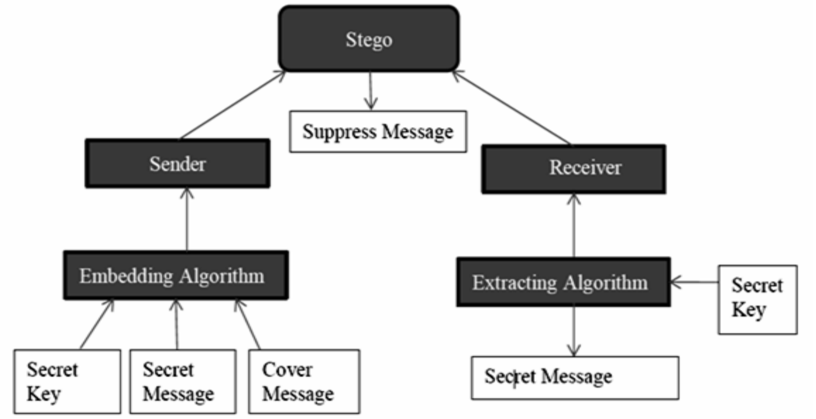

Figure 1. General model for steganography [39]

2.2. Method of information hiding

This can be categorized into three stages namely: Embedding, Attacking and Extracting stages. Figure 2 displayed the stages.

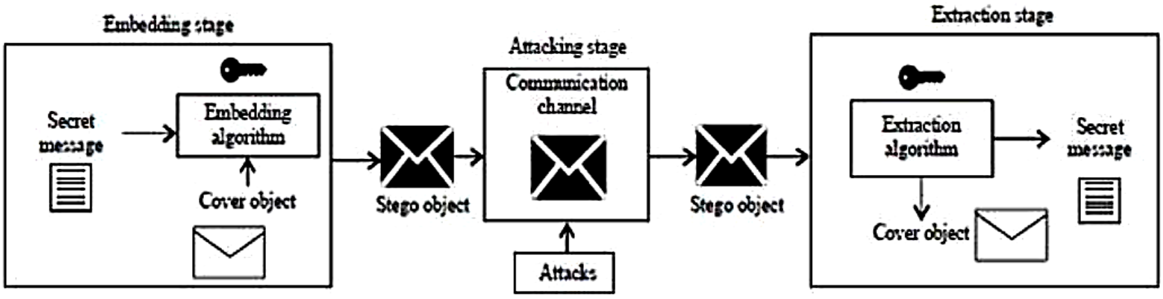

Figure 2. Process of data hiding [35]

In Figure 1, the embedding algorithm and the undisclosed key are used to entrench the undisclosed information into the concealment object (text, image, audio and video) which gives stego image, the stego image is then transmitted over a channel (network) while in the attacking stage, the stego image can be attached or becomes degraded by certain noise and this implies that the stego image can be transformed or damaged and lastly in the extracting phase, the undisclosed documents is extracted from the stego image via using the same algorithm and undisclosed key which was applied in the embedding stage.

The following factors are considered in designing a perfect data hiding system

- Imperceptibility
- Security
- Capacity
- Robustness
- Embedding complexity

2.3. Steganography methods

The methods of Steganography can be classified into seven categories, in spite of the fact that in some cases, accurate or precise classification is not possible [40] and this is shown in Figure 3. Figure 4 displays the image steganography categories that had been in trend and used by different researchers.

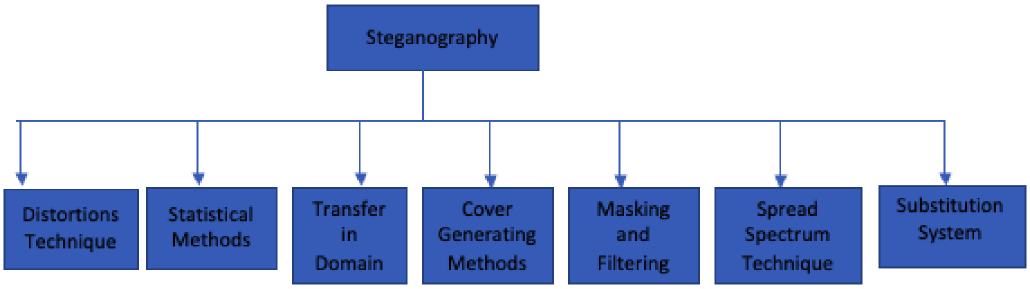

Figure 3. Categories of steganography [41]

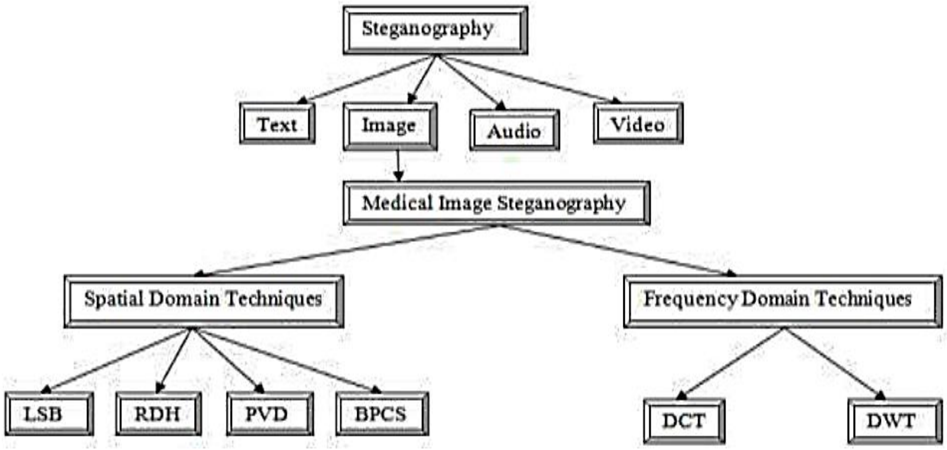
Steganography
Text
Image
Audio
Video
Medical Image Steganography
Spatial Domain Techniques
Frequency Domain Techniques
LSB
RDH
PVD
BPCS
DCT
DWT

Figure 4. Classification of medical image steganography [38]

2.4. Related works

Masoud and Ghazi [42] proposed the improvement of the least significant digit (LSD). Digital Watermark method rooted on optimizing the chosen pixels in the protected image. The exact reliability was not attained through the unsystematic choosing of pixel's value. In this research work, authors implemented the use of the least significant digit (LSD) Digital Watermark Technique and at the same time the method of optimizing preference are employed. Optimizing preference lessens the quantity of pixel's value that are going to be altered. The digital watermark and digital cover image are in gray scale. The handling domain is in spatial domain.

Muhammad *et al.* [43] postulated an innovative structure aimed at rightfulness of optical constituents by means of steganography. It makes use of gleaming level surface of contributed representation for concealed records entrenching utilizing Morton Scrutinizing- precise least significant bits replacement technique. The undisclosed records were scrambled by means of trio- parallel encoded process preceding implanting, enhancing an extra steady safety for validation.

Juneja and Sandhu [44] put forward an invulnerable robust method of information. Two components based Least significant bit (LBS) procedures for enclosing hidden documents in the LSB's of blue components and partial green components of arbitrary constituent points in the boundaries of the image. They further their study by coming up with a flexible LSB centered steganography for inserting documents established on records existing in LSB's of red, green and blue constituents of arbitrarily preferred picture elements over flat regions. They also integrated an advanced encryption standard (AES) in the proposed method which makes it more robust.

Thiyagarajan *et al.* [45] suggested an advanced elevated dimension of steganography structure by means of 3 dimensional geometrical representations. The process re-trilaterated a proportion of a three-sided engagement and implants the confidential communication into a recently incorporated location of a triangular mesh. The algorithm presented by the study also opposed against consistent assurance conversions such as selecting, spinning and escalating. The stego password is produced out of the piece of information to be implanted. The embedment is carried out with the use of the vertices of the triangle.

Priya *et al.* [46] postulated a peculiar scheme grounded on LSB. Entrenching of data is executed making use of a set of picture elements as a component, whereas LSB of the primary element convey a single portion of communication and an assignment to 2 picture elements values convey 1 extra portion of the report. The approach put forward by the authors displays more superior enhanced achievement in positions of misrepresentation and protection in opposition to prevailing steganalysis. A threshold is being used for embedding in the sharper edge regions. The study as well compared and contrasts the PSNR value for flexible and non-flexible procedures of records concealing in grey proportion and hue drawing.

Sharmila and Shanthakumari [47] presented an algorithm that works on colour images (JPEG). In order to make better the robustness of the system, the edges of the image are being selected for data hiding. The section situated at the stronger boundaries make available extra complex arithmetical characteristics and besides they are extremely reliant or relying on the image contents. Alterations are effortlessly noticed in smooth regions than at the sharper edges. RGB constituents are disconnected or detached and are based on a share key in the embedding techniques, single or extra constituents are chosen. The protected representation is bisected into non-coinciding segments. Every batch is being revolved with an unsystematic ratio controlled by a protected password. The outcome presentation is reorganized as a line angle A by raster browsing. The concealed idea is scrambled by means of LSBMR; 2 hidden portions could be implanted in the direction of every entrenching division. Using a threshold, the piece of information is entrenched following the computation of the dimensions calculation by means of a verge.

Fahim *et al.* [48] recommended noise filtering in the beginning prior to the implantation. Subsequently to obtain at acquiring point, automated repetition is used for inaccuracy discernment and amendment. Encryption and data hiding are integrated in a single step in order to have a protected dissemination of data. Anchor representations as well as confidential documents are converted into portion stream. RGB values before scrambling of protected communication center cleaning is employed. The contribution values are transformed to ASCII and subsequently to binary, the anchor representations red, green and blue values are transformed to binate. Replacement is executed letter by letter by means of encoding password. Conceal bit stream is used to substitute the LSB of each and every pixel octet. Inaccuracy discovered and correction establishes accurate transferal of data.

Luo *et al.* [49] suggested a boundary flexible system that could determine the entrenching parts specified the proportions as concerns confidential piece of information and the variance between two successive pixels in the cover image. The scheme first initializes some variables in the data implanting stage, and these variables are used for roughly calculation of the capacity of the chosen regions. In the end, stego image is acquired subsequent to pre-processing. A region adaptive scheme is put in an application directed towards spatial LSB region along with the divergence in the midst of 2 neighboring constituent is applied as a standard for area choosing and LSB identical Reconsidered by way of documents masking process.

Yang and Tsai [50] predicted an approach to intensify the histogram-based reversible data hiding technique. The predictive stages used for the technique are two. The greatest part of the pixels is forecasted by their dual neighborhood constituent together with quartet immediate constituent in the file-established and chess-panel established method. The differentiation amount of every picture element amidst the authentic model and the stego-model stay within the bound of ±1. Constituent in different files will be projected by constituents in the uniform (alike) files or with the order reversed, in interleaving forecast. The implanting procedure requires using the foretelling inaccurate substance of different files to create a histogram to implant the confidential documents. The foretelling inaccurate substances are transformed towards acquiring the stego-model.

Chandramouli and Memon [51] recommended adaptive steganographic methods that are concerned with protecting information without giving rise to statistically important alteration. It is electronically concealed on the condition that the proportionate degradation of the likelihood frequency of protected message and stego-models is <=m. LSB steganography remains a great deal easy, effortless, simple and uncomplicated. The steganographic proportion or volume of LSB core images are investigated taking advantages of probability approach and execution of steganalysis is computed as well. The composition of an inactive protector is examined exclusively. For safety measure, information is encrypted in preparatory for implanting. LSB based approaches alter pixel worth by ± 1 or exclude them without alteration. The purpose of a steganalyst is to roughly calculate if at any time I have concealed information. (I in this scenario mean Catalogue (index) record a particular that indicates the average deducted protected object).

Gupta *et al.* [52] suggested a new method of LSB that is the enhanced least significant bit (ELSB) because it was found out that the existing least significant bit algorithm has been examined and discovered to have an extra volume of alteration. The performance of LSB was enhanced because communication is secreted in just a unit of the 3 colors of the pixel that is BLUE color of the conveyor image. This reduces the alteration level of the image that is inattentive to a person eye.

Zaher [53] presented a novel steganography method. The method postulates an enhanced system above the conventional LSB technique. The principal goal of the presented work is to intensify quantity of documents to be concealed in the convoying image as well as to surge safety by carrying out data encryption. The benefit of our steganography procedure is that it can conceal greater volume of data than conventional LSB. The key drawback of the procedure if the text flips between small and capital in each character then the size will increase not decrease because of control symbols but it can be said that such scenario is rare.

Masoud *et al.* [54] study article postulated that steganography in image bits by means of Genetic Algorithm is centered on the before implanting hiding procedures. It assists to discover perfect places in transfer or images to warehouse the information with the fewer alterations of fragments. Consequently, to accomplish this, its breakdown is conveyed to translate communication strings as well as the LSBs towards the blocks for transporting the genetic algorithm. The vital file happened to be produced later following the discovery of the particular positions to entrenched information, meanwhile the crucial file is used for communication extraction drive as well. The recommended process investigated established than an effective process obtainable on ground is centered on slightest alterations in the model image then the histogram established it.

Kumar and Sharma [55] established a recently developed document obscuring method which is Harsh-LSB originated from LSB insertion on images. Hash-LSB with RSA procedure aimed at information secreting as well as stipulating additional safekeeping of documents. The establishment method makes use of Hash function to advance individual exceptional pattern for entrenching the data. Firstly, Hash function assists to locate the precise locations of smallest substantial fragment of every RGB pixel's and subsequent these communication fragments are entrenched into RGB pixels individually. Here the protected image is disjointed into portions and values acquired by Hash functions are utilized to warehouse the undisclosed documents at specific portions. Here the undisclosed communication is converted into binary buts such that pixel value is in sequence 3,3,2 for RGB concealed image plus to offer more level of safekeeping. Information secreted in scrambled prior to warehousing it in the concealed image and entrenched documents in conceal image yields a stego image.

Indresh *et al.* [34] postulated a steganography procedure through the means of Multidirectional Block established pixel-worth contrasting alongside with extraordinary payload capability. While edge sections can endure powerful alteration so the document are entrenched in the specific section reasonable than level sections as well as a lesson the feature alteration of the stego-image. The best selection methodology aimed at the location point is used and this methodology can be use in an application for gray image as well as color image. Table 1 (see in appendix) presented the overall performances of data hiding methods in spatial domain and it was noticed that most researchers takes note of imperceptibility and payload as compared to robustness.

3. CONCLUSION

In conclusion, the significance of medical image security during transmission was presented and the study made available a complete knowledge about the evolving of information hiding techniques in spatial domains, which are applied to securing all medical information such as text, image, audio, video. In can be suggested that there should be more attention in the need to increase the robustness of an embedding algorithm and an implementation of hybrid approaches would be better than the existing data hiding techniques as this will enhanced the security of medical information. Therefore, it is suggested that a novel approach needs to be established which will possess extra information hiding capacity and against to the resistance of attacks.

4. FUTURE WORK

It is suggested that another information hiding algorithm is combined with the steganography algorithm to have a robust security level while communicating the medical information so that it will be very difficult for a hacker or intruder to break into the hidden information.

APPENDIX

Table 1. Performance evaluation of image data hiding techniques

Method	Data Hiding	Resistance to Attacks	Domain	Complexity
LSB Based Steganography	High	Low	Spatial	Simple
Compression based RDH Steganography	Low	Moderate	Spatial	Complex
Edge-Adaptive Steganography	Average	Low	Spatial	Simple
PVP Based	High	Low	Spatial	Simple
BPCS Based Steganography	High	High	Spatial	Complex

REFERENCES

[1] B. A, Usha, N. K. Srinath, K. Narayan, and K. N. Sangeetha, “A Secure Data Embedding Technique in Image Steganography for Medical Images,” *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 8, pp. 7753–7775, 2014.

[2] A. O. Christiana, A. N. Oluwatobi, G. A. Victory, and O. R. Oluwaseun, “A Secured One Time Password Authentication Technique using (3, 3) Visual Cryptography Scheme,” *Journal of Physics: Conference Series*, vol. 1299, no. 1, 2019, Art. No. 012059.

[3] N. O. Akande, C. O. Abikoye, M. O. Adebiyi, A. A. Kayode, A. A. Adegun, R. O. Ogundokun, “Electronic Medical Information Encryption Using Modified Blowfish Algorithm,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11623 LNCS, pp. 166–179, 2019.

[4] A. K. Singh, “Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image,” *Multimedia Tools and Applications*, vol. 78, no. 21, pp. 30523–30533, 2019, doi: 10.1007/s11042-018-7115-x.

[5] B. Santoso, “Color-based microscopic image steganography for telemedicine applications using pixel value differencing algorithm,” in *Journal of Physics: Conference Series*, vol. 1175, no. 1, Mar. 2019, Art. No. 012057.

[6] J. Liu, J. Li, K. Zhang, U. A. Bhatti, and Y. Ai, “Zero-watermarking algorithm for medical images based on dual-tree complex wavelet transform and discrete cosine transform,” *Journal of Medical Imaging and Health Informatics*, vol. 9, no. 1, pp. 188–194, 2019.

[7] T. Yuvaraja and R. S. Sabeenian, “Performance analysis of medical image security using steganography based on fuzzy logic,” *Cluster Computing*, vol. 22, no. 2, pp. 3285–3291, 2019.

[8] R. F. Mansour and E. M. Abdelrahim, “An evolutionary computing enriched RS attack resilient medical image steganography model for telemedicine applications,” *Multidimensional Systems and Signal Processing*, vol. 30, no. 2, pp. 791–814, 2019.

[9] 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.

[10] H. Al-Dmour and A. Al-Ani, “Quality optimized medical image information hiding algorithm that employs edge detection and data coding,” *Computer methods and programs in biomedicine*, vol. 127, pp. 24–43, 2016, doi: 10.1016/j.cmpb.2016.01.011.

[11] G. Ke, H. Wang, S. Zhou, and H. Zhang, “Encryption of medical image with most significant bit and high capacity in piecewise linear chaos graphics,” *Measurement*, vol. 135, pp. 385–391, 2019.

[12] R. L. Biradar, “Secure medical image steganography through optimal pixel selection by EH-MB pipelined optimization technique,” *Health and Technology*, pp. 1–17, 2019.

[13] R. Karakış, I. Güler, İ. 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, doi: 10.1016/j.compbiomed.2015.10.011.

[14] A. Boonyapalanant, M. Ketcham, and M. Piyaneeranart, “Hiding Patient Injury Information in Medical Images with QR Code,” in *International Conference on Computing and Information Technology*, pp. 258–267, Jul. 2019, doi: 10.1007/978-3-030-19861-9_25.

[15] S. K. Patel, C. Saravanan, and V. K. Patel, “Cloud-based Reversible Dynamic Secure Steganography Model for embedding pathological report in medical images,” *International Journal of Computers and Applications*, pp. 1–9, 2019.

[16] P. Kamal, and G. Jindal, “Review of Different Steganographic techniques on Medical images regarding their efficiency,” *International Journal of Innovations in Engineering and Technology (IJIET)*, vol. 2, no. 1, pp. 176–180, 2013

[17] S. Elsherif, G. Mostafa, S. Farrag, and W. Alexan, “Secure message embedding in 3d images,” in *2019 International Conference on Innovative Trends in Computer Engineering (ITCE)*, Feb. 2019, pp. 117–123, doi: 10.1109/ITCE.2019.8646685.

[18] S. Arunkumar, V. Subramaniyaswamy, V. Vijayakumar, N. Chilamkurti, and R. Logesh, “SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images,” *Measurement*, vol. 139, pp. 426–437, 2019.

[19] Y. S. Abdulsalam, O. M. Olaniyi, and A. Ahmed, “Securing electronic health system using crystographic technique,” *International Journal of Telemedicine and Clinical Practices*, vol. 3, no. 2, pp. 132–155, 2019, doi: 10.1504/IJTMCP.2019.100037.

[20] 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,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pp. 487–499, 2020, doi: 10.1007/978-3-030-58817-5_36.

[21] 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)*, Oct. 2019, pp. 1–6.

[22] R. O. Ogundokun, O. C. Abikoye, S. Misra, and J. B. Awotunde, “Modified Least Significant Bit Technique for Securing Medical Images,” *Lecture Notes in Business Information Processing*, vol. 402, pp. 553–565, 2020, doi: 10.1007/978-3-030-63396-7_37.

[23] R. L. Biradar, “Secure medical image steganography through optimal pixel selection by EH-MB pipelined optimization technique,” *Health and Technology*, pp. 1–17, 2019.

[24] S. K. Patel, C. Saravanan, and V. K. Patel, “Cloud-based Reversible Dynamic Secure Steganography Model for embedding pathological report in medical images,” *International Journal of Computers and Applications*, pp. 1–9, 2019.

[25] X. Wu, J. Li, R. Tu, J. Cheng, U. A. Bhatti, and J. Ma, “Contourlet-DCT based multiple robust watermarkings for medical images,” *Multimedia Tools and Applications*, vol. 78, no. 7, pp. 8463–8480, 2019, doi: 10.1007/s11042-018-6877-5.

[26] F. W. Alsaade, “Watermarking system for the security of medical image databases used inTelemedicine,” *Res. J. Inform. Technol*., vol. 8, pp. 88–97, 2016.

[27] S. Arunkumar, S. Vairavasundaram, K. S. Ravichandran, and L. Ravi, “RIWT and QR factorization-based hybrid robust image steganography using block selection algorithm for IoT devices,” *Journal of Intelligent and Fuzzy Systems*, vol. 36, no. 5, pp. 4265–4276, 2019.

[28] R. Thanki and S. Borra, “Fragile watermarking for copyright authentication and tamper detection of medical images using compressive sensing (CS) based encryption and contourlet domain processing,” *Multimedia Tools and Applications*, vol. 78, no. 10, pp. 13905–13924, 2019.

[29] C. Irawan, E. H. Rachmawanto, C. A. Sari, and M. Doheir, “Hybrid Encryption using Confused and Stream Cipher to Improved Medical Images Security,” in *Journal of Physics: Conference Series*, vol. 1201, no. 1, May 2019, Art. No. 012022.

[30] B. Praveen, D. Samanta, G. Prasad, C. R. Kumar, and M. L. M. Prasad, “Protecting Medical Research Data Using Next Gen Steganography Approach,” in *International Conference on Information, Communication and Computing Technology*, Oct. 2019, pp. 340–348.

[31] S. I. Nipanikar and V. H. Deepthi, “A multiple criteria-based cost function using wavelet and edge transformation for medical image steganography,” *Journal of Intelligent Systems*, vol. 27, no. 3, pp. 331–347, 2018, doi: 10.1515/jisys-2016-0095.

[32] B. A. Usha, N. K. Srinath, K. Narayan, and K. N. Sangeetha, “A secure data embeddin technique in image steganography for medical images,” *International Journal of Advanced Research in Computer and Communication Engineering.*, vol. 3, no. 8, pp. 7753- 7756, 2014.

[33] 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, doi: 10.1007/s11042-020-08971-x.

[34] Y. Indresh and V. Vikash, “An Enhanced Image Steganographic Method with High Payload Capacity using Multidirectional Block Based PixelValue Differencing,” *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 1, no. 8, pp. 1888-1896, 2013.

[35] G. Santhi, and B. Adithya, “A Survey on Medical Image Protection Using Various Steganography Techniques,” *Advances in Natural and Applied Sciences*, vol. 11, no. 12, pp. 89–94, 2017.

[36] B. A. Usha, N. K. Srinath, K. Narayan, and K. N. Sangeetha, “A secure data embeddin technique in image steganography for medical images,” *Int. J. Adv. Res. Comput. Commun. Eng*, vol. 3, no. 8, pp. 7753-7756, 2014.

[37] O. C. Abikoye, U. A. Ojo, J. O. Awotunde, and R. O. Ogundokun, “A safe and secured iris template using steganography and cryptography,” *Multimedia Tools and Applications*, 2020, doi: 10.1007/s11042-020-08971-x.

[38] Kamal P. and Jindal G., “Review of Different Steganographic techniques on Medical images regarding their efficiency,” *International Journal of Innovations in Engineering and Technology (IJIET)*, vol. 2, no. 1, pp. 176–180, 2013.

[39] P. A. K. Maganbhai, and K. Chouhan, “A Study and literature Review on Image Steganography,” *International Journal of Computer Science and Information Technologies (IJCSIT)*, vol. 6, no. 1, pp. 685–688, 2015.

[40] S. Katzenbeiser and F. A. P. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking,” Artech House, Computer Security series, Boston, London, 1999.

[41] R. Islam, A. W. Naji, A. A. Zaidan, and B. B. Zaidan, “New system for secure cover file of hidden data in the image page within executable file using statistical steganography techniques,” *arXiv preprint arXiv:1002.2416*, 2010.

[42] N. A. Masoud and I. S. Ghazi, “4 A Modification of Least Significant Digit (LSD) Digital Watermark Technique,” *International Journal of Computer Applications*, vol. 179, no. 32, pp. 4–6, 2018.

[43] K. Muhammad, J. Ahmad, S. Rho, and S. W. Baik, “Image steganography for authenticity of visual contents in social networks,” *Multi Tools Appl*, pp. 1–20, 2017.

[44] M. Juneja and P. 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, doi: 10.7763/IJCCE.2013.V2.238.

[45] P. Thiyagarajan, V. Natarajan, G. Aghila, V. Pranna, and R Anitha, “Pattern Based 3D Image Steganography,” 3D Research center, Kwangwoon University and Springer 2013, 3DR Express, pp. 1–8, 2013, doi: 10.1007/3DRes.01(2013)1.

[46] S. S. Priya, K. Mahesh, and K. Kuppusamy, “Efficient Steganography Method to Implement Selected Least Significant Bits in Spatial Domain,” *International Journal of Engineering Research and Applications*, vol. 2, no. 3, pp. 2632–2637, 2012.

[47] B. Sharmila and R Shanthakumari., “Efficient Adaptive Steganography for Colour Images Based on LSBMR Algorithm,” *ICTACT Journal on Image and Video Processing*, vol. 2, no. 3, pp. 387–392, 2012.

[48] I. A. Fahim, K. B. Fateha, and U. A. K. Farid, “An Investigation into Encrypted Message Hiding Through Images Using LSB,” *International Journal of Engineering Science and Technology (IJEST)*, vol. 3, no. 2, pp. 948–960, 2011.

[49] 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, doi: 10.1109/TIFS.2010.2041812.

[50] C. H. Yang and M. H. Tsai, “Improving Histogram-based Reversible Data hiding by Interleaving Predictions,” *IET Image Processing*, vol. 4, no. 4, pp. 223–234, 2010.

[51] R. Chandramouli and N. Memon, “Analysis of LSB Based Image Steganography Techniques,” *IEEE Article*, pp. 1019–1022, 2001, doi: 10.1109/ICIP.2001.958299.

[52] S. Gupta, G. Gujral, and N. Aggarwal, “Enhanced Least Significant Bit Algorithm for Image Steganography,” *International Journal of Computational Engineering and Management (IJCEM)*, vol. 15, no. 4, pp. 40–42, 2012.

[53] M. A. Zaher, “Modified Least Significant Bit (MLSB),” *Computer and Information Science*, vol. 4, no. 1, pp. 60–67, 2011.

[54] N. Masoud, A. Hanani, and K. Ronak, “Steganography in Image Segments using Genetic Algorithm,” *IEEE Fifth International Conference on Advanced Computing and Communication Technologies*, 2015, pp. 102–107, doi: 10.1109/ACCT.2015.57.

[55] A. Kumar and R. Sharma, “A secure image steganography based on RSA algorithm and hash-LSB technique,” *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 7, pp. 363–372, 2013.

BIOGRAPHIES OF AUTHORS

Oluwakemi Christiana Abikoye is an Associate Professor at the Department of Computer Science, Faculty of Communication and Information Sciences, University of Ilorin, Ilorin, Nigeria. She received her B.Sc, M.Sc. and Ph.D degrees in Computer Science from University of Ilorin, Ilorin. She is the author or coauthor of more than 50 papers in international national and local refereed journals and conference contributions. Her research interests include Cryptography, Computer and Communication Network (Cyber) Security, Biometrics, Human Computer Interaction and Text and Data Mining.

Roseline Oluwaseun Ogundokun is a Lecturer at the Department of Computer Science, College of Pure and Applied Sciences, Landmark University, Omu Aran, Kwara State, Nigeria, she holds Bachelor of Science in Management Information System from Covenant University, Ota; Master of Science in Computer Science from the University of Ilorin, Ilorin; Post Graduate Diploma in Education (PGDE) from the National Teachers’ Institute (NTI), Kaduna and; currently a PhD student in the Department of Computer Science, University of Ilorin, Ilorin. Her research interests include Steganography and Cryptography, Information Security, Artificial Intelligence, Data Mining, Information Science and Human Computer Interaction.