Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

Secure Exchange of Confidential Information Of A Patient using Medical Image As Cover Media

Khaula Ismail
Department of Telecommunication, University of Engineering Technology Mardan, Pakistan. Email: khaula.ismail23@gmail.com

Sahib Khan
Department of Telecommunication, University of Engineering Technology Mardan, Pakistan. Email: sahib@uetmardan.edu.pk

Abstract
The proposed technique uses Steganography, which is the process of concealing confidential information in a cover media, to embed patient data in a medical image i.e., X-ray, CT-Scan, MRI etc. This technique ensures the confidentiality of the patient information i.e., medical diagnosis, test results, medical history, etc., and restricts the access of unauthorized people to the data. The confidential data is shared with only the selected and intended stakeholders, i.e. medical specialists, related laboratory experts, and authorized pharmacies. The results obtained demonstrate that the proposed technique is able to hide the secret information of the patients securely and innocently and the mere existence of the confidential data is kept hidden and unnoticeable to any unauthorized people. The hiding process preserves the quality of the medical images without affecting the medical details needed for a diagnosis process. The quality of the image remains higher than 30dB in terms of peak signal-to-noise ratio which ensures confidentiality of sensitive patient information, reports, results, and medications to avoid to the patients and avoid misuse and abuse of the medication.

Keywords: Data Hiding, Medical Image Steganography, LSB Substitution, Peak Signal to Noise Ratio, Human Visual System

I. INTRODUCTION

The science of concealing information in non-suspicious materials, or steganography, has drawn interest from various industries, including the medical field. Using digital steganography requires a typical digital encoder that encodes the secret data into the cover image. The encoder creates the stego image which contains the secretly concealed message. In casual examination and analysis, the stego image should look like the image on the cover. The encoder usually employs a stego-key in order to further guarantee that only recipients with the corresponding decoding key may extract the message from a stego image. Recovering the message from a stego image requires both the corresponding decoding key and the stego image if a stego-key was used during the encoding phase. While it is not always required, it is preferred in most applications that the cover picture not be required to extract the message. It is important to understand that cryptography and steganography are not the same. In cryptography, a message's structure is changed to make it worthless and incomprehensible without the decryption key. The encoded message is not hidden or disguised in any way by cryptography. Steganography, on the other

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

hand, conceals the hidden message under a cover without changing its structure.[1][2] Different types of mediums can be used as a cover medium for the secret information that is set to be encapsulated in the cover medium. The steganography mediums used in techniques as a cover are[2][3].

- *Image steganography:* when the medium is used for the cover photo is an image and the secret data is encapsulated in the pixels of the image.
- *Video Steganography:* when a digital video format is used to hide information. This is done by using discrete cosine transform (DCT)
- *Audio Steganography:* Wave, MPEG, etc are the digital audio formats used in Audio steganography
- *Network Steganography:* A network protocol is chosen as a carrier in network steganography such as UDP, ICMP, etc.
- *Text Steganography:* Mostly capital letters, and white spaces etch are used as a medium in text steganography.

Steganography has produced excellent results in medical imaging when it comes to hiding private data, including patient records, diagnosis, and treatment specifics. The protection of medical records, and keeping the secrecy of the results, treatment, and diagnosis of the patient is necessary because at times the diagnosis is severe, and the patient has a deadly disease. The severity of the condition puts stress on the patient causing their health to crash. It also affects the people surrounding them. The other reason is that many prescription drugs are abused by addicts to fulfil their narcotic needs. The medications are available at pharmacies and are sold to anyone with or without a prescription. To stop the misuse of the medication by addicts a very secure pharmaceutical exchange is provided in this paper, which is both secure and accessed only by authorization. Many people avoid visiting the doctors and self-medicate with medicine. Self-treating the patient, or oneself, and using the medicine without a doctor's advice creates immunity to the medication causing a decline in their health.

The cover photos used in the technique used in this paper are medical photos, which are frequently shared among healthcare professionals and are essential in diagnoses. These images contain sensitive data of the patient such as their information, medical records, and the medicine prescription. A high level of security is necessary when transferring them. Steganography in medical images enables safe data transmission. Many times, information is embedded in medical images using a variety of steganographic techniques, which can be broadly divided into two categories: frequency domain techniques (DCT Method) and spatial domain techniques (LSB Method) [4][5].

One of the main challenges when using steganography is maintaining the diagnostic quality of medical images. Medical professionals rely heavily on image features to make accurate diagnoses; even minor distortions can affect a picture's clinical value. The proposed technique ensures the quality of the image and protects its integrity, providing it accurate for diagnosis. High robustness is offered by more complex techniques like DCT and DWT, but they may also be more complex to implement and more vulnerable to computational overloads [3][6]. To find or eliminate hidden data, attackers may employ steganalysis techniques, which aim to reveal or eliminate the embedded data [6][7]. The proposed technique is a structured and secure way of transferring sensitive information as authorization to access the information is a key part.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

II. LITERATURE REVIEW

Sensitive data in medical imaging must be protected, steganography, the study of hiding information within seemingly harmless carriers, has grown in importance. The goal of this review of the literature is to give a thorough overview of the work that has been done so far and the latest advancements in the use of steganography to improve data security and concealment in medical imaging. Many steganography techniques are used to on preferences to hide the sensitive data. These techniques are divided into two main domains [2, 8, 9] i.e., transform domain techniques and spatial domain techniques.

The transform domain techniques use the coefficient of the respective transform and embed the secret information in the least significant bits of the coefficient and least significant coefficients. A variety of Algorithms and modifications are implemented to hide the information. It can be categorized as follows:

- Discrete cosine transformation technique (DCT)
- Discrete Wavelet Transformation Technique (DWT)
- Discrete Fourier Transformation Technique

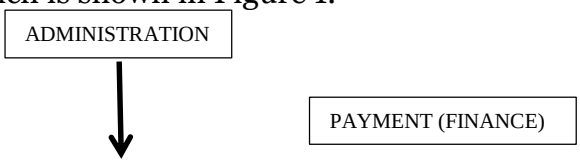
In the spatial domain techniques, the least significant bits of cover image pixels are used for embedding the confidential data. The well-known techniques of this family include:

- Pixel Value Differencing
- Edge-Based Data Embedding Method
- Least Significant Bit (LSB)
- Random Pixel Embedding Method

Steganography is crucial for securely transferring medical images, especially as telemedicine becomes more and more common. Steganography can facilitate secure communication for online consultations and diagnostics, according to research. During image transfer, confidentiality and integrity are prioritized. To maintain a balance between data security and collaborative research projects, scientists have looked into the application of steganography to secure medical image sharing and collaboration. Using steganography for forensic purposes, researchers have examined the traceability of medical images. Studies demonstrate that steganographic methods aid in forensic investigations by ensuring the authenticity and integrity of medical data. Recent research has focused on preventing accidental data leaks in medical images [10-14].

III. METHODOLOGY

A patient arrives at a medical establishment for their ailment or medical-related emergency. They are directed to the administration section where they provide all their personal information, which is uploaded into the centralized information system (CIS). A centralized information System (CIS) is an interconnected secure network, connecting all the departments of the establishment, providing secure transfer of the cover photo containing sensitive information along with communication as well which is shown in Figure 1.



Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

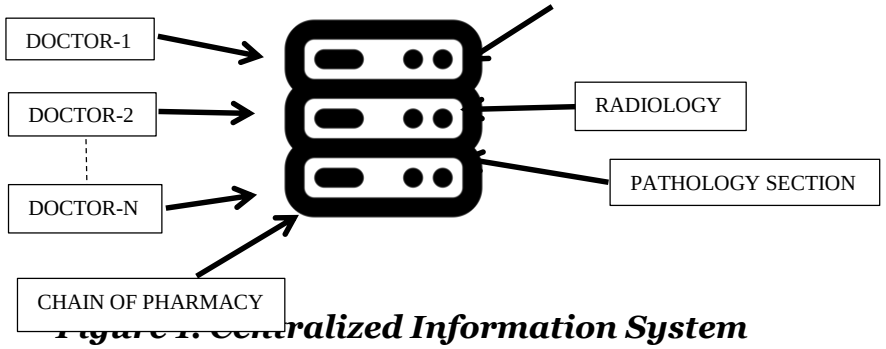


Figure 1. Centralized Information System

During this process, a photograph is also captured of them and uploaded to the central information system. The initial photograph of the patient is used by the concerned doctor as a cover photo to add the tests and initial findings, it is later forwarded to the concerned department for further investigation. After the administration process, the patient is directed to the payment desk (finance section) to initially deposit payment for the concerned doctor's appointment. Once the patient is with the doctor the process of data embedding starts.
The proposed framework consists of the following stages:

- Initial evaluation stage
- Testing and result stage
- Medicine prescription
- Pharmaceutical stage.

A. Initial evaluation stage

The initial evaluation stage consists of two stages, the administration stage and payment stage, secondly the doctor's evaluation stage. The administration and payment stage consists of simply the patient entering the establishment providing their information along with their photograph and heading to the payment desk to pay for the doctor's appointment.
Once the patient is with the doctor, the concerns of the patient are evaluated extensively by the doctor. The doctor after concluding prescribes some tests and some X-rays, MRIs, or a CT scan. The list of the tests will be used as a secret message. The secret message is binarized and is divided into chunks or groups of 4 bits. It is embedded in the 4 least significant bits of the top left fixes of the image.
Each test in the proposed method is presented in 36 bits so hiding 4 bits, each test will require 9 pixels to be for embedding. Each test name (ID) is hidden in the individual group, if there are n number of tests prescribed it will require n rows and 9 pixels of each row, so, it will utilize 9xn pixels of the top left side of the image. The cover image will be shared with the pathology expert via a centralized system.

B. Testing and result stage

In this stage the proposed technique retrieves the hidden information or bits hidden in **Stage A** and retrieves 4 bits from each pixel in the reverse order, using the reverse of 4 LSB embedding technique by the pathology/radiology section. By this retrieval process, the pathology section gets a list of all the prescribed tests. The expert performs the test and gets the results and reports. Based on each test they generate a report, and the report is hidden in the pixels of the top right of

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

the image using the 4 LSB technique. Similar to **Stage A** the results of each test are hidden in a single row. Each test in the proposed method is presented in 36 bits so hiding 4 bits, each test requires 9 pixels to be for embedding. After the embedding of the test results the cover image is shared with the doctor via CIS as presented in *Figure 1*. Whereas the results of the MRI, X-ray, or CT scan are extensive reports, hence specifically those reports are embedded in the medical image of the required X-ray, MRI, CT scan. This is because the extensive report along with other data from different concerned medical departments might distort the medical image.

C. Medicine prescription stage

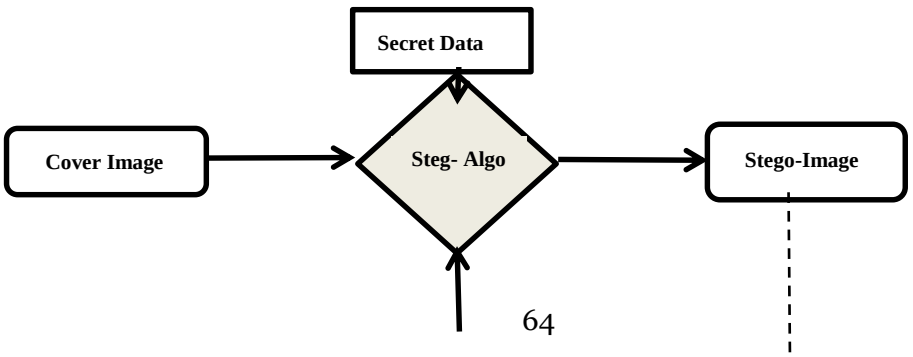
The concerned doctor after receiving the image retrieves the relevant results of the test embedded in the second stage using the 4 LSB retrieval process. [15] Based on the initial scrutinizing and the test results the doctor prescribes the medicine to the patient if required. The prescription is not directly shared with the patient; it is shared with the authorized pharmacy. For this purpose, the list of medicines is binarized and embedded through the 4 LSB technique on the bottom left side of the image. The name of each medicine is embedded in a single row.

If m number of medicine is prescribed, 9xm number of right left bottom pixels will be utilized. The process images are shared with the authorized pharmacies using a centralized system (CIS).

D. Pharmaceutical stage

The authorized pharmacies when receiving the cover image of the patient, the concerned pharmacist retrieves the embedded information from the designated location which is the bottom left of the image. The information is retrieved by the reverse 4 LSB method, a list of medicines is obtained by the pharmacy doctor, who then provides the patient with the right medicine and the exact dosage prescribed by the concerned doctor.

Having discussed the proposed framework, each of the steps involves either data embedding, data retrieval, or both. When secret information is embedded in a medical image it follows a series of steps to ensure credibility and authentication of such information. A medical image is taken as a cover image. It is passed through a steganographic algorithm, the secret data is embedded in it using a steganographic key which is unique every time. A steganographic image is generated which is then transmitted to the concerned party as shown in *Figure 2*. The data embedding process is carried out if the authorization for data embedding is approved to ensure the security of confidential information.



Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

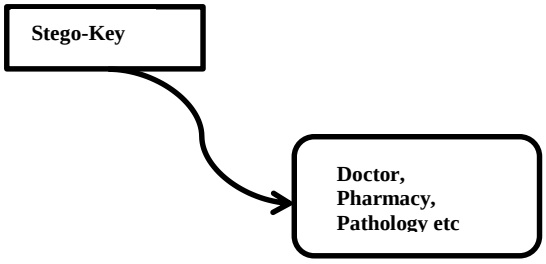


Figure 2. Data Embedding

When a steganographic image is received, there is secret information embedded in it. To retrieve the confidential data the image is processed through the retrieval algorithm, and the steganographic key is used to retrieve the data in the retrieval algorithm as shown in Figure 3. This process only takes effect if the authorization is approved for the retrieval process.

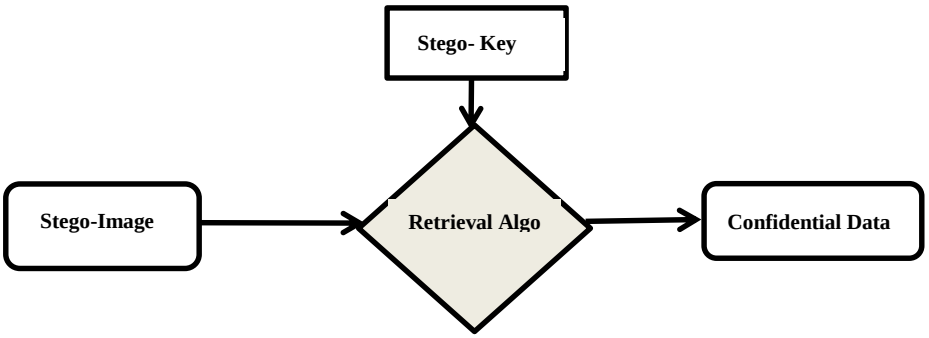


Figure 3. Retrieval Process

VI. RESULTS

As discussed in methodology II (A), a patient visits the medical establishment, goes through a series of processes, and has an initial evaluation with a concerned doctor. The proposed algorithm embeds the confidential data into the cover image. The data such as tests are assigned unique codes to differentiate from the other data, as shown in Table 1, and to binarize them to embed in the cover image. Each test in the proposed method is presented in 36 bits, i-e hiding 4 bits, and each test requires 9 pixels as discussed in methodology II (B) for embedding the data. Each test is embedded in a single row in the top left corner of the image following the process shown in Figure 2.

Table 1: List of Test, Test Codes and Result Codes

SERIAL NUMBER	**TESTS**	**RESULTS**
8350	TROPONIN	13
2590	CRP	180

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

1550	CBC	10
4360	BNP	0
25452	LIPID PROFILE	120
1263584	CARDIAC CT-SCAN	

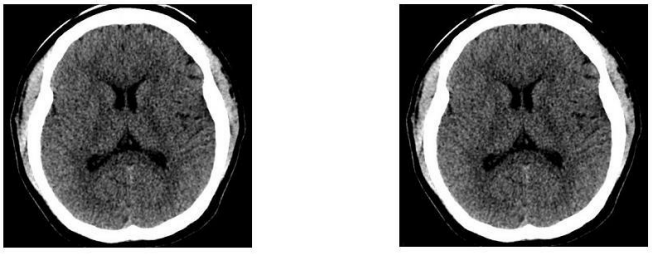
The reports of the tests are retrieved by the concerned doctor following the process shown in Figure 3. The reports of the tests are referenced with the same codes as the tests as shown in Table 2. The data of the reports is embedded in the top right corner of the cover image following the process shown in Figure 2 using 9 pixels for embedding 4 bits of data as discussed in methodology II(B). Each report of the test is embedded in a single row of the image in the specified location i.e., the top right corner of the image to avoid any overlap with other data embedded into the image.

The doctor prescribes medicine to the patient. Each of the medicine has an unique code as shown in Table 2. The medicine details are embedded into the bottom left corner of the cover image following the process shown in Figure 2. Using the 4 LSB method, as discussed in methodology II(C) each medicine is embedded in a single row of the specified location of the cover image to avoid overlapping and losing data.

Table 2: Medicine and respective Codes

SERIAL NUMBER	**MEDICINE**
101	ANTICOAGULANT
110	ASPIRIN
1000	DIURETIC
1500	CHOLESTROL MEDICATION
120	ANTIARRHYTHMIC AGENT
1300	BETA BLOCKERS

Authorized Pharmacies retrieve the data following the process shown in Figure 3 and give the patient their medicine as discussed in methodology II (D). The proposed method ensures the integrity of the image, and no visible difference can be detected through the Human Visual System (HVS) as given in Figure 4.



(a) *(b)*

Figure 4.. a) Cover image (CT Scan), b) Stego image with hidden information of the patient

To ensure the quality of the image is not affected by the embedding of the information, PSNR, SSIM, and MSE, is calculated at all the 3 stages of

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

embedding information. The results of which are shown in Table 4.

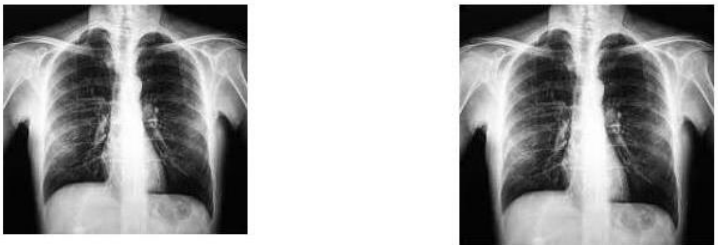
Table-2: Quantitative analysis of the proposed framework using Brain CT-Scan.

STAGES	PSNR	SSIM	MSE	HIDING CAPACITY
STAGE 1	Infinity	0.9997	0	0.0205
STAGE 2	Infinity	0.9999	0	0.0411
STAGE 3	Infinity	0.9997	0	0.0616

To prove the credibility of the proposed method more than one Test example was done further, which made it evident that the proposed method holds the integrity of the image intact and hides the data innocently from the Human Visual System (HVS).
Another test is performed using a Chest X-ray, when confidential data is embedded into the X-ray which is being used as the cover image for the patient, the data is embedded into the cover image i.e., Figure. 5(a), as stated in Methodology II(B) we get the Stego-Image i.e., Figure. 5(b). It is evident from the images that the integrity of the image is intact and there is no visible difference in both the images as shown in Figure. 5, Evaluation metrics such as PSNR, SSIM, MSE, and Hiding capacity are applied. The results are shown in Table 5.

Table-5: Quantitative analysis of the proposed framework using Chest X-ray.

STAGES	PSNR	SSIM	MSE	HIDING CAPACITY
STAGE 1	135.7081	0.9994	0.0831	0.0460
STAGE 2	140.9131	0.9994	0.0494	0.0919
STAGE 3	158.1170	0.9996	0.0088	0.1379



(a) *(b).*

Figure 5:.a) Cover image (Chest X-ray), b) Stego image with hidden information of the patient

Using another X-ray image to deduce the results that embedded important data into the medical image does not affect the quality or integrity of the image. It is clear from the results of calculating the PSNR, SSIM, and MSE as shown in Table 6. that the quality of the image is not affected, as shown in Figure. 6.

Table-6: Quantitative analysis of the proposed framework using Hand X-ray.

STAGES	PSNR	SSIM	MSE	HIDING CAPACITY
STAGE 1	170.6427	1.0000	0.0025	0.0023
STAGE 2	168.6158	1.0000	0.0028	0.0047

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

STAGE 3	167.2941	1.0000	0.0035	0.0070

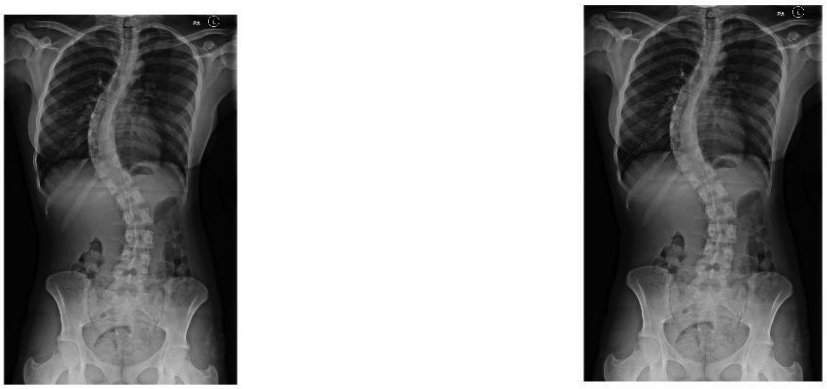
(a) *(b)*

Figure 5:. a) Cover image (Chest X-ray), b) Stego image with hidden information of the patient

Some images are of greater quality than others. Using a high-quality image as another Medical image, used as a cover photo as shown in Figure 6(a) to securely store all the information and confidential data, has no significant effect on the quality of the image which can be seen from the naked eye as shown in Figure 6(b) which is the Stego-image. When calculating PSNR, SSIM, and MSE the results show no significant change in the image as shown in Table 7.

Table-6: Quantitative analysis of the proposed framework using *Spine X-ray*.

STAGES	**PSNR**	**SSIM**	**MSE**	**HIDING CAPACITY**
STAGE 1	166.6414	1.0000	0.0038	0.0021
STAGE 2	170.0446	1.0000	0.0027	0.0042
STAGE 3	182.2337	1.0000	7.9209e-04	0.0063



(a) *(b)*

Figure 6:.a) Cover image (Spine X-ray), b) Stego image with hidden information of the patient

VII. CONCLUSION

In this paper, we have used the 4-LSB method to implement steganography to securely hide confidential data in the pixels of the medical image without causing any changes in the image. Any changes occurring in the image would instantly make the image lose its integrity and a medical image that is used as a cover

ISSN Online: 3007-3154
ISSN Print: 3007-3146

photo would not be considered credible on the base of which any credible diagnosis is given. The proposed algorithm embeds confidential information into the medical image, which is used as a cover photo to securely hide confidential data, which ensures the image does not lose its credibility and integrity.

REFERENCES

[1]. E. T. Lin and E. J. Delp, "A Review of Data Hiding in Digital Images," *Soc. Imaging Sci. Technol. Image Process. Image Qual. Image Capture, Syst. Conf.*, pp. 274–278, 1999.
[2]. R. Sindhu and P. Singh, "Information Hiding using Steganography," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 4, pp. 1549–1554, 2020, doi: 10.35940/ijeat.d8760.049420.
[3]. M. D. Swanson, B. Zhu, and A. H. Tewfik, "Robust data hiding for images," *IEEE Digit. Signal Process. Work.*, pp. 37–40, 1996, doi: 10.1109/dspws.1996.555454.
[4]. J. Shukla and M. Shandilya, "A Recent Survey on Information-Hiding Techniques," *Data, Eng. Appl. Vol. 1*, vol. 1, pp. 57–70, 2019, doi: 10.1007/978-981-13-6347-4_6.
[5]. N. I. Wu and M. S. Hwang, "Data hiding: Current status and key issues," *Int. J. Netw. Secur.*, vol. 4, no. 1, pp. 1–9, 2007.
[6]. M. A. Dăgădiţă, E. I. Sluşanschi, and R. Dobre, "Data hiding using steganography," *Proc. - 2013 IEEE 12th Int. Symp. Parallel Distrib. Comput. ISPDC 2013*, pp. 159–166, 2013, doi: 10.1109/ISPDC.2013.29.
[7]. Hua, C., Wu, Y., Shi, Y., Hu, M., Xie, R., Zhai, G., & Zhang, X. (2023). Steganography for medical record image. *Computers in Biology and Medicine*, *165*, 107344. https://doi.org/10.1016/j.compbiomed.2023.107344
[8]. Chowdhuri, P., Pal, P., & Si, T. (2023, January 6). *A novel steganographic technique for medical image using SVM and IWT*. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-022-14301-0
[9]. Karawia, A. A. (2021). Medical image steganographic algorithm via modified LSB method and chaotic map. *IET Image Processing*, *15*(11), 2580-2590. https://doi.org/10.1049/ipr2.12246
[10]. P. A, U. R, J. N and P. S, "Securing Medical Images using Encryption and LSB Steganography," 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 2021, pp. 1-5, doi: 10.1109/ICAECT49130.2021.9392396.
[11]. Abdul, W. (2022). Security of medical images over insecure communication channels using zero-steganography. *International Journal of Distributed Sensor Networks*. https://doi.org/10.1177/15501477211006347
[12]. Ahmad, M. A., Elloumi, M., Samak, A. H., Al-Sharafi, A. M., Alqazzaz, A., Kaid, M. A., & Iliopoulos, C. S. (2022, December 1). *Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images*. Alexandria Engineering Journal. https://doi.org/10.1016/j.aej.2022.03.056
[13]. Manikandan, T., Muruganandham, A., Babuji, R., Nandalal, V., & Iqbal, J. M. (2021, June 1). *Secure E-Health using Images Steganography*. Journal of Physics. https://doi.org/10.1088/1742-6596/1917/1/012016
[14]. Hussien, A. Y. (2022, January 1). *Image Steganography Based Spatial*

ISSN Online: 3007-3154
ISSN Print: 3007-3146

and Transform Domain Techniques: A Review. https://doi.org/10.54216/fpa.080101
[15]. Shtayt, B. A., Zakaria, N. H., & Harun, N. H. (2021, June 20). *A Comprehensive Review on Medical Image Steganography Based on LSB Technique and Potential Challenges*. Baghdad Science Journal. https://doi.org/10.21123/bsj.2021.18.2(suppl.).0957
[16]. *Khan, S. (2021). CLIFD: A novel image forgery detection technique using digital signatures. Journal of Engineering Research, 9(1).*
[17]. *Khan, S., Irfan, M. A., Khan, K., Khan, M., Khan, T., Khan, R. U., & Ijaz, M. F. (2020). ACO based variable least significant bits data hiding in edges using IDIBS algorithm. Symmetry, 12(5), 781.*
[18]. Vazquez, E., Torres, S., Sánchez, G., Avalos, J. G., Abarca, M., Frias, T., Juarez, E., Trejo, C., & Hernandez, D. (2022, October 6). *Confidentiality in medical images through a genetic-based steganography algorithm in artificial intelligence*. Frontiers in Robotics and AI. https://doi.org/10.3389/frobt.2022.1031299
[19]. AlEisa, H. N. (2022, May 6). *Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things*. Journal of Healthcare Engineering. https://doi.org/10.1155/2022/7528583
[20]. Chowdhuri, P., Pal, P., & Si, T. (2023, January 6). *A novel steganographic technique for medical image using SVM and IWT*. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-022-14301-0
[21]. Mansour, R. F., & Girgis, M. R. (2021). Steganography-Based transmission of medical images over unsecure network for telemedicine applications. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *68*(3), 4069–4085. https://doi.org/10.32604/cmc.2021.017064
[22]. Chunjun Hua, Yue Wu, Yiqiao Shi, Menghan Hu, Rong Xie, Guangtao Zhai, Xiao-Ping Zhang, Steganography for medical record image,Computers in Biology and Medicine, Volume165,2023,107344,ISSN0010-4825, https://doi.org/10.1016/j.compbiomed.2023.107344.
[23]. Songul Karakus, Engin Avci,A new image steganography method with optimum pixel similarity for data hiding in medicalimages,MedicalHypotheses,Volume139,2020,109691,ISSN0306-9877,https://doi.org/10.1016/j.mehy.2020.109691.
[24]. Mostafa A. Ahmad, Mourad Elloumi, Ahmed H. Samak, Ali M. Al-Sharafi, Ali Alqazzaz, Monir Abdullah Kaid, Costas Iliopoulos, Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images, Alexandria Engineering Journal, Volume 61, Issue 12,2022, Pages 10577-10592, ISSN 1110-0168, https://doi.org/10.1016/j.aej.2022.03.056.
[25]. *A high quality secure medical image steganography method*. (2023, September 13). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/10273950
[26]. Mansour, R. F., & Girgis, M. R. (2021c). Steganography-Based transmission of medical images over unsecure network for telemedicine applications. *Computers, Materials & Continua/Computers, Materials & Continua (Print)*, *68*(3), 4069–4085. https://doi.org/10.32604/cmc.2021.017064

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 6 (June) (2025)

[27]. Karawia, A. A. (2021). Medical image steganographic algorithm via modified LSB method and chaotic map. *IET Image Processing*, *15*(11), 2580-2590. https://doi.org/10.1049/ipr2.12246