1573-4056/24

*Send Orders for Reprints to reprints@benthamscience.net*

BENTHAM SCIENCE

Current Medical Imaging

Content list available at: https://benthamscience.com/journals/cmir

RESEARCH ARTICLE

# Patient Data Hiding and Transmitting during COVID-19 for Telemedicine Application using Image Steganography

B Lakshmi Sirisha[1,*], Shaik Fayaz Ahamed[1] and VBKL Aruna[1]

[1]*Department of Electronics and Communication Engineering, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, India*

**Abstract:**

***Aim of the Study:***

Post COVID-19, everyone needs to be aware of health. The condition of the human body is judged based on various health reports like X-ray, CT scan and MRI scan. Due to misplacement or loss of medical reports, there lies a high chance of improper diagnosis.

***Methods:***

In order to avoid improper diagnosis, a novel data-hiding technique is proposed in this work. In the proposed method, the patient's health records are hidden using polynomial theory in the patient photograph. This is used by doctors in telemedicine for better treatment at the right time. Image steganography is useful for hiding secret images and also for generating secret keys. This enables only the authorized people (patient and corresponding doctor) to access the reports using secret keys.

***Results:***

Four secret images (medical reports of the patient) are successfully embedded onto a single cover image (patient photo) with good quality. After embedding, the stego images look like cover images so that unauthorized persons will not be able to access the data, and hence, safe transmission is being carried out.

***Conclusion:***

A patient's medical report plays an important role in proper medical treatment. Particularly in telemedicine, the safe transmission of patient reports without any loss or damage is necessary. The proposed method embeds reports of a patient in his/her photo and transmits them to the destination safely with a quality of 45.5 dB. This hiding method is helpful to avoid cyber crimes, illegal transactions, malpractices *etc*.

**Keywords:** COVID-19, Data hiding, Image metrics, Steganography, Telemedicine, Internet.

| **Article History** | Received: November 16, 2023 | Revised: January 12, 2024 | Accepted: January 25, 2024 |
|---|---|---|---|

## 1. INTRODUCTION

Transmitting digital data over the internet is not safe, as it leads to the deception of data. Hence, a highly secure means of data communication is required. In the present technology, the public applications are flooded with private data. A similar problem has to be addressed in telemedicine applications. In telediagnosis, the treatment is given based on the health reports of the patient. The confidentiality and quality of the reports are the prominent challenging issues. Data hiding [1 - 3] is one of the solutions to maintain security. The most popular data-hiding techniques are cryptography, watermarking, and steganography. Cryptography [4 - 6] hides the meaning of the data. 2D-LAIC can generate an unpredictable keystream, which is highly suitable for cryptography, and exhibit better dynamical behavior than classical chaotic systems. Watermarking [7 - 9] is to create a translucent image on paper to provide authenticity. One of the key tools for securing image communication is image encryption technology. Well-established methods like DES, AES, and 3DES are used to encrypt text data. However, these algorithms are not relevant when processing images with high data volumes and strong pixel-to-pixel correlations; in these cases, statistical analysis

[*] Address correspondence to this author at the Department of Electronics and Communication Engineering, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, India; E-mail: suravarapuls@yahoo.co.in

DOI: 10.2174/0115734056276785240229073917, 2024, *20*, e15734056276785

can be easily used instead. Furthermore, these encryption methods have very low efficiency. Steganography [10 - 13] is a method of hiding information that does not arouse suspicion. “Steganos” means covered or hidden, and “graphics” is derived from the Greek language, which means writing. Steganography is mainly used in security applications like covert communication, legal fields, and copyright control. Image steganography hides the secret images into a cover image with the help of secret keys to generate stego. Stego and cover data are identical. However, stego data contains both secret and cover essence. An unauthorized person cannot identify or change the secret data. Only an authorized person can access the original data. These techniques are very useful and essential for today’s digital world applications.

## 2. RELATED WORKS

A.H. Mohsin *et al.* [14] proposed a method for COVID-19 data security. This approach is performed based on blockchain technology and hash function. In this method, the patient’s data is hidden in the hospital database. Their results show good embedding capacity and stego quality. However, this is a study work only and is not implemented on real patient reports.

Ghazanfar Farooq Siddiquie *et al.* [15], proposed the Image Region Decomposition (IRD) approach that embedded more concealed information with greater visual quality. The proposed IRD techniques produced excellent results in terms of unobtrusiveness and payload volume. On a set of standard pictures, the IRD approach was also put to the test. Various high-resolution image formats of different areas, and colour photos of the body, were used with the proposed IRD approach.

Aditya Kumar Sahu *et al.* [16] proposed a steganography method that progressed at the same rate as steganalysis. Multiple photo steganography methods are compared to three diametrically opposed steganographic measures. The existing issues as well as prospects are highlighted. Furthermore, steganography, and steganalysis are growing in popularity in this digital age.

Roseline Oluwaseun *et al.* [17] proposed a method that addressed the critical authentication issues. A changed Least Significant Bit (LSB) approach was set up for retaining and concealing medical data. According to the findings of the study, the proposed technique can add medical data to stego photos without leaving a visible deception. When compared to other current systems, with a few entrenching falsifications, the secured healthcare data platform is found to be capable of hiding medical data and developing undetectable stego images. This study also developed a vital info-enabling strategy for protecting its secret and privacy by disguising the existing patient data. However, when compared to other systems, the proposed protected medical information system had a high embedding rate, resulting in an excellent balance of concealment and stego image quality.

Nandhini Subramanian *et al.* [18] proposed a method for the act of concealing hidden information under a cover image that is visible to the naked eye. Overburdening the cover-up image with more pixels to hide the hidden information can result in distorted images, therefore, traditional techniques have a limited hiding capacity.

Faizana Naeem *et al.* [19] proposed a method due to the privacy and confidentiality of information of the patient, and the main cause arises when it comes through individual assessment of medical reports. Secure storage as well as distribution of medical data is frequently hampered by an ever-changing threat landscape by many hackers or attackers. As per the latest cyber reports, it was found that there was a gradual increase in the number of confidentiality flaws and unaware users were accessing this sensitive data. The traditional cryptography and steganography techniques are commonly used to safeguard and conceal files. However, the files are prone to execution errors. The best technique to handle this is Steganography, by which we can hide the secret data into another cover picture and secure the data, a violation of which can result in displaying the secret data.

Zhou *et al.*, [20] proposed a coverless steganographic approach for transmitting a hidden color image that was not edited. The Stego pictures are constructed by splitting every image in the database into various unmodified pictures and naming those pictures related to the behavior of the decoded pictures. Each of these images shares one or more visually related patches with the database's hidden pictures. A stego picture is a normal picture with no changes. This steganography not only withstands steganalysis but also gives a high level of security and concealment.

## 3. PROPOSED METHODOLOGY

The proposed method, as shown in Fig. (**1**), embeds four secret images (patient images like x-rays, scanning reports, test reports) into a cover image (patient photo). All input images are of the same size. The entire process is performed by using polynomial methodology.

### 3.1. Embedding Algorithm

Polynomial theory for steganography is proposed by Shamir’s scheme [21]. Shamir’s scheme embeds one secret image into one cover image. Based on that concept in the proposed method, four secret images are embedded into a single cover image. The embedding procedure is as follows,

#### *3.1.1. Step 1*

Firstly, all secret images are multiplied with some predefined threshold value. As per Shamir’s scheme the threshold value range is from 0 to 1. In the proposed work, the threshold value is chosen as 0.1., so that the gray level value of secret images decreases more than cover image. When the cover gray value is greater than the secret value, the concealment of the secret value is easy and safe. The same threshold value is set at the receiver side for reconstruction.

#### *3.1.2. Step 2*

Generate a 4th-degree polynomial equation using four secret images and a cover image is given by the following equation

$$f(x) = ax^4 + bx^3 + cx^2 + dx^1 + e \qquad (1)$$

where *a, b, c, d* are the pixels of secret images 1, 2, 3, and 4, respectively. The constant value *e* is the cover image pixel.

### *3.1.3. Step 3*

A stego image is generated by placing the secret keys into Eq. (**1**) using polynomial functions as the following:

$$y(1) = f(1), y(2) = f(2), \ldots. y(n) = f(n) \qquad \textbf{(2)}$$

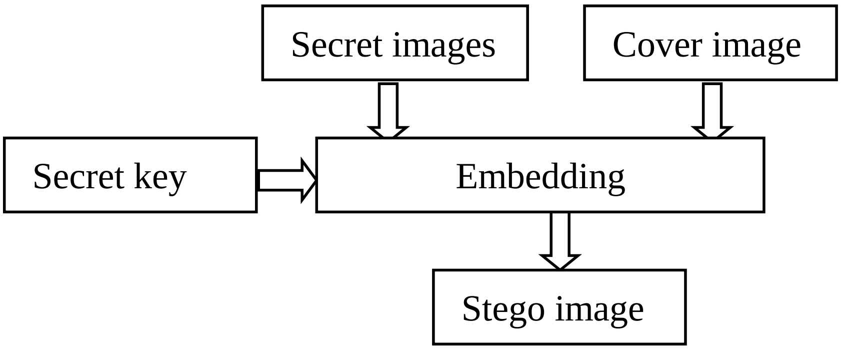
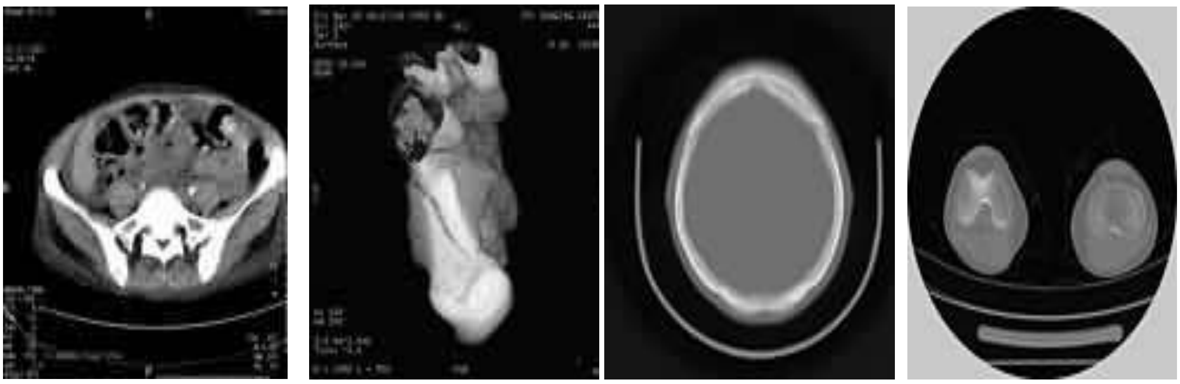
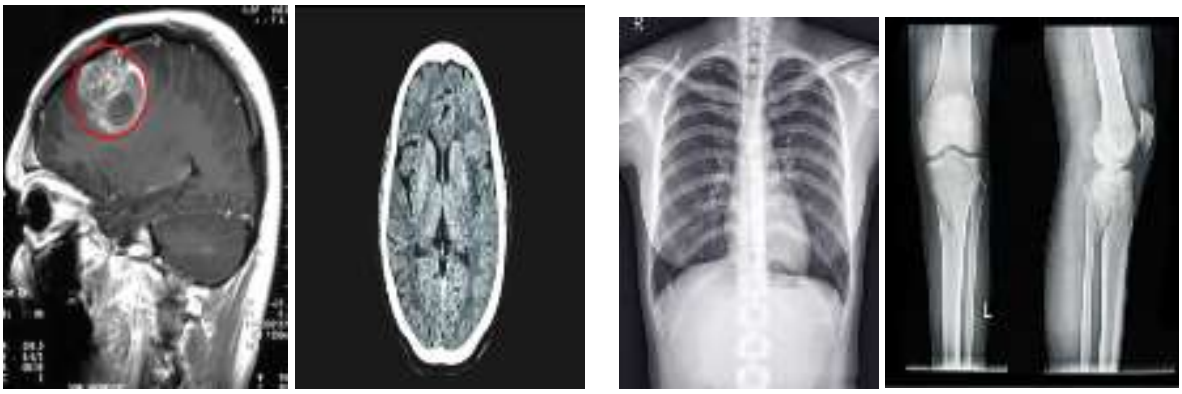


**Fig. (1).** Embedding procedure.



secret 1 secret 2 secret 3 secret 4

Set 1 testing images



**secret 1** **secret 2** **secret 3** **secret 4**

Set 2 testing images

**Fig. (2).** Results of the embedding algorithm.

For the embedding procedure, four secret keys and two sets of medical report images (secrets) were considered for experimentation. When the number of secret keys increases, it means the security also increases; however, solving entire equations becomes complex. Secret key 1 is an abdomen CT scan, Secret key 2 is an ankle CT scan, secret key 3 is a brain CT scan, and secret key 4 is an ort CT scan, these are considered as set 1. Similarly, secret key 1 is a brain CT scan, secret key 2 is an abdomen CT scan, secret key 3 is a chest CT scan, and secret key 4 is a leg bone CT scan, these are considered as set 2. The benchmark gray level image 'Lena' is considered a patient photo for the cover image. After embedding four secret images into the cover image to get a stego image, which will be very similar to the cover image, as shown in Fig. (**2**). Moreover, because the Stego image resembles a cover image, safe communication can occur because unauthorized parties cannot assume that the secret data is included. In the proposed work, up to 4 secret images are embedded in a single cover image with good quality, as shown in Fig. (**3**). When more than four secret images are embedded, it means the quality of the stego image decreases, and the secrets are out from the cover image, as shown in Fig. **4**, so that the unauthorized indivduals also have a chance to obtain the secret information.

**Fig. (3).** Stego image with 4 secret images embedded.

**Fig. (4).** Stego image with more than 4 secret images embedded.

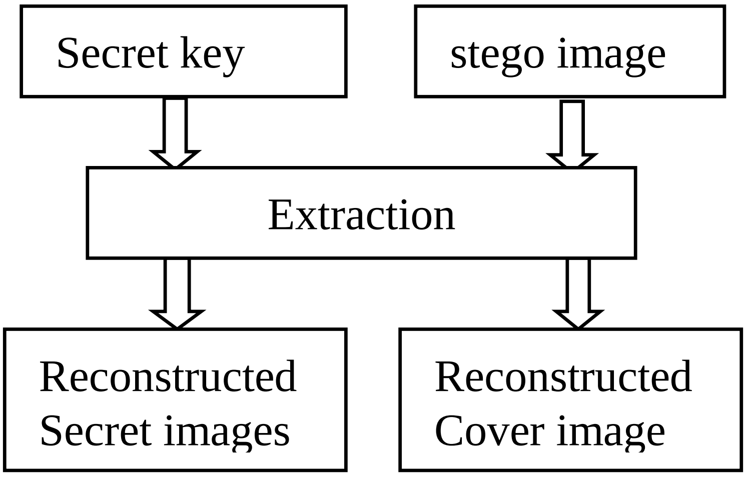


**Fig. (5).** Extraction procedure.

### 3.2. Extraction Algorithm

Stego image, threshold value, and the secret keys are provided for the receiver to recover the secret and cover images. The algorithm is shown in Fig. (**5**).

#### *3.2.1. Step 1*

The inverse matrix method is applied with the help of secret keys on the stego image to recover the coefficients of 4th order degree polynomial function *f*(*x*).

#### *3.2.2. Step 2*

The coefficient of $x^4$ is considered a secret image with 1 pixel, similarly, the coefficient of $x^3$, $x^2$, $x^1$ are secret images 2, 3, and 4 pixels, respectively. These pixels are formed in a proper order to obtain images of size *MXN*. In the proposed work, 512 × 512 images are considered.

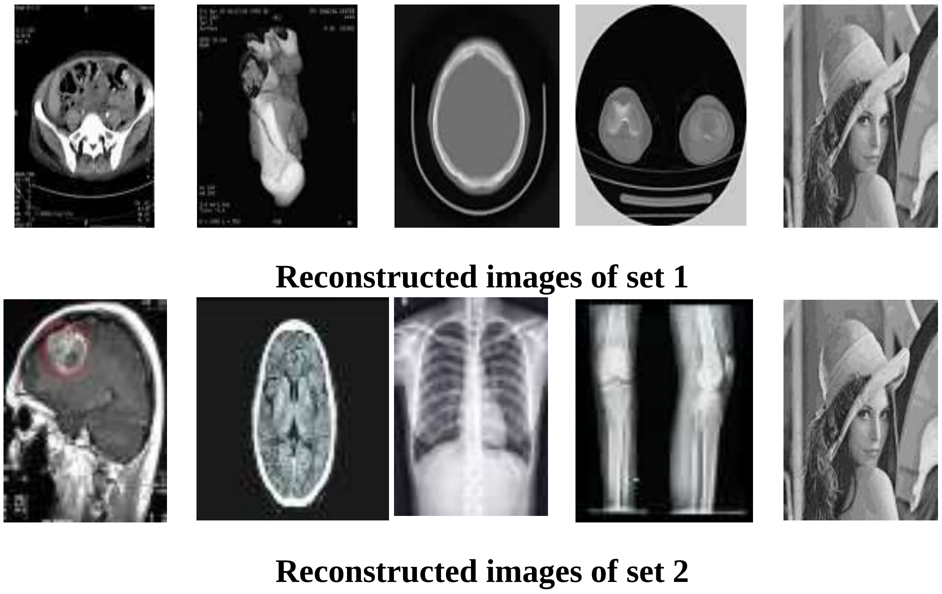
#### *3.2.3. Step 3*

Finally, these images are divided with threshold values to recover the secret images. The constant value is considered as the cover pixel. Therefore, all secret images and cover images are recovered without any damage. Reconstructed images are shown in Fig. (**6**).

### 4. RESULT ANALYSIS AND DISCUSSIONS

Stego image quality and embedding capacity are the main targets in the proposed work. The quality is measured based on the Peak Signal to Noise Ratio (*PSNR*). A higher *PSNR* value indicates a higher quality of reconstruction.

$$PSNR = 10log\frac{255^2}{MSE} \quad \textbf{(3)}$$



Reconstructed images of set 1

Reconstructed images of set 2

**Fig. (6).** Results of the extraction algorithm.

The similarity between the stego and cover is measured by Structural content (*SC*)

$$SC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{ij})^2}{\sum_{i=1}^{m}\sum_{j=1}^{n}(B_{ij})^2} \quad \textbf{(4)}$$

A greater *SC* (Structural Content) rating indicates that cover and stego images look similar to each other. So that unauthorized intender cannot imagine the content which is embedded in the stego image. The reference range of SC is 0 - 1. The embedding capacity indicates, the number of secret bits embedded into the cover image as shown in Tables **1** and **2**. *M X N* represents the size of the images (both secret and cover).

The embedding capacity and quality of the stego image are inversely proportional to each other, as shown in Table **1**. As shown in Table **1**, a single secret image embedded into the cover image to achieved a PSNR of 75.1dB, and similarly, two secret images embedded achieved a PSNR of 68.9 dB. The results indicates that, more images embedded into a cover image will effect the quality of the stego image. The number of secret images embedded increases, however, the stego image quality decreases. Another set of results is shown in Table **2**.

**Table 1. Result analysis of stego image for set 1.**

| Secret Images | Cover Image | PSNR (dB) | SC | Embedding Capacity |
|---|---|---|---|---|
| **Embedding of One Image** | | | | |
| Secret image 1 | Lena image | 75.1 | 0.9997 | 1 *M X N* |
| **Embedding of two images** | | | | |
| Secret images 1 & 2 | Lena image | 68.9 | 0.9994 | 2 *M X N* |
| Secret images 3 & 4 | Lena image | 68.7 | 0.9993 | 2 *M X N* |
| **Embedding of three images** | | | | |
| Secret images 1, 2 & 3 | Lena image | 52.8 | 0.9989 | 3 *M X N* |
| Secret images 2, 3 & 4 | Lena image | 53.1 | 0.9990 | 3 *M X N* |
| **Embedding of four images** | | | | |
| Secret images 1, 2, 3 & 4 | Lena image | 45.5 | 0.9981 | 4 *M X N* |

**Table 2. Result analysis of stego image for set 2.**

| Secret Images | Cover Image | PSNR (dB) | SC | Embedding Capacity |
|---|---|---|---|---|
| **Embedding of one image** | | | | |
| Secret image 1 | Lena image | 78.02 | 0.9998 | 1 *M X N* |
| **Embedding of two images** | | | | |
| Secret images 1 & 2 | Lena image | 70.43 | 0.9997 | 2 *M X N* |
| Secret images 3&4 | Lena image | 67.12 | 0.9995 | 2 *M X N* |

*(Table 2) contd.....*

| Secret Images | Cover Image | PSNR (dB) | SC | Embedding Capacity |
|---|---|---|---|---|
| **Embedding of one image** | | | | |
| **Embedding of three images** | | | | |
| Secret images 1, 2 & 3 | Lena image | 63.89 | 0.9991 | 3 *M X N* |
| Secret images 2, 3 & 4 | Lena image | 55.26 | 0.9987 | 3 *M X N* |
| **Embedding of four images** | | | | |
| Secret images 1, 2, 3 & 4 | Lena image | 47.20 | 0.9984 | 4 *M X N* |

**Table 3. Experimental comparisons of the proposed method with existing methods.**

| Method/Refs. | PSNR (dB) | Reconstruct the Secret Image without Loss | Reconstruct the Cover Image without Loss | Embedding Capacity |
|---|---|---|---|---|
| Thien *et al*. 2002 [22] | 32 | Yes | No | - |
| Lin cc *et al*. 2004 [23] | 40 | Yes | Yes | *M X N* |
| Wu *et al*. 2004 [24] | 34 | No | No | - |
| Yang *et al*. 2007 [25] | 40 | Yes | No | *M X N/4* |
| Chang cc *et al*. 2008 [26] | 40.66 | Yes | No | *M X N* |
| Zhao *et al*. 2009 [27] | 39 | Yes | No | *M X N/4* |
| Lin py *et al*. 2009 [28] | 41 | Yes | No | *M X N/2* |
| Pei *et al*. 2010 [29] | 42 | Yes | Yes | *M X N/2* |
| Yen-po *et al*. 2012 [30] | 44 | Yes | Yes | *M X N/2* |
| Xintao Duan *et al*. 2020 [2] | 43.13 | Yes | Yes | *M X N/2* |
| Ghazanfar Farooq Siddiqui *et al*. 2020 [15] | 45.09 | Yes | Yes | *2 x (M X N)* |
| Xinliang Bi *et al*. 2021 [3] | 40.66 | Yes | Yes | *M X N/2* |
| J. Xie, H. *et al*. 2022 [31] | 43.01 | No | No | *M X N* |
| W. El-Shafai *et al*. 2023 [32] | 38.63 | Yes | No | *M X N* |
| Proposed method | 45.5 | Yes | Yes | *4 x (M X N)* |

Comparisons of the proposed method with existing methods are presented in Table **3**. All the existing methods embed only one secret image into one cover image and achieve an average PSNR of upto 44dB. In the Proposed method four secret images are embedded into a single cover image and achieve a PSNR of 45.5dB in set 1 and 47.20dB in set 2. These results shows that the proposed work is superior compared to the existing methods.

## CONCLUSION

A patient's report plays an important role in their medical treatment. Particularly in telemedicine, the safe transmission of patient reports without any misplacement or loss of information is necessary. The proposed method embeds four reports of a patient in his/her photo and transmits it to the destination safely with a quality of 45.5 dB for set 1 and 47.20 dB for set 2. Compared with the existing methods, the proposed method has high embedding capacity with good quality. While other methods can only embed one image inside another image, the proposed work uses a revolutionary technique where four secret images are placed at once. The results show that when more than four hidden images are incorporated into a single cover image, the quality of the stego image declines, and this is a challenge for the proposed method in this study.

## LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| **CT scan** | = | Computed Tomography scan |
| **DES** | = | Data Encryption Standard |
| **AES** | = | Advanced Encryption Standard |
| **dB** | = | decibels |
| **2D-LAIC** | = | 2 Dimensional Logistic map And Infinite Collapse |
| **MRI** | = | Magnetic Resonance Imaging |
| **PSNR** | = | Peak Signal to Noise Ratio |
| **SC** | = | Structural Content |

## ETHICAL STATEMENT

In this work, no research was done on the human body directly, and this work does not affect human health. The medical reports from the authorized personnel were transferred to another place (Telemedicine) using Steganography techniques for protection from unauthorized persons and cybercrimes only. Nowadays, due to an increase in cybercrimes and fake documentation, a novel model was proposed to prevent these types of crimes with this research and hence, the right treatment was provided to the patient. Therefore, no experimentation was performed on a Humans and hence, the ethical committee report is not applicable to this research work.

## CONSENT FOR PUBLICATION

All the medical reports of the patient are hidden in the face of the patient only to identify the right person easily for better treatment. Here, we use benchmark images (faces) such as a patient's face.

## AVAILABILITY OF DATA AND MATERIALS

All the images used in this work are benchmark images downloaded from Image Databases (imageprocessingplace.com)

## FUNDING

None.

## CONFLICT OF INTEREST

The authors declare no conflicts of interest, financial or otherwise.

## ACKNOWLEDGEMENTS

Declared none.

## REFERENCES

[1] Wei W, Wen Y. A novel image steganography using wavelet contrast and modulus operation. Lect Notes Comput Sci 2016; 9772: 418-25. [http://dx.doi.org/10.1007/978-3-319-42294-7_37]

[2] Duan X, Guo D, Liu N. A new high capacity image steganography method combined with image elipitic curve cryptography and deep neural network. IEEE Access 2020; 8

[3] Bi Xinliang, Yang Xiaoyuan, Wang Chao, Liu Jia. High capacity image steganography algorithm based on image style transfer. Secur Commun Networks 2021; 1: 1-14.

[4] Lakshmi SB. Image steganography based on SVD and DWT techniques. J Discrete Math Sci Cryptograph 2020; 23(3): 779-86. [http://dx.doi.org/10.1080/09720529.2019.1698801]

[5] Lakshmi SB, Srinivas KS, Chandra MB. Steganography based image sharing with reversibility. J Discrete Math Sci Cryptograph 2016; 19(1): 67-80. [http://dx.doi.org/10.1080/09720529.2015.1086109]

[6] Lakshmi SB, Srinivas KS, Chandra MB. Identification of cheaters in elections using steganography. J Inform Optimiz Sci 2016; 37(2): 271-8. [http://dx.doi.org/10.1080/02522667.2015.1130891]

[7] Prasanth VS. Adaptive temper detection watermarking scheme for medical images in transform domain. Multimed Tools Appl 2022; 81(8): 11605-19.

[8] Prasanth VS. Adaptive medical image watermarking system for E-Health care applications. S N Comp Sci 2022; 3(2): 107-10.

[9] Rayi S. EPNN based high secure intensive hidden digital wateemark application in telemedicine. Adv Model Analy 2019; 56(1): 22-5.

[10] Lakshmi SB, Srinivas KS, Chandra MB. Advances in modelling and analysis Steganography based information security with high embedding capacity. National conference on Recent Advances in Electronics & Computer Engineering.

[11] Usha RK, Aruna PP. Identification of attention-deficit-hyperactivity disorder subtypes based on structural mri grey matter volume and phenotypic information. J Curr Med Imag 2023; 19(14): 1656-64.

[12] Wang J, Zhao X, Zhang W. Pituitary adenoma with multiple calcifications in a child: A rare case presentation. J Curr Med Imag 2023; 19(14): 1685-8.

[13] Su X, Wang S. Is magnetic resonance imaging (mri) still a gold standard to detect breast cancer: A meta-analysis. J Curr Med Imag 2023; 19(14): 1643-55.

[14] Mohsin H. PSO–Blockchain-based image steganography: Towards a new method to secure updating and sharing COVID-19 data in decentralized hospitals intelligence architecture. Multimedia Tools and Applications . Berlin: Springer 2020; pp. 14137-61.

[15] Siddiqui GF, Iqbal MZ, Saleem K. A dynamic three-bit image steganography algorithm for medical and e-healthcare systems. IEEE 2020; 181893-903.

[16] Sahu AK, Sahu M. Digital image steganography and steganalysis: A journey of the past three decades. Open Comp Sci 2020; 10: 296-342.

[17] Ogundokun RO, Abikoye OC. A safe and secured medical textual information using an improved LSB image steganography. Int J Dig Multimed Broadcast 2021; 2021: 8827055.

[18] Subramanian N, Elharrouss O, Al-Maadeed S, Bouridane A. Image steganography: A review of the recent advances. IEEE Access 2021; 9: 23409-23. [http://dx.doi.org/10.1109/ACCESS.2021.3053998]

[19] Fridrich J, Kodovsky J. Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security. 7(3): 868-82.

[20] Zhou Z. Coverless image steganography using partial-duplicate image retrieval. Soft Computing 2019; 23: 4927-38.

[21] Shamir A. How to share a secret. Commun ACM 1979; 22(11): 612-3. [http://dx.doi.org/10.1145/359168.359176]

[22] Thien CC, Lin JC. Secret image sharing. Comput Graph 2002; 26(5): 765-70. [http://dx.doi.org/10.1016/S0097-8493(02)00131-0]

[23] Lin CC, Tsai WH. Secret image sharing with steganography and authentication. J Syst Softw 2004; 73(3): 405-14. [http://dx.doi.org/10.1016/S0164-1212(03)00239-5]

[24] Wu YS, Thien CC, Lin JC. Sharing and hiding secret images with size constraint. Pattern Recognit 2004; 37(7): 1377-85. [http://dx.doi.org/10.1016/j.patcog.2004.01.002]

[25] Yang CN, Chen T-S, Yu KH, Wang CC. Improvements of image sharing with steganography and authentication. J Syst Softw 2007; 80(7): 1070-6. [http://dx.doi.org/10.1016/j.jss.2006.11.022]

[26] Chang CC, Hsieh YP, Lin C-H. Sharing secrets in stego images with authentication. Pattern Recognit 2008; 41(10): 3130-7. [http://dx.doi.org/10.1016/j.patcog.2008.04.006]

[27] Zhao R, Zhao J, Dai F, Zhao F. A new image secret sharing scheme to identify cheaters. Comput Stand Interfaces 2009; 31(1): 252-7. [http://dx.doi.org/10.1016/j.csi.2007.10.012]

[28] Lin PY, Lee JS, Chang CC. Distortion-free secret image sharing mechanism using modulus operator. Patt Recognit 2009; 42(5): 886-95. [http://dx.doi.org/10.1016/j.patcog.2008.09.014]

[29] Pei Y. Invertible secret image sharing with steganography. Patt Recognit Lett 2010; 31: 1887-93. [http://dx.doi.org/10.1016/j.patrec.2010.01.019]

[30] Lee Y-P, Lee J-C, Chen W-K, Chang K-C, Su I-J, Chang C-P. High-payload image hiding with quality recovery using tri-way pixel-value differencing. Inf Sci 2012; 191: 214-25. [http://dx.doi.org/10.1016/j.ins.2012.01.002]

[31] Xie J, Wang H, Wu D. Adaptive image steganography using fuzzy enhancement and grey wolf optimizer. IEEE Trans Fuzzy Syst 2022; 30(11): 4953-64. [http://dx.doi.org/10.1109/TFUZZ.2022.3164791]

[32] El-Shafai W, Abd El-Hameed HA, El-Hag NA, Khalaf AAM, Soliman NF. Proposed privacy preservation technique for color medical images. Intell Automat Soft Comput 2023; 36(1): 719-32. [http://dx.doi.org/10.32604/iasc.2023.031079]

[33] Gao S, Wu R, Wang X, Liu J, Li Q, Tang X. EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory. Inf Sci 2023; 621: 766-81. [http://dx.doi.org/10.1016/j.ins.2022.11.121]

[34] Gao S, Wu R, Wang X, *et al.* A 3D model encryption scheme based on a cascaded chaotic system. Sign Process 2023; 202: 108745. [http://dx.doi.org/10.1016/j.sigpro.2022.108745]