Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-B, pp. 775–784
DOI : 10.47974/JDMSC-1954

Enhanced security of EMI using an edge-based steganography with four-layered cryptography

Divya Sharma [†]
Chander Prabha *
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab
India

Ankur Goyal [§]
Department of Computer Science and Engineering
Symbiosis Institute of Technology
Symbiosis International Deemed University
Pune
Maharashtra
India

Meena Malik [‡]
Raman Kumar [@]
University Centre for Research & Development
Chandigarh University, Mohali
Punjab
India

Abstract

Security and privacy of EMI images while being transmitted over an insecure medium or when stored on third-party storage. In this paper, an enhancement of the EBS steganography with four layers of cryptography has been implemented to ensure the secrecy and privacy of a large and diverse data set of X-ray images available in JPEG format. The major objective of this research is to secure a large and diverse data set of EMI into a cover image without degrading the EMI quality as these can be used for future medical referencing. A data set of

[†] *E-mail:* **divya009sharma@gmail.com**
* *E-mail:* **prabhanice@gmail.com (Corresponding Author)**
[§] *E-mail:* **ankur_gg5781@yahoo.co.in**
[‡] *E-mail:* **meenamlk@gmail.com**
[@] *E-mail:* **ramankakkar@gmail.com**

© Taru Publications

5856 varying dimensioned and sizes X-ray images is hidden one at a time around the Edge of the normalized cover image Lena using edge-based steganography. The algorithms with various performance evaluation tests such as Computational Time is 0.135217 seconds for creating one stego-crypto-image, Peak Signal to Noise Ratio (PSNR) is 74.55838892 dB, Mean Square Error (MSE) is 3.50075E-08, Bit Error Rate (BER) is 2.25493E-05, SSIM is 0.46291047, etc. The results obtained showed less computational time, while quality tests such as BER, and SSIM ensure that the image extracted is the same as the original hence better performance and reduction in computational time.

Subject Classification: *00A71.*

Keywords: *Real-time applications (RTA), Electronic medical image (EMI), Secrecy, Privacy, Computational time.*

1. Introduction

EMI is mostly communicated on an insecure medium or stored on third-party storage renders them vulnerable to attackers, or hackers [1, 2]. The security and privacy of EMI need to be enhanced [3,4]. EMI such as X-Ray [5,6], MRI, CT-Scan, [7,8], etc. EMI are valued and crucial for patients as they can be used for future diagnosis. EMI is generally stored by hospitals, patients, labs, etc. either locally or on a cloud. The recent year has witnessed a mass increase in hacks and threats to EMI [9] thus is a rise in concern.

1.1 *Problem Statement*

The previous researchers implemented various data hiding techniques for enhancing the security of EMI but their validity has not been proved as they were not applied with even standard performance evaluation tests such as PSNR, MSE, R, etc. The researchers in [2,10–12] used conventional data hiding techniques such as Least Significant Bit (LSB), Advanced Encryption Standard (AES), Discreet Wavelet Transform (DWT), Rivest Shamir Adleman (RSA), Exploiting Modification Direction (EMD), Arithmetic Coding (AC) with Most Significant Bit (MSB), Blowfish, Data Encryption Standard (DES), 3DES or triple-DES. These are well known to all, easy to detect, and are vulnerable to attacks, and computationally complex to implement [13,14]. They lack to carry maximum covert information and often suffer from the same limitations as the conventional approach [15].

1.2 *Research Contributions*

The major contribution of this research work has been summarized below:

- Implementation an enhanced EBS with four layer cryptography on 5856 X-Ray images sized 1.6 GB which are large, complex and vary in dimensions. Performance testing with PSNR, MSE, SSIM, R, etc.

The rest of this article is organized in the following sections: Section 2 is a background study tabulates the latest, relevant, and current research work in EMI. Section 3, discusses the enhanced EBS steganography with four-layer cryptography. Section 4 discusses the results achieved from performance evaluation tests. Finally, the conclusion and future scope of this research work.

2. Literature Review

The research work proposed in this research focuses on lesser computational time steganography which is suitable for real-time applications. In Table 1, it can be seen that few research works such as [15,16,18,20] focused on hiding alphabets in ASCII format in an EMI. ASCII numbers are hidden in a cover image using an LSB or MSB algorithm. Here a limited number of alphabets are hidden. This research work hides a larger and varying data set of 5856 images. The amount of data hidden is less compared to the amount that can be hidden. Thus, the payload capacity is not fully utilized. While this research work hides a maximum payload of 2414342 Bytes. Most of the previous research works are not focused on providing security to EMI accessed through real-time applications [12]. While researchers in [21,24, 25] secured medical data such that it can be implemented for RTA.

Table 1

Study Based on Cover and Secret Message Types, Sizes, and Dimensions.

Cited as	Cover Images (CI)	CI dimensions	Hidden message	Message size
[20]	50 ECG records (20 mitdb, 30 ptbdb) 90 records European ST-T database, tested 222 records were 130 from ptbdb database, 40 and 52 from mitdb and European ST-T database	-	ASCII equivalent of patient's confidential information	-

Contd...

[16]	Lena, Pepper	512×512	Text	-
[18]	Lena, Baboon, Airplane F16, Tiffany, Pepper	512×512	26 Characters	52,400 Bytes
[19]	Grey and colour medical images	Grey 512× 512, color 256× 256	Secret text 8 and 192 digits	-
[10]	10 MR Images	256×256	10 Grey scale images	165×165
[11]	10 MRI and CT images	512×512	1000 to 20000 characters	-
[14]	Lena, Pepper, Baboon	512×512	Secret image	-
[15]	2,00,000 CelebFaces grey images	70 ×109	Text	37 Bytes
[23]	Medical images (CT, MRI, US, X-Ray)	480 × 480	Patient info, doctor comments, logo	-
[22]	Seven medical images from the SIPI dataset	512×512	Patients report	-

Few research works [10] have hidden smaller dimensions of images 165 × 165 into the cover image. While [11,15,18,19,20,23] have converted text into ASCII and then hidden them into an image.

3. Proposed Method

In this paper, the authors have implemented a hybrid combination of steganography and cryptography. Firstly, performing edge-based steganography (EBS) which hides the normalized cover image Lena (NL) with one of the X-Ray images from a data set of 5856 images one at a time. Then save them with the same name as the X-ray image. Secondly, the stego-image generated above is applied with four layers of cryptography. The computational time for encryption and decryption is calculated. Finally, a common performance evaluation test is performed on the stego-crypto-image to ensure the validity of the proposed algorithm.

3.1 *Edge Based Steganography (EBS)*

EBS method works in the background region of the cover Lena. Here Lena's image is converted as per Figure 1 noise is added around Lena. This will be separated into RGB components. Then one secret X-ray image will

be hidden around the edges of the RGB components separately. This will generate a stego image.



Figure 1

Normalized cover image Lena (NL)

3.2 *Four Layers of Cryptography*

The stego-image generated above will be applied with four layers of cryptography. Firstly, initial permutation here a random table of the same size as one of the components of the NL will be constructed then it will be applied with randomized values that will be used as substitution values for the stego-image. Secondly, Circular right shift (CRC) where each component of the stego-image will be divided into two halves say left half (LH) and right half (RH). Both LH and RH will be applied with a circular right shift by four columns. Here four columns from the front are moved back circularly for both LH and RH for all RGB components. Thirdly, the LH is XORed with the RH which will generate the new LH while the old LH will become the new RH. Fourth, both the new LH and new RH are combined into one image. Here the even columns are interchanged with the odd columns. The resulting image is a stego-crypto-image will be used for transmission and storage on third-party storage.

Algorithm: Enhancement of EBS steganography with four layers of cryptography.

Step1: Load the Normalized cover image Lena. Initialize count to 0.

Step 2: Detect the edges around Lena in the normalized image from step 1.

Step 3: Load one X-ray image from a data set of 5856 images. Increment count by 1.

Step 4: Hide the X-ray image in the edges found in step 2.

Step 5: Check if count is 5856 (or total length) else go to step 3.

Step 6: Stop.

4. Results

The results for the proposed method were achieved in MATLAB on data set discussed in this section. The normalized cover image is dimensions 1080 × 1080 size is 720 KB. The varying-sized X-ray images belong to 5856 X-ray images downloaded from Mendeley (Kermany, 2018 https://doi.org/10.17632/rscbjbr9sj.2).

Computation time is measured in terms of Encryption and decryption time. Encryption time is the time taken to secure the EMI after creation on the storage or for transmission. While decryption time is the time taken to extract back the X-ray image. The total encryption time is 18.2153 minutes while decryption time is 4.60174 Hrs.

4.1 *Performance Evaluation Test*

To prove the validity of the proposed enhanced EBS with four layer the following test were performed. The values achieved for the test have been tabulated in Table 2 below.

Mean Square Error(MSE) $MSE = \sum_{i=1}^{m}\sum_{j=1}^{n} \frac{I(i,j)-SI(i,j)}{m\times n}$ (1)	Peak Signal to Noise Ratio (PSNR) $PSNR = 10\log_{10}\frac{\max^2}{MSE}$ (2)
Root Mean Square Error (RMSE) $RMSE = \sqrt{\frac{1}{L}\sum_{i=1}^{L}(c_1(i)-c_2(i))^2}$ (3)	Structural Similarity Index Metrics (SSIM) $SSIM(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2\mu_y^2+c_2)(\sigma_x^2+\sigma_y^2+c_2)}$ (4)
Embedding Ratio (ER) $ER = \frac{p}{M\times N}$ (5)	Pearson Coefficient (R) $R(Ac,\mathrm{Re}) = \frac{Cov(Ac,\mathrm{Re})}{\sigma_{Ac}\sigma_{\mathrm{Re}}}$ (6)
Coeffecient of Variation (CV) $std = \sqrt{\frac{\Sigma(Ac-\mu)}{N}}$ (7) $mean = \frac{\Sigma Ac}{N}$ (8) $CV = \frac{std(img)}{mean(img)}$ (9)	Number of Pixel Changing Rate (NPCR) $NPCR = \frac{\Sigma_{i,j}D(i,j)}{M\times N}\times 100$ (10) $D(i,j) = \begin{cases} 0 & c_1(i,j)=c_2(i,j) \\ 1 & \text{otherwise} \end{cases}$ (11)
	Edge Differential Ratio (EDR) $EDR = \frac{\Sigma_{i,j=1}^{N}\lvert c_1(i,j)-c_2(i,j)\rvert}{\Sigma_{i,j=1}^{N}\lvert c_1(i,j)+c_2(i,j)\rvert}$ (13)

Contd...

Unified Average Changing Intensity (UACI) $UACI = \frac{1}{M \times N}\left(\sum_{i,j}\frac{\lvert c_1(i,j) - c_2(i,j)\rvert}{255}\right) \times 100$ (12)	
Entropy (E) $E = -\sum_{i=1}^{N} P(c_i)\ \log_2 P(c_i)$ (14)	Kullback–Leibler Divergence (KLD) $KLD = \int c_2(x)\ \log \frac{c_1(x)}{c_2(x)}$ (15)
Bit Error Rate (BER) $BER = \frac{\Sigma_i\, c_1 \otimes c_2}{L}$ (16)	Mean Absolute Percentage Error (MAPE) $MAPE = \frac{1}{L}\sum_{i=1}^{L}\left(\frac{\lvert c_1(i) - c_2(i)\rvert}{c_1(i)}\right) 100\ \%$ (17)
Signal to Noise Ratio (SNR) $SNR = 10\ \log_{10} \frac{\sum_{i=1}^{L}(c_1(i) - c_2(i))^2}{\sum_{i=1}^{L}(c_1(i))^2}$ (18)	Percentage Residual Difference (PRD) $PRD = \sqrt{\frac{\sum_{i=1}^{N}(c_1(i) - c_2(i))^2}{\sum_{i=1}^{L}(c_1(i))^2}}.100\%$ (19)

5. Conclusion

EMI while being transmitted over an insecure medium or stored on unsecure third-party storage should be secured. As the number of EMI has increased with the increase in population. Thus, the security and privacy of EMI needs to be ensured. To secure large amount of EMI of varying dimensions and properties the authors have proposed an enhancement of EBS steganography with four layers of cryptography. Which has proved to be light as the computational time taken to implement is less. The performance evaluation test prove that the proposed method has enhanced secrecy and privacy while dealing with larger and diverse data set of EMI. In EMI the secret X-ray image is embedded in the region of no interest (RONI). The proposed method has achieved a PSNR of 74.558 Db, SSIM is 0.999 these value show that the X-ray image after decryption and extraction from the cover signal retains images quality. In future, a machine learning algorithm could be developed to detect edges in any cover image which can then be used for hiding X-ray images.

Table 2

Performance test values achieved for the proposed methods.

Performance Measure	Minimum Value	Maximum Value
MAE	1.68014E-06	0.040669068

Contd...

PRD	0.000109967	7.462821777
CR	0.995818345	8.834928525
UACI	6.5888E-09	0.000159487
NPCR	0.002254929	95.5854502
E	5.99882228	7.839790659
MSE	3.50075E-08	0.003261895
PSNR	24.86530032	74.55838892
SSIM	0.46291047	0.999981058
ER	100	100
CV	894.5573283	690610.063
R	0.97765712	0.999999371
SNR	-0.016539737	0.049219314
RMSE	0.000187103	0.057113001
BER	2.25493E-05	0.955854502
KL-D	-9.58722E-06	0.000248958

References

[1] Abdul W. Security of medical images over insecure communication channels using zero-steganography. *Int J Distrib Sens Netw*; 18 (2022). https://doi.org/10.1177/15501477211006347.

[2] Kumar M, Soni A, Shekhawat ARS, Rawat A. Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique. Proceedings of the 2nd International Conference on Artificial Intelligence and Smart Energy, ICAIS 2022, Institute of Electrical and Electronics Engineers Inc.; p. 1453–7 (2022). https://doi.org/10.1109/ICAIS53314.2022.9742942.

[3] Marichamy VS, Natarajan V. Blockchain based Securing Medical Records in Big Data Analytics. *Data Knowl Eng*; 144 (2023). https://doi.org/10.1016/j.datak.2022.102122.

[4] Daraghmeh R, Brown R. A Big Data Maturity Model for Electronic Health Records in Hospitals. 2021 International Conference on Information Technology, ICIT 2021 - Proceedings, Institute of Electrical and Electronics Engineers Inc.; p. 826–33 (2021). https://doi.org/10.1109/ICIT52682.2021.9491781.

[5] Malhotra P, Gupta S, Koundal D, Zaguia A, Kaur M, Lee HN. Deep Learning-Based Computer-Aided Pneumothorax Detection Using

Chest X-ray Images. *Sensors*; 22 (2022). https://doi.org/10.3390/s22062278.

[6] Aggarwal S, Gupta S, Alhudhaif A, Koundal D, Gupta R, Polat K. Automated COVID-19 detection in chest X-ray images using fine-tuned deep learning architectures. *Expert Syst*; 39 (2022). https://doi.org/10.1111/exsy.12749.

[7] Al Hamid HA, Rahman SMM, Shamim Hossain M, Almogren A, Alamri A. A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography. *IEEE Access*; 5 : 22313–28 (2017). https://doi.org/10.1109/ACCESS.2017.2757844.

[8] Bansal B, Jenipher VN, Jain R, Dilip R, Kumbhkar M, Pramanik S, et al. Big Data Architecture for Network Security. Cyber Security and Network Security, Wiley; p. 233–67 (2022). https://doi.org/10.1002/9781119812555.ch11.

[9] Said O. LBSS: A Lightweight Blockchain-Based Security Scheme for IoT-Enabled Healthcare Environment. *Sensors*; 22 (2022). https://doi.org/10.3390/s22207948.

[10] Chowdhuri P, Pal P, Si T. A novel steganographic technique for medical image using SVM and IWT. Multimed Tools Appl; 82 : 20497–516 (2023). https://doi.org/10.1007/s11042-022-14301-0.

[11] Ahmad MA, Elloumi M, Samak AH, Al-Sharafi AM, Alqazzaz A, Kaid MA, et al. Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images. *Alexandria Engineering Journal*; 61 : 10577–92 (2022). https://doi.org/10.1016/j.aej.2022.03.056.

[12] Alkhliwi S. Encryption-based Image Steganography Technique for Secure Medical Image Transmission During the COVID-19 Pandemic. *IJCSNS International Journal of Computer Science and Network Security*; 21 : 83 (2021). https://doi.org/10.22937/IJCSNS.2021.21.3.12.

[13] Sharma D, Kawatra R. Security Techniques Implementation on Big Data Using Steganography and Cryptography. Lecture Notes in Networks and Systems, vol. 517, Springer Science and Business Media Deutschland GmbH; p. 279–302 (2023). https://doi.org/10.1007/978-981-19-5224-1_30.

[14] Khan A, Sarfaraz A. FFT-ETM based distortion less and high payload image steganography. *Multimed Tools Appl*; 78 : 25999–6022 (2019). https://doi.org/10.1007/s11042-019-7664-7.

[15] Hachaj T, Koptyra K, Ogiela MR. Eigenfaces-based steganography. Entropy; 23 : 1–24 (2021). https://doi.org/10.3390/e23030273.

[16] Jabbar MS, Issa SS. A crypto-steganography healthcare management: Towards a secure communication channel for data COVID-19 updating. *Indonesian Journal of Electrical Engineering and Computer Science*; 29 : 1102–12 (2023). https://doi.org/10.11591/ijeecs.v29.i2.pp1102-1112.

[17] Sharma S, Malik M, Prabha C, Al-Rasheed A, Alduailij M, Almakdi S. Robust Image Watermarking Using LWT and Stochastic Gradient Firefly Algorithm. Computers, Materials and Continua; 75: 393–407 (2023). https://doi.org/10.32604/cmc.2023.033536.

[18] Malik, M.; Sharma, S.; Uddin, M.; Chen, C.-L.; Wu, C.-M.; Soni, P.; Chaudhary, S. Waste Classification for Sustainable Development Using Image Recognition with Deep Learning Neural Network Models. *Sustainability*, 14, 7222 (2022). https://doi.org/10.3390/su14127222.

[19] Aleisa HN. Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things. J Healthc Eng 2022 (2022). https://doi.org/10.1155/2022/7528583.

[20] Konyar MZ, Öztürk S. Reed Solomon coding-based medical image data hiding method against salt and pepper noise. Symmetry (Basel); 12 (2020). https://doi.org/10.3390/SYM12060899.

[21] Georgieva-Tsaneva G, Bogdanova G, Gospodinova E. Mathematically Based Assessment of the Accuracy of Protection of Cardiac Data Realized with the Help of Cryptography and Steganography. Mathematics; 10 (2022). https://doi.org/10.3390/math10030390.

[22] Banerjee S, Singh GK. A new approach of ECG steganography and prediction using deep learning. Biomed Signal Process Control; 64 (2021). https://doi.org/10.1016/j.bspc.2020.102151.

[23] Li C, Dong M, Li J, Xu G, Chen XB, Liu W, et al. Efficient Medical Big Data Management With Keyword-Searchable Encryption in Healthchain. *IEEE Syst J*; 16 : 5521–32 (2022). https://doi.org/10.1109/JSYST.2022.3173538.

[24] S. Sharma, "Image Watermarking in Frequency Domain using Hu's Invariant Moments and Firefly Algorithm," no. April, pp. 1–15, (2022) doi: 10.5815/ijigsp.2022.02.01.

[25] Lilhore, U. K., Poongodi, M., Kaur, A., Simaiya, S., Algarni, A. D., Elmannai, H., … Hamdi, M. Hybrid model for detection of cervical cancer using causal analysis and machine learning techniques. *Computational and Mathematical Methods in Medicine*, 1–17 (2022). doi:10.1155/2022/4688327.