Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 3, pp. 767–777
DOI : 10.47974/JDMSC-1753

Steganlysis on data embedded medical image

J. Stella *
P. Karthikeyan †
Department of Information and Communication Engineering
Velammal College of Engineering and Technology
Madurai
Tamil Nadu
India

S. J. Thomas Schwarz §
Department of Computer Science
Marquette University
U.S.A.

S. J. John Rose ‡
Department of IT
Xavier Institute of Engineering
Mumbai
India

Abstract

Cybercrime around the world is increasing day by day abruptly. Stego attack is one of the popular methods of transferring the message secretly through the cover medium. Most of the sources are using this process for covert communication. The paper discusses the importance and analysis of data hiding theft and covert communication process through steganalysis where it talks about the "covered writing" in such a way that the mutation of an image is not discernible. The main motive of this paper is to attack and analyze the Digital Imaging and Communications in Medicine (DICOM) file format. The file format DICOM discussed in this research is mostly supported in the medical field. CT Scans and MRI Scans are widely used in hospitals to view the human body. The random pixels is chosen to hide the text on the DICOM formats and the performance is measured using different metrics.

* *E-mail:* **jstella.js01@gmail.com (Corresponding Author)**
† *E-mail:* **kpkarthi2001@gmail.com [0000-0001-8515-7370]**
§ *E-mail:* **tschwarzsj@gmail.com [0000-0003-4433-3360]**
‡ *E-mail:* **johnrose@xavier.ac.in [0000-0001-8487-5370]**

The proposed approach produces 100% recovery of the hidden text inside an image with maximum payload capacity.

Subject Classification: *94A13.*

Keywords: *Steganography, Steganalysis, Least significant bits, Image formats.*

1. Introduction

Data Security is an essential need in the preset digital world. All the age groups from age 10 onwards use online sources for other purposes. More the online subscriptions more the security measures should take place. Steganalysis is the method that identifies the hidden message behind the cover medium which is a stego image. There are lot more techniques available these days to hide the secret message. Stalking through internet communication and recovering the messages being transferred between channels is miserable work for cyberfraud.

Earlier steganography was started for transferring confidential information inside a cover medium but soon after it converted to covert communication for terrorism and cyber-attack to damage the country's economy.

The art of digital forensics consists in collecting, storing, and analyzing digital evidence. Evidence such as steganographic images collected by forensic investi- gators appears normal to the human eye. Through the web analysis process, researchers learned hidden context. There are two different types of web analytics approaches passive and active [12]. While the passive type classifies the stego image and identifies the algorithm, the active steganalysis additionally indicates the length of the message embedded in it.

2. Related Work

In [19] JPEG file format is used as a cover medium for secure communication. In this paper, the LSB of a cover image is manipulated with secret image data and encrypted using the Viegner Cipher. The paper [9] states about finding the effective stego key for LSB Steganography on JPEG decompressed images using a random LSB steganographic model. In this technique, a random sequence and random embedding positions are generated by a pseudo-random number generator for carrying the stego key. The number of message bits to be embedded is calculated and random numbers are generated using a Logistic map [17] multiplied by

10 to make an integer thus the secret encrypted message is embedded in least significant bit. DFT algorithm considers the sine and cosine waves and it provides real and imaginary parts of values. In [6], secret messages are embedded in the spatial domain such as DCT coefficients for both JPEG and GIF file formats. Utilization of histogram to conceal the data is proposed [8] in the medical images showing the PSNR value is less than 70dB. The effective denoise of an image using Digital wavelet Transform is applied [10] to reduce the noise in the gray scale images and the PSNR values shows the reduction of noise with sharp edges.

Integer Haar Wavelet transform is proposed in the paper [15] to suppress the secret messages into the different categories of frequency bands such as HH,LH,HL and LL. The embedded secret bits inside the vector coefficient produces the average PSNR of 54dB with the message size of 67.7kB. The researcher in [14] stretch the image horizontally based on the message embedding size. A 3D Chebyshev polynomials and 3D logistic maps, a 1st order differential equations[5] utilized for hiding the secret messages. The cover images are Leena [14],[5], Baboon, Peppers and Barbara. Deep Neural Network algorithms such as Ensem- ble Classifiers [13] VGG and Xception[1] algorithms are applied to the stego image to yield the embedded secret message. This model is applied on the Ima- geNet, COCO, MNIST, and CelebA such as data sets of JPEG, TIFF, and PNG image file formats. The outcome of these algorithms shows 95 - 98% of accuracy in detecting the hidden message. The convolution based neural network search method is developed by the researchers [17] which captures the statistical features of images of an digital image. In this model they proposed two steganographic algorithm such as Wavelet obtained weights (WOW) and Spatial universal wavelet relative distortion (SUNIWARD).

3. Design Methodology

The method of reconstructing and extracting the hidden message from the original message is known as Steganalysis. Figure 1 shows the Steganography and steganalysis of an image.

3.1 *Basic Terminology*

Steganography: Steganography is the process of concealing a secret message (M) in mediums including images, audio, video or text. The

proposed model uses cover media such as DICOM images. Different sized payload messages are embedded in the cover holder.

Steganalysis: The flip side of steganography is that retrieving hidden messages from stego images is known as steganalysis. From the image, embedded bits are retrieved to separate the embedded message as well as the cover image.

3.2 *Image File Format*

This paper analyzes the Image file format Digital Imaging and Communications in Medicine (DICOM)

Digital Imaging and Communications in Medicine (DICOM): The DICOM image is a standard for storing and retrieving details of a human body in terms of medical imaging. It supports binary lossless information in medical imaging. The DICOM Standard is the central method in the development of modern radio graphic imaging where it standards for imaging modalities such as computed tomography (CT), X-ray, magnetic resonance imaging (MRI), ultrasound, and radiation therapy. The proposed system utilizes Computed tomography (CT) images for steganography and steganalysis

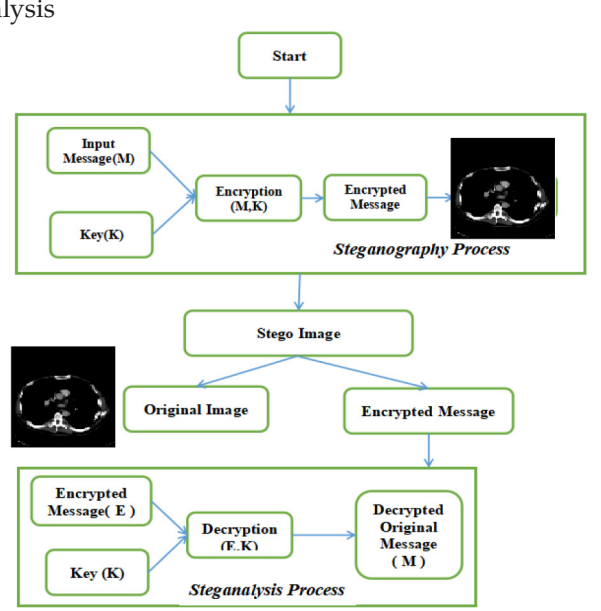

Figure 1

Flow Diagram of Steganography and Steganalysis

4. Implementation Strategies

The proposed system utilized the cover medium as an image in DICOM file format and it is considered for analysis. Since it is a lossless binary image the binary information of the image is considered for embedding data into the image.

4.1 *Embedding a Secret Message*

Different payload size of data is embedded into the DICOM images in the pro- posed system and analyzed the sensitivity of the image. The image utilized in the proposed system is resized into 516 KB (512 x 512) sizes as a cover medium and the text message needed to hide inside an image is taken into consideration and encrypted using AES 256 algorithm. The Encrypted text is converted into ASCII Characters and to equivalent binary numbers (10110101), the last bit 1 is the least significant bit[8] of the binary number will be embedded into the pixels of DICOM images one by one.

Algorithm 1 Phase1: Steganography on DICOM image format

Require: 1. Select the Input: CI = Cover Image, M = Input Message and E = Encrypted Message

2. Compute the shape of the cover image.
3. Calculate the maximum payload capacity, (width * height * channel)/8
4. Convert secret message to Encrypted Message, Message → Encrypted message → ASCII → Binary

Ensure: for letters in message

if Key_size == 256 **then**

Compute, iv = generate random values of block_size = 256
encrypted message = AES.new(key,AES.MODE_CBC, iv)
return iv + cipher.encrypt(original message)

end if

5. Choosing random pixels from the image and the pixel value is converted to binary

Ensure: for values in pixels

if msgindex < len(msg) **then**

for each pixel of Pi
embed message bit
msgindex+1

end if

6. Construct as an image

Considering an example, the ASCII value of character a = 65 and the equivalent binary number for this character is 01100001. Embedding the secret message into the Least Significant bit of the DICOM image is provided in the diagram below, The Encrypted Message Ei of 8 bits are one by one embedded into the binary pixels of an image randomly. The first bit of the encrypted message will be equal to the Least Significant bit of any of the Pixels. First Bit of Ei = Cover Medium of Pi. Similarly, the whole message is embedded in the fashion with incrementing Ei + 1 on the cover image of Pixels Pi + 1 ….. where n is the number of bits, Ei is the encrypted input message and Pi is the pixels in the message.

4.2 *Extracting the Embedded Message*

Extracting secret messages from stego images is called steganalysis. The least significant bits of the pixels are taken into consideration and recovered one by one to form completed binary values (bi, bi+1, …bi+n). The extracted binary values are reconstructed one by one to form ASCII values. From the ASCII values, the hidden messages and cover images are separated. The hidden message extracted is encrypted so it is decrypted using AES 256 algorithm to recover the original text. Different payload sizes are embedded and extracted from the cover image in the proposed system. The Figure 2 shows the embedding and extracting phase of a sample binary image.

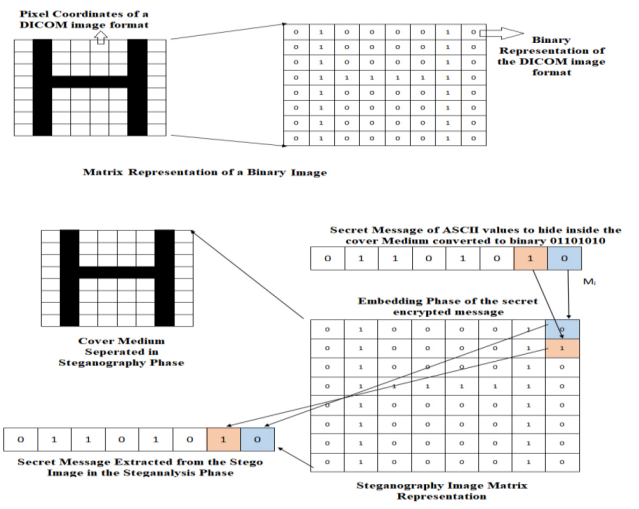

Figure 2

Steganography and Steganlysis on DICOM image

5. Results and Analysis

Original Image and the Stego Image is shown in the Figure 3 and Figure 4 below and the performance of the algorithms such as Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR) and Root Mean Square Error (RMSE) is measured.

5.1 *Evaluation Metrics*

Mean Square Error (MSE): Original image and the stego image is compared pixel by pixel in order to identify the difference between them [14] and the equation (1) is shown below,

$$MSE = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}[C(i,j)-S(i,j)]^2 \quad (1)$$

Where,

C(i,j) - illumination severities in cover image , S(i,j) - illumination severities in stego image, M and N are the dimensions of the cover and stego image.

If the difference between both the images are low then it has less differences otherwise it is considered to be the attack is more severe. So Low MSE gives higher quality of Stego Image.

Peak Signal-to-Noise Ratio (PSNR): Another Metrics for evaluating the perfor- mance are PSNR stated below in equation (2), It depicts the maximum signal to the noise appended on it. Practically higher PSNR value shows the quality of images.

$$PSNR = 10*\log\frac{P^2}{MSE} \quad (2)$$

Where, P = max[C(i,j), S(i,j)]

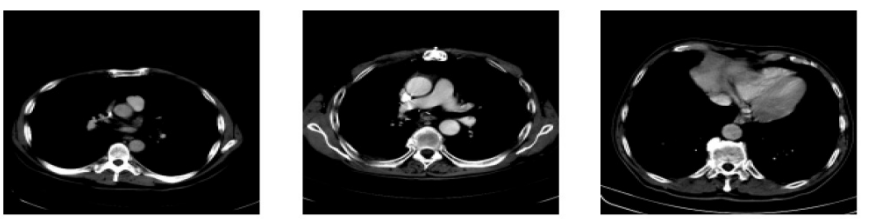

Figure 3

Original Image of DICOM file Format

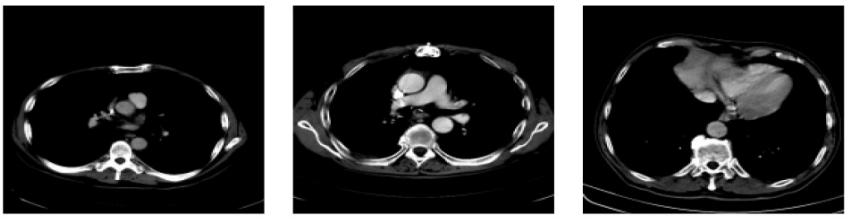

Figure 4

Stego Images of DICOM file format after steganography

Root Mean Square Error(RMSE): Finally Root Mean Square is Evaluated by the below equation(3) to analyze the performance,

$$RMSE = \sqrt{\frac{\Sigma_{i=1}^{N} x_i - \hat{x}_i^2}{N}} \quad (2)$$

Where, x_i = Observation of Original Image, $x\hat{}i$ = Observation after steganography

6. Comparative Analysis

The proposed scheme defines three different images of different sizes that hide different data loads. Payload may vary depending on cover image size. The im ages calculated for different payload capacity are shown in the table below, An analogy between two images with different payload sizes shows that DICOM has a higher PSNR the metrics are compared and shown in Table 1

Table 1

Evaluation Metrics of DICOM File Format with the previous researches

	Metrics	Image1	Image2	Image3
Proposed Method (Image Size 50kB and Payload Size is 5Kb)	MSE	0.006366	0.006542	0.007142
	RMSE	0.082859	0.085981	0.095892
	PSNR	68.8534	66.4507	67.1378
Proposed Method (Image Size 50kB and Payload Size is 10Kb)	MSE	0.007386	0.007842	0.006957
	RMSE	0.072952	0.0817882	0.080913
	PSNR	69.5324	70.5417	68.7217

Contd...

Proposed Method (Image Size 50kB and Payload Size is 15Kb)	MSE	0.006825	0.007014	0.006923
	RMSE	0.079589	0.083791	0.081922
	PSNR	67.8529	67.0586	69.4318
Ahmed et [23] al.'s (2022)	MSE	0.005203	0.005226	0.005192
	RMSE	0.072134	0.072292	0.072054
	PSNR	71.00199	70.98293	71.01155
Karakus and [24] Avci's (2020)	MSE	0.014366	0.014542	0.01442
	RMSE	0.119859	0.120589	0.120081
	PSNR	66.5574	66.5047	66.5413

7. Conclusion

The proposed system shows the hiding capacity inside a cover medium of DICOM file format. The improvement of the steganography method and recovery of the embedded data shows the algorithms higher efficiency of embedding capacity and its 100% recovery. The metrics utilized for the evaluation of algorithm shows the performance of the algorithm. The positive view of the proposed system possess, the maximum hiding capacity of 20kB with the good quality of the image. It can recover all the embedded message. Confidentiality is ensured in the algorithm

References

[1] A. ALabaichi, M. A. A. K. Al-Dabbas and A. Salih, "Image steganography using least significant bit and secret map techniques.," *International Journal of Electrical & Computer Engineering* (2088-8708), vol. 10 (2020).

[2] A. Pradhan, K. R. Sekhar and G. Swain, "Digital image steganography using LSB substitution, PVD, and EMD," *Mathematical Problems in Engineering*, vol. 2018 (2018).

[3] Ahmad, M. A., Elloumi, M., Samak, A. H., Al-Sharafi, A. M., Alqazzaz, A., Kaid, M. A., & Iliopoulos, C. Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images. *Alexandria Engineering Journal*, 61(12), 10577-10592 (2022).

[4] B. Sinha, "Comparison Of PNG & JPEG Format For LSB Steganography," *International Journal of Science and Research*, vol. 4, p. 198–201 (2015).

[5] C. C. Islamy and T. Ahmad, "Enhancing Quality of the Stego Image by Using Histogram Partition and Prediction Error," *Int. J. Intell. Eng. Syst.*, vol. 14, p. 511–520 (2021).

[6] Elgabar, Eltyeb E. Abed, and Fkhreldeen A. Mohammed. "JPEG versus GIF Im- ages in forms of LSB Steganography." *International Journal of Computer Science and Network* 2.8 : 86-93 (2013).

[7] H. Wang, X. Pan, L. Fan and S. Zhao, "Steganalysis of convolutional neural network based on neural architecture search," *Multimedia Systems*, vol. 27, p. 379–387 (2021).

[8] J. Liu, Y. Tian, T. Han, J. Wang and X. Luo, "Stego key searching for LSB steganography on JPEG decompressed image," *Science China Information Sciences*, vol. 59, p. 1–15 (2016).

[9] Karakus, S., & Avci, E. A new image steganography method with optimum pixel similarity for data hiding in medical images. Medical Hypotheses, 139, 109691 (2020).

[10] Karthikeyan, P., & Vasuki, S. Multiresolution joint bilateral filtering with modified adaptive shrinkage for image denoising. *Multimedia Tools and Applications*, 75(23), 16135 (2016).

[11] K. Karampidis, E. Kavallieratou and G. Papadorakis, "A review of image steganalysis techniques for digital forensics, "*Journal of Information security and application*s, vol. 40, p. 217-235 (2018).

[12] M. Fateh, M. Rezvani and Y. Irani, "A new method of coding for steganography based on LSB matching revisited," *Security and Communication Networks*, vol. 2021 (2021).

[13] M. K. Harahap and N. Khairina, "Dynamic steganography least significant bit with stretch on pixels neighborhood," *Journal of Information Systems Engineering and Business Intelligence,* vol. 6, p. 151–158 (2020).

[14] M. Płachta, M. Krzemień, K. Szczypiorski and A. Janicki, ”Detection of Image Steganography Using Deep Learning and Ensemble Classifiers,” Electronics, vol. 11, p. 1565 (2022).

[15] N. I. Yassin and E. Houby, ”EM Image Steganography Technique Based on Integer Wavelet Transform Using Most Significant Bit Categories,” *Int. J. Intell. Eng. Syst*, vol. 15, p. 499–508 (2022).

[17] O. Cataltas, T. KEMAL ”Improvement of LSB Based Image Steganography,” vol. 5, p. 1–5 (2017).

[16] X. Duan, M. Gou, N. Liu, W. Wang and C. Qin, ”High-capacity image steganog- raphy based on improved Xception,” Sensors, vol. 20, p. 7253 (2020).

[17] Z. Danny Adiyan, T. W. Purboyo and R. A. Nugrahaeni, ”Implementation of secure steganography on jpeg image using LSB method,” *International Journal of Applied Engineering Research,* vol. 13, p. 442–448 (2018).