UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Steganography Algorithms in Computed Tomography (CT) Scan Images

Kabilashwaran A/L Selvarajan[1*] & Yusliza Yusoff[2]
Faculty of Computing,
Universiti Teknologi Malaysia,
81310 UTM Johor Bahru, Johor, Malaysia
Email: kabilashwaran@graduate.utm.my[1]; yusliza@utm.my[2]

Submitted: 1/7/2024. Revised edition: 1/10/2024. Accepted: 6/10/2024. Published online: 25/11/2024
DOI: https://doi.org/10.11113/ijic.v14n2.472

***Abstract*—Steganography is a technique which allows to hide information or data inside a medium without giving an idea to people that the hidden data even existed. In the medical field, there are cases where patient's medical images breached along with their sensitive and personal data because of poor security. This problem leads to a wanting of a good solution to have the medical image with secured patient data. Here is where the image steganography takes place to hide the patient data inside the medical images. This study is conducted to determine the effective image steganography algorithm to be used in the medical field to embed the patient information inside their medical images specifically in Computed Tomography (CT) scan images. The image steganography algorithms that will be used in this study are Least Significant Bit (LSB), Exploiting Modification Direction (EMD) and Discrete Wavelet Transform (DWT). The flow of the image steganography technique will be studied and analyzed and after that, the algorithms will be implemented with different file formats which are Portable Network Graphics (PNG), Bitmap (BMP) and Joint Photographic Experts Group (JPG) and different image sizes which are 1024x1024 and 2048x2048 pixels. After that, the results are evaluated with performance metrics which are Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Structural Similarity Index Measure (SSIM) and Pairs Analysis. The results are then compared to determine the best image steganography algorithm along with the image file format which gives the highest robustness, visual quality, security and imperceptibility. The research result displays the EMD algorithm as the best paired with BMP file format in image steganography where it resulted in producing highest average of SSIM and PSNR which is 1.0 and 67.421 respectively and lowest MSE average of 0.012 with no traces in pairs analysis.**

***Keywords*—Steganography, Exploiting Modification Direction, Least Significant Bit, Discrete Wavelet Transform**

I. INTRODUCTION

Steganography is an approach of hiding information in the image, audio, or video file without giving idea to others that the concealed information even existed inside the file. The word steganography was derived from Greek word steganographia which gives the meaning of "covered writing" [1]. The medical field is going digital nowadays as the world is turning digital. It concerned that unauthorized individuals could access all their private and sensitive information.

Data breaches happened in the past. For example, In India in the year of 2020, more than 120 million of patients medical related images has been revealed [2]. The X-rays and scans images have been leaked online for public access. According to German cybersecurity firm Greenbone Networks, the patient records, scans, and images containing information that is intended to be kept confidential, such as the patient's name, date of birth, national ID, name of the medical facility, medical history, and physician names. Similar kind of incident happened in 2019, where millions of American people's medical related photos can be disclosed on internet [3] Moreover, the number of medical images shared online are increasing because some people might do online consultations. When storing or sending data for diagnostic reasons, it is essential to consider the critical issue of medical image security. So, image steganography is a great method for enhancing the confidentiality of the medical images since it does not give a clue to the people that hidden data exists in the medical image.

The project will run within the following scope starting with Spatial domain methods which are Least Significant Bit (LSB) and Exploiting Modification Direction (EMD) algorithm and frequency domain method which is Discrete Wavelet Transform

(DWT) algorithm are compared. Secondly, Computed Tomography (CT) scan images with Portable Network Graphics (PNG), Bitmap (BMP) and Joint Photographic Experts Group (JPG) file format are being used in this comparison. Thirdly, the performance of the images in the different algorithms are studied using Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM) and Pairs Analysis. Fourthly, different sizes for all CT scan images are used for comparison which are 1024x1024 and 2048x2048 pixels.

In this study, image steganographic algorithms will be used to secure private and confidential information in medical field. The results of this study will help medical organizations manage medical data more efficiently and securely, especially during storage and transmission of the data. The main benefit of this will be a better understanding of how to apply three image steganographic algorithms to different picture file formats and sizes. As a result, people can hide a secret image inside a cover image to hide the data in an image file. This ensures that all communications reach their intended recipient securely and storing data inside image is stressless because no one will be aware of the hidden data. So, no unauthorized person will be able to view or change the data in the image which ensures confidentiality, integrity and availability (CIA). Finally, the results of this study will be extremely helpful to the upcoming academic researchers when it comes to image steganography. Future researchers can learn about the Least Significant Bit (LSB), Exploiting Modification Direction (EMD) and Discrete Wavelet Transform (DWT) algorithms and its performance to determine robustness, visual quality, and imperceptibility.

The aim of this project is to determine the best image steganography algorithm from the chosen algorithms along with the image file format which gives the highest robustness, visual quality, and imperceptibility.

This paper is structured as follows: Section II represents the literature review and methodology in Section III. Result and analysis are illustrated in Section IV. Finally, the conclusion and recommendation were made in Section V.

II. Literature Review

To clearly understand this research, literature review was done in steganography. Image steganography algorithms and related past research papers were studied as well.

A. Least Significant Bit (LSB)

LSB is a popular approach for concealing and revealing confidential information or data to cover images. This technique normally uses LSB substitution and matching methods to achieve the steganography in the cover images [4]. To hide the data, some chosen least significant bits from the pixel of the cover image are substituted and embedded with the secret information or data. The LSB method can be selected on how many bits of LBS pixels are needed to be substituted to hide the data from 1 bit of LSBs to 7 bit of LSBs. The LSB method is less complex to be used and it is flexible too [5].

B. Exploiting Modification Direction (EMD)

The Exploiting Modification Direction (EMD) steganography method is a popular embedding technique that guarantees great fidelity for the stego-image. In this method, the (2n + 1)-ary notational system is used. The n variable in it is cover pixels amount. It transforms the secret data throughout the EMD embedding process [6]. The range of the highest pixel distortion values is just increased or decreased by 1 [7]. More secret information or data can be hidden in the pixels in high texture areas since the EMD method depends on a certain base for determining the local pixel variation intensity in an image. EMD also robust against the steganalysis which gives higher security to the stego-image [8]. However, as the number of chosen pixels rises, a smaller embedding capacity [9].

C. Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform (DWT) is the technique of decomposing a picture into multiple resolutions by expanding the image over a collection of wavelet basis functions. DWT algorithm transforms the image from spatial domain to frequency domain. The popular type of DWT is Haar based DWT technique (HDWT) [5]. During the DWT method, the signal is divided into high-frequency band (H) and low-frequency band (L). The low frequency band from the decomposition will decompose again into high and low frequency bands which will result to the total of four sub-bands which are LL, LH, HL and HH [10]. LL is the low-frequency sub-band, LH and HL are middle-level frequency sub-bands, HH is high-frequency sub-band. Crucial information about the image is in the LL portion. Stego-image can become distorted if the secret data embedded in LL portion, but it also makes it resistant to other attacks [11]. So, DWT technique uses HH sub-band to embed the secret data into the cover image [12].

III. Methodology

Fig. 1 shows the overall framework of the experiment. The experiment was divided into three parts where every one of the part will be running on LSB, EMD and DWT. Each part of the experiment was carried out with PNG, BMP and JPG images with 1024x1024 and 2048x2048 pixel images as cover images and an image with patient detail as the secret image. The collection of data, the execution of the image steganography technique and the testing of the algorithm was done for all the parts of this experiment. The code for the algorithms was later run using MATLAB for LSB and EMD while Visual Studio Code for EMD to conceal the secret image inside the cover image. The stego image which was the output image is tested with the MSE, PSNR, SSIM and Pairs Analysis performance measure metrics. The results were analyzed and evaluated between the algorithms. The following are the research framework which consist of 3 phases.

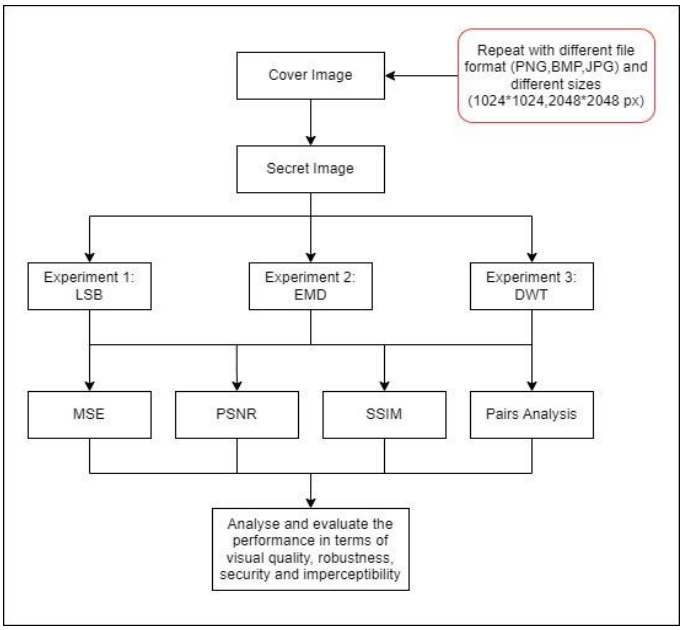


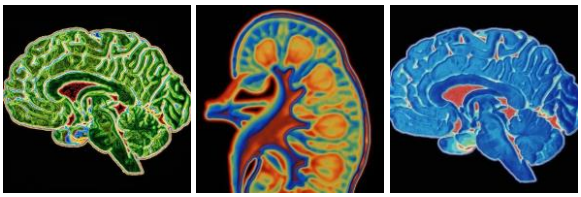
Fig. 2. Overall framework for the experiment

A. Phase 1: Review, study and identify potential image steganography algorithms

Image steganography algorithms are chosen which are LSB, EMD and DWT. Then, properties of different image file formats which are JPG, BMP and PNG are studied. Next, previous research papers on image steganography were studied to understand this research better. Then, performance measures are chosen which are MSE, PSNR, SSIM and Pairs Analysis.

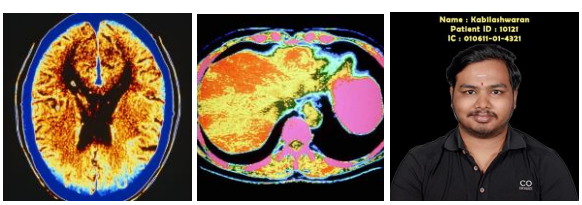
B. Phase 2: Design and Implement the experiment

Then, Input images to run the experiment were gathered. All the 5 cover images and a secret image are prepared in JPG, BMP and PNG file format as well as 1024 x 1024 px and 2048 x 2048 px sizes. Fig. 1 shows cover image 1,2,3 while Fig. 2 shows cover image 4,5 and secret image.



CT_Scan_1.png CT_Scan_2.png CT_Scan_3.png

Fig. 2. Cover Image 1,2,3



CT_Scan_4.png CT_Scan_5.png secr.png

Fig. 3. Cover Image 4,5 and Secret Image

Then software to conduct the experiment, which are MATLAB and VS Code was installed. Source code for the algorithms was acquired and the experiment was conducted. The source code for the algorithm was found in GitHub for the collection of data as mentioned in [24], [25], [26] and [27].

C. Phase 3: Analysis, comparison, evaluation and discussion

The performance of the algorithms was analyzed based on the results from MSE, PSNR, SSIM and Pairs Analysis. The visual quality, security, robustness, imperceptibility of the algorithm was then evaluated and discussed.

1) Visual Quality

The cover image's visual quality was affected by the secret information that was embedded using any steganographic technique. Even though it might not be immediately obvious to the human eye, since there is changes made in the image the quality is affected at least in a tiny portion [13]. It is crucial that the embedding takes place without the cover picture retracting significantly or losing its perceptual quality [14]. To identify the visual quality, standard measurement procedures such as PSNR and MSE value are used.

2) Security

The embedded algorithm is said to be secure if the embedded information is not eliminated after being exposed by an attacker since it depends on the full disclosure of the embedded algorithm [14]. The data hiding approach should be protected with data security to ensure that only intended or authorized users can access it. It also has to do with preventing unauthorized user recognizing concealed information [16].

3) Robustness

Robustness refers to the ability to withstand channel noise or interface distortion intended to prevent the use of steganography techniques [17]. In other words, it is the capacity of the embedded data to remain unaltered when the stego-image went to transformations such as scaling, rotation, random noise addition, linear and non-linear filtering, and lossy compression [18]. PSNR can used to represent distortion value.

4) Imperceptibility

It stands for the capacity to elude detection, that is, to go undetected by the human eye. While not altering the image in a way that can be seen by the human eye, some techniques may nonetheless do so in a way that can be seen by statistical testing [15]. There shouldn't be any noticeable visual artefacts in stego-images. Higher fidelity of the stego-images indicates better imperceptibility. Metrics that can be used to evaluate the imperceptibility are by using the MSE, PSNR and SSIM [19].

5) Mean Squared Error (MSE)

MSE is the squared failure among the cover image as well as the stego-image that has been incrementally increased over time. The discrepancy among numbers entailed by the approximator and the actual numbers get approximated is measured using the Mean Squared Error (MSE). As it compares the cover image and the stego-image, the higher the

MSE value tells that the error is higher [20]. The formula of the MSE is as the equation 1 below where n is the point of data, Y_i is value that is observed, and Y^_i is the predicted value:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2 \quad (1)$$

6) Peak Signal-to-Noise Ratio (PSNR)

As the name suggests, PSNR is the ratio of the peak signal and the noise in the image. The effectiveness of steganography is indicated by the PSNR rate where the greater the PSNR, the better the steganography algorithm [20]. PSNR needs the MSE value to be calculated. The PSNR value more than 40db is considered great image quality [21]. The formula of the PSNR is as the equation 2 below:

$$PSNR = 10 \times \log\left(\frac{255^2}{MSE}\right) \quad (2)$$

7) Structural Similarity Index Measure (SSIM)

The Structural Similarity Index Measure (SSIM) is a model based on perception. Image degradation is viewed in this manner as an alteration about the way the structural information is detected. Moreover, luminance masking as well as contrast masking aspects also it takes effect. The perceived quality of images is estimated using SSIM as it compares the similarities among the cover image as well as the stego-image. The formula of the SSIM is as the equation 3 below where μ_x and μ_y is pixel mean sample, μ_x^2 and μ_y^2 is variance, σ_xy is cross-correlation for x and y respectively:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (3)$$

8) Pairs Analysis

Pair Analysis is a steganalysis technique which used to detect camouflaged information or data in an image that looks at the statistical properties of the differences between adjacent pixel values. The technique concentrates on looking at the absolute differences between neighbour pixels because steganographic techniques usually alter pixel values only a little to hide information [22]. By calculating the differences, a "pair-difference map" is generated where deviations from natural image statistics are highlighted. Pairs analysis can efficiently detect the existence of undisclosed data through spotting these irregularities on the pair difference map [23].

IV. Result & Analysis

This section discusses the experiment result that was conducted using LSB, EMD and DWT algorithms and three different image formats which are PNG, JPG and BMP. LSB and DWT were implemented in MATLAB while EMD was implemented in Visual Studio Code.

TABLE I. PSNR VALUES FOR 2048 X 2048PX IMAGES

PSNR (dB)				
Cover Image	***Image Format***	***LSB***	***EMD***	***DWT***
1	.bmp	31.895	67.872	32.770
2		30.969	68.075	32.589
3		31.256	67.857	32.613
4		30.369	65.557	33.035
5		30.719	67.745	33.047
1	.png	31.740	65.421	32.757
2		30.944	65.333	32.586
3		31.140	65.494	32.603
4		30.256	65.225	33.032
5		30.596	65.410	33.011
1	.jpg	31.505	65.168	32.622
2		30.783	65.302	32.511
3		30.957	65.192	32.550
4		30.274	65.228	32.965
5		30.715	65.468	32.849

Table I shows the comparison of PSNR values for the images in LSB, EMD and DWT algorithms. Overall, EMD algorithm's 2048 x 2048px image with BMP file format gave the best result among all the data. The EMD produces significantly higher value compared to LSB and DWT. This indicates that the EMD algorithm with BMP file format and 2048x2048px image size is the best pair for producing high quality stego-image compared to LSB and DWT algorithm.

TABLE II. MSE VALUES FOR 2048 X 2048PX IMAGES

MSE				
Cover Image	***Image Format***	***LSB***	***EMD***	***DWT***
1	.bmp	42.029	0.011	34.360
2		52.021	0.010	35.821
3		48.698	0.011	35.624
4		59.727	0.018	32.327
5		55.107	0.011	32.241
1	.png	43.558	0.019	34.466
2		52.317	0.019	35.847
3		50.018	0.018	35.707
4		61.303	0.020	32.350
5		56.687	0.019	32.509
1	.jpg	45.977	0.020	35.557
2		54.303	0.019	36.471
3		52.172	0.020	36.146
4		61.052	0.020	32.857
5		55.152	0.019	33.745

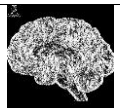
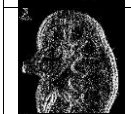
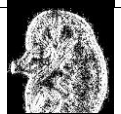
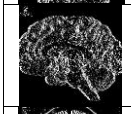
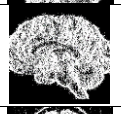
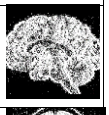
Table II shows the comparison of MSE values for the images in LSB, EMD and DWT algorithms. The table clearly shows the effectiveness of EMD algorithm in terms of the MSE values where it produces lowest MSE values than LSB and DWT especially in bmp images makes the EMD algorithm as the most practical and secure to be used. This shows that EMD is more robust, imperceptible and closest quality to the actual cover image.

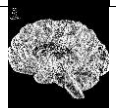
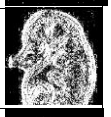
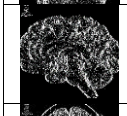
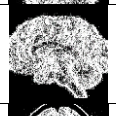
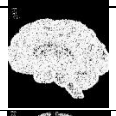
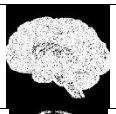
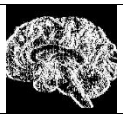
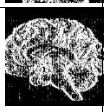
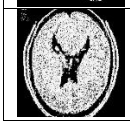
TABLE III. SSIM VALUES FOR 2048 X 2048PX IMAGES

SSIM				
Cover Image	***Image Format***	***LSB***	***EMD***	***DWT***
1	.bmp	0.962	1.0	0.986
2		0.925	1.0	0.994
3		0.941	1.0	0.990
4		0.956	1.0	0.996
5		0.908	1.0	0.995
1	.png	0.838	1.0	0.991
2		0.882	1.0	0.995
3		0.804	1.0	0.994
4		0.954	1.0	0.997
5		0.806	1.0	0.994
1	.jpg	0.725	0.999	0.993
2		0.781	0.999	0.996
3		0.742	0.999	0.996
4		0.961	0.999	0.996
5		0.835	0.999	0.991

Table III shows the graphical comparison of SSIM values for Images in LSB, EMD and DWT algorithm. The EMD algorithm gave a value of 1.0 for both BMP and PNG image and 0.999 for the JPG image. The structural information alteration in EMD algorithm's BMP and PNG images were stayed undetected by the SSIM algorithm which shows the effectiveness of EMD algorithm on embedding data inside the cover image without compromising the structure of the image.

TABLE IV. PAIRS ANALYSIS IN 2048 X 2048PX IMAGES

Pairs Analysis				
Cover Image	***Image Format***	***LSB***	***EMD***	***DWT***
1	.bmp			
2				
3				
4				

Pairs Analysis				
Cover Image	***Image Format***	***LSB***	***EMD***	***DWT***
5				
1	.png			
2				
3				
4				
5				
1	.jpg			
2				
3				
4				
5				

Based on the result in Table IV, the hidden information details from the stego-image can be seen partially in the LSB algorithm images using Pairs Analysis. Each and every Pairs Analysis results from LSB algorithm stego-images produced the partial structure of the secret image that used in this research experiment. This applies to all the image file formats used in this experiment. Even though it does not reveal the complete details of the information at the top left corner, the leak of the information indicates a lower level of security from the LSB algorithm compared to EMD and DWT. It is proven that the LSB isn't that robust, given that the two other algorithms secret image information couldn't be detected.

V. CONCLUSION AND RECOMMENDATION

For all the five images, EMD algorithm gave the highest PSNR value and lowest MSE values. Similarly, BMP image file format in 2048 x 2048 px image size particularly

performed so well. EMD algorithm also produced stego-image with similar structure with the cover image where it gives 1.0 value which is the highest value for SSIM performance measure for all the tested images in BMP and PNG file format. This really proves the exceptional stego-image quality produced by the algorithm. The Pairs Analysis result for the EMD also did not make any traces for the secret image information. It shows that the algorithm has high security and robustness. So, EMD image steganography algorithm is the most effective in hiding the image data with highest imperceptibility, robustness, security and great image quality in medical field especially in CT scan images

ACKNOWLEDGMENT

Firstly, I want to thank the God for making me complete this thesis. Secondly, I cannot forget my final year project supervisor who is Dr. Yusliza binti Yusoff for her guidance and support. Finally, I want to express my gratitude and thanks to everyone who helped with the project.

CONFLICTS OF INTEREST

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

REFERENCES

[1] Rădescu, R., & Gliga, R. (2004). An introduction to steganography. *UPB Scientific Bulletin, Series C: Electrical Engineering, 64*, 17-24.

[2] Inc42, T. (2020). Healthcare data leak: Over 120 Mn medical images of Indian patients left exposed. Inc42. https://inc42.com/buzz/india-healthcare-data-leak-over-120-mn-medical-images-exposed/.

[3] Jack Gillum, J. K. a. J. L. (2019). Millions of Americans' medical images and data are available on the internet. Anyone can take a peek. *ProPublica.* https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet.

[4] Dr. Amarendra K, V. N. M., B.Chetan gupta, G. Geetha Sudheshna, V. Venkata Anusha. (2019). Image steganography using LSB. *International Journal of Scientific & Technology Research, 8*(12)

[5] Pratap Chandra Mandal, I. M., Goutam Paul, B. N. Chatterji. (2022). Digital image steganography: A literature survey. *Information Sciences, 609.*

[6] Niu, X., ma, M., Tang, R., & Yin, Z. (2015). Image steganography via fully exploiting modification direction. *International Journal of Security and its Applications*, *9*, 243-254. https://doi.org/10.14257/ijsia.2015.9.5.24.

[7] Pradhan, Krovi, R. S., & Swain, G. (2018). Digital image steganography using LSB substitution, PVD, and EMD. Mathematical Problems in Engineering, 2018. https://doi.org/10.1155/2018/1804953.

[8] Kim, H., Kim, C., Choi, Y., Wang, S., & Zhang, X. (2010). Improved modification direction methods. *Computers & Mathematics with Applications, 60*, 319-325. https://doi.org/10.1016/j.camwa.2010.01.006.

[9] Taha, M., Mahdi, Q., Sabah, M., Shafry, M., Rahim, M., Hashim, M., Mardziah, A., & Ahmad, B. (2018). Categorization of spatial domain techniques in image steganography: A revisit. *Journal of Advanced Research in Dynamical and Control Systems, 10*, 13.

[10] Tevaramani, S. S., & J, R. (2022). Image steganography performance analysis using discrete wavelet transform and alpha blending for secure.

[11] Pratap Chandra Mandal, I. M., Goutam Paul, B.N. Chatterji. (2014). A study of steganography techniques using discrete wavelet transform. *Journal of Global Research in Computer Sciences*, *5*(5)

[12] Tushara M, K. A. N. (2016). Image Steganography Using Discrete Wavelet Transform–A review. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 3*(1)

[13] AL-Naima, A. S. A. (2015). Image steganography based on discrete wavelet transform and enhancing resilient backpropogation. *Neural Network.* Middle East University.

[14] Islam, M., A.W, N., Zaidan, A., & Bahaa, B. (2010). New system for secure cover file of hidden data in the image page within executable file using statistical steganography techniques. *International Journal of Computer Science and Information Security.*

[15] Roy, R., & Changder, S. (2016). Quality evaluation of image steganography techniques: A heuristics based approach. *International Journal of Security and its Applications*, *10*, 179-196. https://doi.org/10.14257/ijsia.2016.10.4.18.

[16] Vijayakumar, M. S. (2011). Image Steganography based on Polynomial Functions. *Journal of Global Research in Computer Sciences*, *2*.

[17] Altaay, A., Sahib, S., & Zamani, M. (2012). *An Introduction to Image Steganography Techniques.*

[18] Yadav, R., Saini, R., & Joshi, K. (2011). Cyclic combination method for digital image steganography with uniform distribution of message. *Advanced Computing: An International Journal, 2,* 29-43. https://doi.org/10.5121/acij.2011.2604.

[19] Setiadi, D. R. I. M. (2021). PSNR vs SSIM: Imperceptibility quality assessment for image steganography. *Multimedia Tools and Applications, 80*(6), 8423-8444. https://doi.org/10.1007/s11042-020-10035-z.

[20] Jambhekar, N., Dhawale, C., & Hegadi, R. (2014). Performance analysis of digital image steganographic algorithm. *ICTCS '14: Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies.* https://doi.org/10.1145/2677855.2677937

[21] Li, Z., Peng, Y., Zou, L., & He, Y. (2022). Intelligent algorithm-based ultrasound for evaluating the anesthesia and nursing intervention for elderly patients with femoral intertrochanteric fractures. *Comput Intell Neurosci, 2022*, 3557994. https://doi.org/10.1155/2022/3557994.

[22] Dumitrescu, S., Wu, X., & Wang, Z. (2003). Detection of LSB steganography via sample pair analysis. *Signal Processing, IEEE Transactions on, 51*, 1995-2007. https://doi.org/10.1109/TSP.2003.812753.

[23] Bansal, A., Muttoo, S., & Kumar, V. (2016). Security against sample pair steganalysis in eight queens data hiding technique. *International Journal of Computer Network and Information Security, 8*, 39-46. https://doi.org/10.5815/ijcnis.2016.08.05.

[24] altrk19. (2018). GitHub - altrk19/Steganography-EMD. GitHub. https://github.com/altrk19/Steganography-EMD.

[25] RArnoco. (2021). GitHub – Rarnoco / steganography - LSB_DWT_masking-and-filtering: Implemented Comparison Analysis of LSB, DWT and MFT in Image Steganography. GitHub. https://github.com/RArnoco/steganography-LSB_DWT_Masking-And-Filtering.

[26] akshatagarwal1265. (2019). GitHub - akshatagarwal1265 / steganography-image-4LSBs: Using MATLAB to embed the secret-image's each pixel's first 4 MSBs in the cover-image's pixel's last 4 LSBs. GitHub. https://github.com/akshatagarwal1265/steganography-image-4LSBs.

[27] mostafaGwely. (2018). GitHub - mostafaGwely/Structural-Similarity-Index-SSIM-: how to compare two images with Python using the Structural Similarity Index (SSIM). GitHub. https://github.com/mostafaGwely/Structural-Similarity-Index-SSIM-.