Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 2, April 2025, Page. 1029-1040
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4426

Securing Medical Images Using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) for Image Steganography

Elkaf Rahmawan Pramudya*[1,2], L. Budi Handoko[1,2], Budi Harjo[1,2], Ramadhan Rakhmat Sani[1,2], Christy Atika Sari[1,2], Guruh Fajar Shidik[1,2], Pulung Nurtantio Andono[1,2], Md. Kamruzzaman Sarker[3]

[1]Study Program in Informatics Engineering, Universitas Dian Nuswantoro, Indonesia
[2]Research Center for Intelligent Distributed Surveillance and Security, Universitas Dian Nuswantoro, Semarang, Indonesia
[3]Department of Computer Science, Bowie State University, United States

Email: elkaf.rahmawan@dsn.dinus.ac.id

Received : Feb 10, 2025; Revised : April 14, 2025; Accepted : May 15, 2025; Published : May 17, 2025

Abstract

Steganography is a technique for embedding secret information into digital media, such as medical images, without significantly affecting their visual quality. The primary challenge in medical image steganography is preserving the quality of the cover image while ensuring robustness against distortions such as compression or data manipulation attacks, which may impact diagnostic accuracy. This study proposes an enhanced steganographic method based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to improve the security and robustness of medical image embedding. DWT decomposes the medical image into four frequency sub-bands (LL, LH, HL, HH), while SVD is applied to embed the secret image while maintaining essential medical features. Experimental results show that the proposed method achieves a PSNR value of up to 78 dB and an SSIM value approaching 1, indicating that the stego image quality is nearly identical to the original cover image. Compared to previous DCT-SVD and IWT-SVD-based approaches, the DWT-SVD method offers superior robustness and imperceptibility, particularly in preserving image quality in complex-textured medical images. This method contributes to enhancing data security in telemedicine and AI-based medical imaging applications by ensuring that sensitive medical data remains protected while preserving image integrity for diagnostic use.

Keywords : *Data Hiding, Discrete Wavelet Transform, Image Steganography, Singular Value Decomposition.*

1. INTRODUCTION

Data security ensures the protection of data from unauthorized access, manipulation, theft, or damage [1], [2], [3]. In the rapidly evolving digital era, data has become a valuable asset that holds critical information, ranging from medical records to financial data [4], [5]. Therefore, data security is a top priority to maintain confidentiality, integrity, and availability [6], [7]. Data security strategies encompass various techniques such as encryption, authentication, and access control, which are designed to safeguard data both in storage and during transmission [8].

Medical data, including medical images such as MRI, CT scans, and radiographic images, often contain highly sensitive information that could be misused if it falls into the wrong hands [9]. In reality, many healthcare institutions still rely on outdated security protocols, making their data more vulnerable to exposure and cyberattacks. For instance, ransomware attacks on hospitals have demonstrated how medical images can be locked or altered, disrupting diagnosis and patient care. Moreover, the deliberate

introduction of noise into medical images can compromise data integrity and reduce the accuracy of computer-aided analysis, potentially threatening patient safety [10].

As a solution to these challenges, image steganography based on Discrete Wavelet Transform (DWT) can be implemented to enhance the security of medical data [11], [12]. This technique enables the embedding of confidential data, such as patient identities or diagnostic information, into medical images by leveraging frequency-domain transformations, ensuring that the embedded data remains protected without degrading the visual quality of the medical cover image. With DWT, embedding is performed on the transform coefficients while preserving the primary structure of the image, ensuring that the image remains suitable for diagnosis without significant distortion [13], [14]. Additionally, DWT provides better resilience against noise attacks, compression, and other manipulations commonly encountered in digital data processing [15]. This approach not only maintains the confidentiality of medical data but also preserves the accuracy and reliability of medical images for diagnostic purposes.

Song et al. [16] proposed a DCT-SVD approach to enhance the robustness and imperceptibility of steganographic systems. Based on this approach, a robust JPEG steganography algorithm was developed in the nonsubsampled shearlet transform domain. This algorithm integrates the advantages of nonsubsampled shearlet transform, DCT, and SVD to establish a compression-resistant embedding domain. With a minimal distortion principle, the framework and key steps of the embedding and extraction process are explained in detail. Experimental results demonstrate that this method not only achieves competitive robustness but also enhances resistance against steganalysis, surpassing several state-of-the-art robust steganography algorithms.

El-Shahed et al. [17] introduced an SWT-SVD approach to develop a steganographic algorithm that embeds a secret image into video frames using multi-resolution techniques. In this method, three-level 3D Stationary Wavelet Transform (SWT) is applied to the cover video frames, followed by the application of Singular Value Decomposition (SVD) on one of the transformed sub-bands. SVD is also applied to the secret image to extract its singular matrices, which are then embedded into the singular matrix of the video sub-band. Finally, an inverse transformation is performed to reconstruct the stego-video. This study compared the embedding performance at different resolutions and found that embedding at the third resolution level yielded the best Peak Signal-to-Noise Ratio (PSNR) values. The proposed algorithm demonstrated promising results both qualitatively and quantitatively when tested on color and grayscale images.

Durafe et al. [18] proposed an IWT-SVD approach to enhance robustness and imperceptibility in image steganography using a hybrid combination. This method embeds a color secret image into a fractal cover image, producing a stego-image that closely resembles the original cover image. By utilizing fractal compression and the hybrid IWT-SVD scheme, the algorithm achieves high embedding capacity and strong resistance against image-processing attacks. The secret image is embedded into the U and V components of the fractal cover image using a scaling factor based on the Human Visual System (HVS) model, ensuring a secure and resilient stego-image.

Vol. 6, No. 2, April 2025, Page. 1029-1040
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4426

Table 2. Analysis of the novelty of methods from related research

Researcher	Methods	Research Objective
Song et al. [16]	Discrete Cosine Transform (DCT) - Singular Value Decomposition (SVD)	Image Steganography
El-Shahed et al. [17]	Stationary Wavelet Transform (SWT) - Singular Value Decomposition (SVD)	Image Steganography
Durafe et al. [18]	Integer Wavelet Transform (IWT) - Singular Value Decomposition (SVD)	Image Steganography
Our Study	Discrete Wavelet Transform (DWT) - Singular Value Decomposition (SVD)	Image Steganography

The three studies above propose SVD-based approaches to enhance the robustness of image steganography, each employing different key techniques. Song et al. [16] integrated SVD with DCT to establish a compression-resistant embedding domain in a JPEG steganography algorithm. El-Shahed et al. [17] combined SVD with SWT to embed a secret image into video frames using a multi-resolution approach. Meanwhile, Durafe et al. [18] leveraged a hybrid IWT-SVD combination to embed a secret image into fractal cover images, ensuring resistance against image-processing attacks. DCT-SVD suffers from blocking artifacts and lower resistance to distortions when applied to compressed medical images [16]. Meanwhile, IWT-SVD achieves good robustness but can introduce visible artifacts in medical images with complex textures, reducing the quality of the stego image [18]. SWT-SVD provides strong embedding capacity but increases computational complexity, making it less efficient for real-time applications [17]. In contrast, the proposed DWT-SVD method overcomes these limitations by embedding secret information in the LL sub-band of DWT, ensuring minimal distortion while maintaining the medical image's diagnostic value.

Based on these approaches, this study aims to develop an optimized steganographic method using DWT-SVD to enhance data security in medical images while ensuring high robustness and imperceptibility. The primary objective is to improve the security of embedded data in medical images while maintaining visual fidelity and computational efficiency. Additionally, this study evaluates the performance of the proposed method against existing DCT-SVD and IWT-SVD techniques to assess its effectiveness in preserving image quality. The results of this research contribute to the advancement of secure medical image transmission, particularly in telemedicine and AI-assisted diagnostics, where data confidentiality and image integrity are crucial.

Vol. 6, No. 2, April 2025, Page. 1029-1040
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4426

2. METHOD

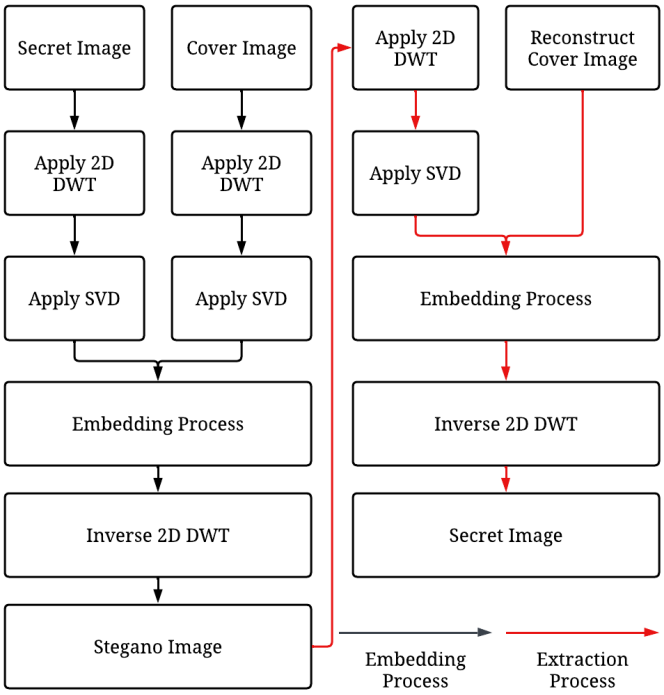


Figure 1. Proposed Scheme

Based on Figure 2, the research process begins with the embedding stage, where a 2D Discrete Wavelet Transform (DWT) is applied to both the secret image and the cover image, followed by Singular Value Decomposition (SVD) on each transformed result. Next, the embedding process is carried out to insert the secret image into the cover image. After embedding, an inverse 2D DWT is applied to generate the stego-image.

In the extraction process, the stego-image is reconstructed by performing the reverse steps, including the application of DWT and SVD, to recover the secret image from the stego-image. This process ensures efficient integration and reliable extraction of the embedded data.

2.1. Discrete Wavelet Transform (DWT)

DWT in image steganography is used to break down an image into several sub-bands that represent information at different scales or resolution levels [19]. This process begins by applying a wavelet transform to produce four main components: LL, LH, HL, and HH [20]. The formula for DWT on a 2D image can be seen in eq (1) and (2).

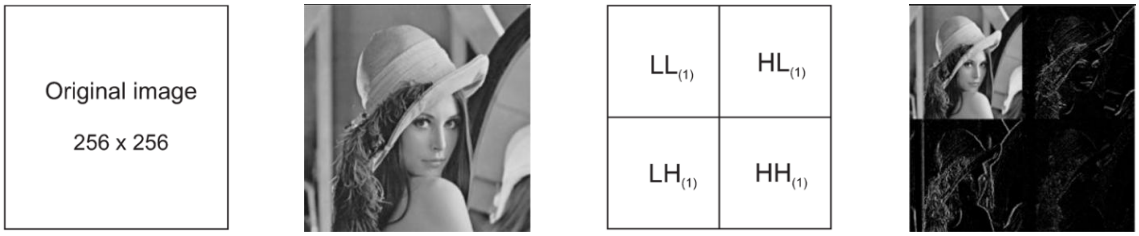
$$H(x,y) = \sum_{i}\sum_{j} I(i,j) \cdot W_h(i-x) \cdot W_h(j-y) \quad (1)$$

Where, eq (1) is the transformation process on image $I(i,j)$ in the horizontal direction and W_h is the horizontal wavelet filter. Where, eq (2) is the transformation process on image $H(i,j)$ in the vertical direction and W_u is the vertical wavelet filter.

$$D(x,y) = \sum_{i}\sum_{j} H(i,j) \cdot W_u(i-x) \cdot W_u(j-y) \quad (2)$$

Vol. 6, No. 2, April 2025, Page. 1029-1040
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4426

After DWT transformation, the image $D(x, y)$ is divided into four main sub-bands: LL, LH, HL, and HH. The results can be seen in Figure 2. Figure 2(a) shows the secret image to be used in the steganography process, while Figure 2(b) shows the Level 1 DWT result of the image, which is divided into LL, LH, HL, and HH sub-bands, each depicting a different frequency of the original image. The LL sub-band contains low-frequency information and retains the most essential structural details, making it the most suitable for embedding secret data with minimal distortion. The LH and HL sub-bands capture horizontal and vertical edge details, respectively, which contribute to texture and contour information, while the HH sub-band represents high-frequency noise and fine details. Given that the LL sub-band holds the majority of perceptual and structural information, it is selected for embedding to ensure imperceptibility and robustness against compression and noise.



(a) Secret Image (b) DWT Level 1

Figure 2. Pre-processed DWT

The LL sub-band represents low frequencies in both horizontal and vertical directions, containing dominant information of the main image. The LH sub-band contains low frequencies in the horizontal direction and high frequencies in the vertical direction, preserving the vertical details of the image. In contrast, the HL sub-band contains high frequencies in the horizontal direction and low frequencies in the vertical direction, focusing on the horizontal details of the image. Finally, the HH sub-band contains high frequencies in both horizontal and vertical directions, depicting the texture or noise details of the image. Each of these sub-bands provides different information that is used in various steganography and image processing applications [21].

2.2. Singular Value Decomposition (SVD)

In this study, SVD is used to insert secret information by utilizing the singular values of the image matrix [22]. The SVD process begins by breaking the image matrix A into three matrices, namely $U, \Sigma,$ dan V^T. Where, Σ contains singular values that represent the information strength of the original image [23].

Implementation of SVD on cover image, applied to each RGB color channel of the cover image. It divides the cover image into three matrix components: U_c (as the left component), r_c (as the right component). Matrix U_c contains the left singular vectors of the cover image, which represent the main orientation information of the image. While the implementation of SVD on the secret image is through the same process as the cover image, where both have a size of 512x512 and undergo a 2D DWT transformation using the Haar transform. After DWT, the LL (Low-Low) sub-band of the secret image is selected to store the most dominant information, which is considered the most important to insert information. A higher α value increases embedding capacity but may introduce visible distortions, while a lower α value maintains better visual quality at the cost of lower robustness. In this study, α is empirically set to 0.1–0.5, ensuring that the PSNR remains above 70 dB while maintaining a high SSIM above 0.96. The combination of cover and secret image can be seen in eq (3).

Vol. 6, No. 2, April 2025, Page. 1029-1040
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4426

$$\sigma_{emnedded} = \sigma_c + \alpha \cdot \sigma_s \quad (3)$$

Where, $\sigma_{emnedded}$ is the singular value generated after embedding the secret image into the cover image. This value is calculated by adding the singular value σ_c of the cover image and the singular value σ_s of the secret image that has been scaled by a factor α. The factor α controls how much influence the secret information has on the cover image, thus maintaining the visual quality of the cover image while hiding the information.

After the process of embedding the secret image into the cover image, the next step is to change the singular coefficient of the cover image with the singular coefficient of the secret image using eq (4).

$$s_s = U_c \cdot \sigma_{emnedded} \cdot V_c^T \quad (4)$$

Where, s_s is the modified singular matrix, obtained after embedding the secret information into the cover image. This process is done by multiplying the U_c matrix (left component of the cover image), the $\sigma_{emnedded}$ matrix (singular values that have been embedded with information), and the V_c^T matrix (right component of the cover image).

2.3. Quality Assessment

At this stage, image quality measurements are carried out to evaluate the extent to which the applied method affects the stego image results, which will be discussed through the MSE, PSNR, and SSIM metrics. The discussion of these two metrics will be further described in the points below.

1. Mean Squared Error (MSE)

MSE is one of the metrics used to measure how big the difference is between the original image and the stego image after the information insertion process [24]. MSE calculates the average of the square of the difference between each pixel of the original image and the stego image. The calculation formula for MSE can be seen in eq (5).

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(I(i,j) - K(i,j))^2 \quad (5)$$

2. Peak Signal to Noise Ratio (PSNR)

PSNR is a metric used to measure image quality by comparing the original image and a distorted image, such as a stego image [24]. PSNR measures the ratio between the maximum signal (the highest pixel value) to the level of noise or distortion present in the image [25]. PSNR is usually measured in decibels (dB), and the higher the PSNR value, the better the quality of the stego image because it shows less distortion or noise. The calculation of PSNR can be seen in eq (6).

$$PSNR = 10 \log 10 \left(\frac{\max\ \_pixel\_value^2}{MSE}\right) \quad (6)$$

3. Structural Similarity Index (SSIM)

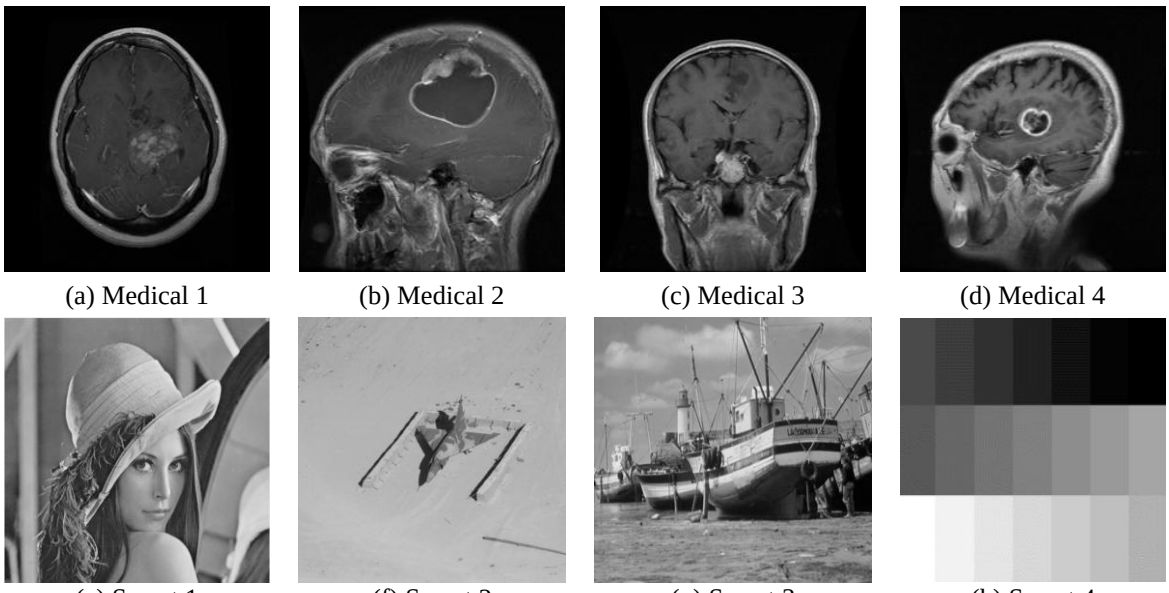
SSIM is a metric used to measure the similarity of visual structures between two images, taking into account luminance, contrast, and structure [24]. Unlike MSE and PSNR which only measure pixel differences numerically, SSIM focuses on how images are perceived by humans based on perceptual similarity. The calculation of SSIM can be seen in eq (7).

Vol. 6, No. 2, April 2025, Page. 1029-1040
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4426

$$SSIM\ (x,y) = \frac{(\mu x2+\mu y2+c1)(\sigma x2+\sigma y2+c2)}{(2\mu x\mu y+c1)(2\sigma xy+c2)} \quad (7)$$

3. RESULTS

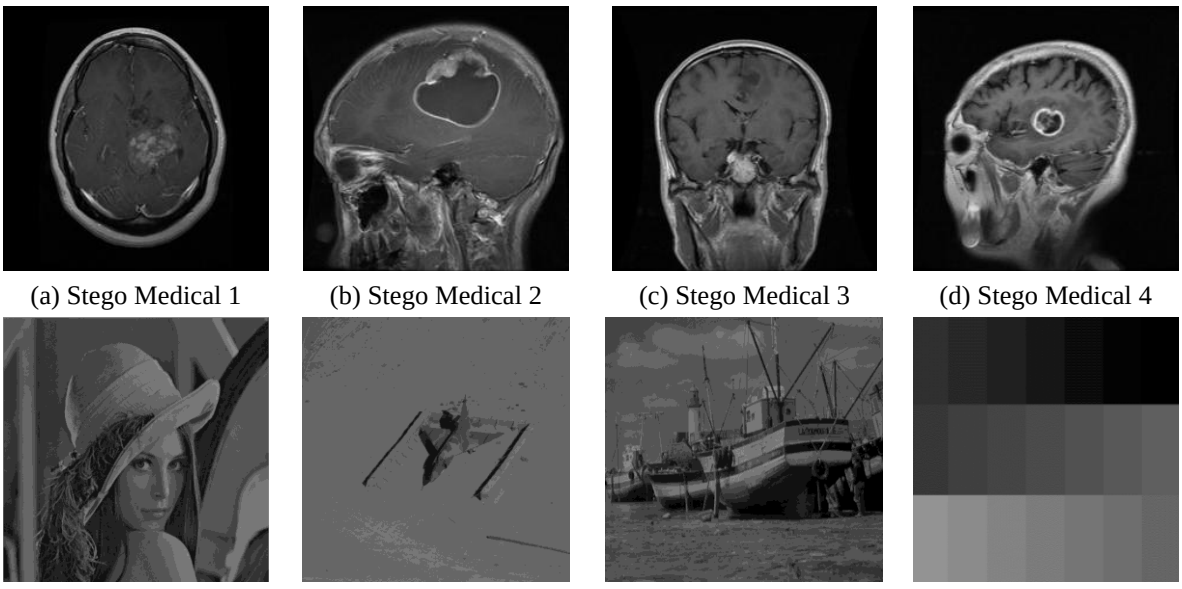
Testing in this study was carried out using MATLAB software version 2024a running on a computer with specifications of an Intel Core i5-12400F processor, NVIDIA RTX 3060 GPU, 2 TB SSD storage, and 32 GB RAM. These specifications were chosen to ensure that the entire computational process, including DWT transformation and SVD decomposition, runs efficiently and supports optimal analysis of steganography results.



(a) Medical 1 (b) Medical 2 (c) Medical 3 (d) Medical 4

(e) Secret 1 (f) Secret 2 (g) Secret 3 (h) Secret 4

Figure 3. Sample data cover image and secret image



(a) Stego Medical 1 (b) Stego Medical 2 (c) Stego Medical 3 (d) Stego Medical 4

(e) Extracted Secret 1 (f) Extracted Secret 2 (g) Extracted Secret 3 (h) Extracted Secret 4

Figure 4. Results of embedded image steganography and extraction of the secret image.

Vol. 6, No. 2, April 2025, Page. 1029-1040
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4426

In this test, the image size used for the cover image and secret image is 512 x 512 pixels each. The visualization of the cover image used can be seen in Figure 3 (a) - (d), while the visualization of the secret image used to be inserted into the cover image is shown in Figure 3 (e) - (h). Based on Figure 4, in parts (a) - (d), the stego image display using a medical image as a cover image is visible. The four stego images have a visualization that is almost identical to the original cover image without any significant changes to the naked eye. This indicates that the applied steganography algorithm has succeeded in maintaining the visual quality of the stego image with a high level of imperceptibility, making it difficult to detect the presence of the inserted secret image.

Meanwhile, parts (e) - (h) show the results of extracting the secret image from the processed stego image. The extracted secret image appears to have been successfully reconstructed, but there is a slight difference in terms of brightness, where the image looks slightly darker than the original secret image. This is likely due to the transformation and reconstruction process involving DWT and SVD, resulting in small changes in pixel intensity values. However, the shape and main information of the secret image can still be recognized well, indicating the success of the algorithm in maintaining the integrity of the embedded data. Furthermore, image quality measurements were carried out to assess the performance of the algorithm in maintaining the visual quality of each cover image using the secret image in (Figure 3 (e) - (h)). This measurement includes an analysis of the level of distortion that occurs in the stego image compared to the original cover image, as well as an evaluation of the success of the algorithm in reconstructing the secret image. The complete results of this measurement can be seen in Table 2.

Table 2. Image quality results for inserting the secret image “Secret 1”

Cover Image	MSE	PSNR	SSIM	Running Time
Medical 1	0.00032	72.811 dB	0.9691	0 Min 36 Sec
Medical 2	0.00012	68.732 dB	0.9428	0 Min 36 Sec
Medical 3	0.00028	68.119 dB	0.9467	0 Min 36 Sec
Medical 4	0.00071	68.036 dB	0.9201	0 Min 37 Sec

Table 3. Image quality results for the “Secret 2” secret image insertion

Cover Image	MSE	PSNR	SSIM	Running Time
Medical 1	0.00021	74.006 dB	0.9610	0 Min 36 Sec
Medical 2	0.00017	74.198 dB	0.9600	0 Min 36 Sec
Medical 3	0.00014	74.721 dB	0.9690	0 Min 36 Sec
Medical 4	0.00022	73.677 dB	0.9687	0 Min 36 Sec

Table 4. Image quality results for inserting the secret image “Secret 3”

Cover Image	MSE	PSNR	SSIM	Running Time
Medical 1	0.00018	72.609 dB	0.9555	0 Min 36 Sec
Medical 2	0.00021	72.160 dB	0.9514	0 Min 36 Sec
Medical 3	0.00041	71.124 dB	0.9573	0 Min 36 Sec
Medical 4	0.00043	72.089 dB	0.9467	0 Min 36 Sec

Table 5. Image quality results for the “Secret 4” secret image insertion

Cover Image	MSE	PSNR	SSIM	Running Time
Medical 1	0.00012	78.081 dB	0.9891	0 Min 36 Sec
Medical 2	0.00010	78.765 dB	0.9834	0 Min 35 Sec
Medical 3	0.00018	78.777 dB	0.9846	0 Min 35 Sec
Medical 4	0.00032	78.321 dB	0.9818	0 Min 35 Sec

Table 2 shows the image quality results in the Secret Image "Secret 1" embedding process using several cover images. From the table, it can be seen that the MSE (Mean Squared Error) value is quite small for all cover images, indicating a very low level of distortion. The PSNR (Peak Signal-to-Noise Ratio) value for all cover images is above 68 dB, indicating very good visual quality in the stego image. However, the difference in SSIM (Structural Similarity Index Measure) values shows that cover images with complex textures, such as Medical 4, have slightly lower SSIM values than Medical 1 or Medical 2. The processing time for all images is relatively consistent, around 36–37 seconds.

Table 3 presents the image quality results for the Secret Image "Secret 2" embedding. Overall, the algorithm performance looks better compared to Table 2, with higher PSNR values for all cover images, reaching more than 73 dB. This shows that the secret image "Secret 2" has a smaller impact on the visual quality of the stego image. In addition, the SSIM value is also more consistent, with all cover images recording values above 0.96. This indicates that the algorithm has successfully maintained the image structure at a higher level. The execution time remains uniform, which is 36 seconds.

Table 4 shows the results of image quality after the insertion of the Secret Image "Secret 3". From these results, the MSE value shows a slight increase in distortion when compared to the previous Secret Image, especially on the cover images Medical 3 and Medical 4. PSNR also shows a slight decrease in both images, although it remains above 71 dB. However, the SSIM value remains quite high, which means that the original image structure can still be maintained well. The processing time remains consistent, indicating the efficiency of the algorithm in data processing.

Table 5 shows the best results among all tests, where the Secret Image "Secret 4" provides the highest PSNR value, reaching up to 78 dB, with a very small MSE on all cover images. SSIM values above 0.98 for all cover images indicate that the structure and visual quality of the image are very well maintained. Differences in brightness and structure are barely visible, thus supporting a high level of imperceptibility. In addition, the processing time is slightly faster for some cover images, such as Medical 2, indicating the potential for optimizing the algorithm for images with certain characteristics.

4. DISCUSSIONS

In this study, the experimental results demonstrate that the proposed DWT-SVD steganographic method successfully embeds secret images into medical cover images while maintaining high imperceptibility and robustness. As shown in Tables 2–5, the method consistently achieves PSNR values above 70 dB and SSIM values exceeding 0.96, indicating that the stego images are visually indistinguishable from the original cover images. The effectiveness of the approach is further validated by its ability to preserve image quality across different medical datasets, making it suitable for telemedicine and AI-assisted diagnostic applications.

Compared to existing steganographic methods, the DWT-SVD approach offers several advantages in imperceptibility and robustness. Previous research using DCT-SVD [16] reported high imperceptibility but suffered from blocking artifacts and lower resistance to compression distortions, which can degrade stego image quality in compressed formats such as JPEG. In contrast, IWT-SVD-based methods [18] demonstrated strong robustness but introduced visible artifacts in images with complex textures, limiting their applicability in medical imaging. SWT-SVD techniques [17] provided higher embedding capacity but significantly increased computational complexity, making them less efficient for real-time applications. The proposed DWT-SVD method addresses these limitations by embedding secret information in the LL sub-band of DWT, ensuring minimal distortion while preserving diagnostic details. Additionally, the integration with SVD enhances resistance against noise and compression, providing a balance between robustness and visual fidelity.

Despite its advantages, the DWT-SVD approach has some limitations. First, the embedding capacity is constrained by the LL sub-band, meaning that while the method ensures high imperceptibility, it may not be suitable for applications requiring high-capacity embedding. Second, the computational complexity of SVD can be a bottleneck when processing high-resolution images, despite optimization efforts to reduce operations in the LL sub-band. Third, while the method performs well in controlled test environments, its robustness in real-world scenarios involving lossy transmission channels or diverse imaging modalities needs further validation.

To further improve steganographic security and efficiency, several enhancements can be considered. One potential improvement is integrating machine learning-based optimization to automate the selection of embedding parameters, thereby optimizing the trade-off between imperceptibility and robustness. Another area of future research is extending the approach to multi-resolution medical images, where different wavelet decomposition levels can be used to adaptively embed information in varying frequency components. Additionally, testing the method on real-world telemedicine systems could provide valuable insights into its practical deployment, especially in AI-driven medical imaging workflows. Lastly, exploring hybrid encryption-steganography frameworks could further enhance security by integrating cryptographic techniques with DWT-SVD-based embedding.

5. CONCLUSIONS

This study successfully implemented a DWT-SVD-based steganography method to enhance the security of medical images while maintaining high imperceptibility and robustness. The proposed approach effectively embeds secret images in the LL sub-band of DWT, minimizing visual distortion while ensuring strong resistance against compression and noise. Experimental results demonstrate that the proposed method achieves a PSNR value of up to 78 dB and an SSIM value approaching 1, indicating that the stego image quality is nearly identical to the cover image, ensuring minimal perceptual distortion. This research contributes to the field of computer science and information security by optimizing transform-based steganography techniques for medical image protection. Unlike DCT-SVD and IWT-SVD methods, which suffer from blocking artifacts and texture distortions, the DWT-SVD approach ensures superior image fidelity and computational efficiency. The ability to maintain high image quality while embedding confidential information makes this method particularly suitable for applications in secure healthcare data management, where both data confidentiality and diagnostic integrity are critical. While the proposed method demonstrates strong performance, some limitations remain, such as limited embedding capacity and computational complexity in high-resolution images. Future research should explore adaptive embedding strategies using machine learning optimization, extend the method to multi-resolution medical images, and evaluate its effectiveness in real-world telemedicine environments. Additionally, integrating cryptographic encryption with steganography could further enhance data security in medical image transmission and AI-assisted diagnostics.

ACKNOWLEDGEMENT

The author would like to express his deepest gratitude to the LPPM of Dian Nuswantoro University (UDINUS) for providing financial support for this research through the Internal Research Scheme with Grant No. 005/A.38-04/UDN-09/I/2025.

REFERENCES

[1] R. Verma, A. Kumari, A. Anand, and V. S. S. Yadavalli, "Revisiting Shift Cipher Technique for Amplified Data Security," Journal of Computational and Cognitive Engineering, vol. 3, no. 1, pp. 8–14, Aug. 2022, doi: 10.47852/bonviewJCCE2202261.

[2] M. S. Abdalzaher, M. M. Fouda, and M. I. Ibrahem, "Data Privacy Preservation and Security in Smart Metering Systems," Oct. 01, 2022, MDPI. doi: 10.3390/en15197419.

[3] E. R. Pramudya et al., "Optimation of image encryption using fractal Tromino and polynomial Chebyshev based on chaotic matrix," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 22, no. 6, p. 1529, Aug. 2024, doi: 10.12928/telkomnika.v22i6.26080.

[4] B. S. Reddy, I. A. Babu, and S. Bachu, "Implementation of Medical Image Watermarking using RDWT and SVD for Secure Medical Data Transmission in Healthcare Systems," in 2022 First International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), 2022, pp. 1–6. doi: 10.1109/ICEEICT53079.2022.9768429.

[5] S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-Naji, and J. Chahl, "Medical Image Encryption: A Comprehensive Review," Aug. 01, 2023, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/computers12080160.

[6] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," Cyber Security and Applications, vol. 2, p. 100031, 2024, doi: 10.1016/j.csa.2023.100031.

[7] T. Alsuwian, A. Shahid Butt, and A. A. Amin, "Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review," Nov. 01, 2022, MDPI. doi: 10.3390/su142114226.

[8] M. J. Altalqani and Z. J. Jaber, "Improving The Security Of Steganography In Video Using Genetic Algorithm," 2021.

[9] B. Abd-El-Atty, M. A. El-Affendi, S. A. Chelloug, and A. A. A. El-Latif, "Double Medical Image Cryptosystem Based on Quantum Walk," IEEE Access, vol. 11, pp. 69164–69176, 2023, doi: 10.1109/ACCESS.2023.3289932.

[10] A. Shafique, J. Ahmed, M. U. Rehman, and M. M. Hazzazi, "Noise-Resistant Image Encryption Scheme for Medical Images in the Chaos and Wavelet Domain," IEEE Access, vol. 9, pp. 59108–59130, 2021, doi: 10.1109/ACCESS.2021.3071535.

[11] A. Alzahrani, "Enhanced Invisibility and Robustness of Digital Image Watermarking Based on DWT-SVD," Appl Bionics Biomech, vol. 2022, 2022, doi: 10.1155/2022/5271600.

[12] Mohammed Hassan Abd and Osamah Waleed Allawi, "Secured Mechanism Towards Integrity of Digital Images Using DWT, DCT, LSB and Watermarking Integrations," Ibn AL-Haitham Journal For Pure and Applied Sciences, vol. 36, no. 2, pp. 454–468, Apr. 2023, doi: 10.30526/36.2.3088.

[13] N. S. Awarayi, O. Appiah, B. A. Weyori, and C. B. Ninfaakang, "A Digital Image Watermarking Using Dwt and L-shaped Tromino Fractal Encryption," International Journal of Image, Graphics and Signal Processing, vol. 13, no. 3, pp. 33–43, Jun. 2021, doi: 10.5815/ijigsp.2021.03.03.

[14] A. O. Mohammed, H. I. Hussein, R. J. Mstafa, and A. M. Abdulazeez, "A blind and robust color image watermarking scheme based on DCT and DWT domains," Multimed Tools Appl, vol. 82, no. 21, pp. 32855–32881, Sep. 2023, doi: 10.1007/s11042-023-14797-0.

[15] J. Khandelwal, V. K. Sharma, D. Singh, and A. Zaguia, "Dwt-svd based image steganography using threshold value encryption method," Computers, Materials and Continua, vol. 72, no. 2, pp. 3299–3312, 2022, doi: 10.32604/cmc.2022.023116.

[16] X. Song, C. Yang, K. Han, and S. Ding, "Robust JPEG steganography based on DCT and SVD in nonsubsampled shearlet transform domain," Multimed Tools Appl, vol. 81, no. 25, pp. 36453–36472, Oct. 2022, doi: 10.1007/s11042-022-13525-4.

[17] R. A. El-Shahed, M. N. Al-Berry, H. M. Ebeid, and H. A. Shedeed, "Multi-resolution Video Steganography Technique Based on Stationary Wavelet Transform (SWT) and Singular Value Decomposition (SVD)," in International Conference on Innovative Computing and Communications, A. Khanna, D. Gupta, S. Bhattacharyya, A. E. Hassanien, S. Anand, and A. Jaiswal, Eds., Singapore: Springer Singapore, 2022, pp. 157–169. doi: 10.1007/978-981-16-3071-2_15.

Vol. 6, No. 2, April 2025, Page. 1029-1040
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.2.4426

[18] A. Durafe and V. Patidar, "Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 7, pp. 4483–4498, Jul. 2022, doi: 10.1016/j.jksuci.2020.10.008.

[19] A. Alzahrani, "Enhanced invisibility and robustness of digital image watermarking based on DWT-SVD," Appl Bionics Biomech, vol. 2022, 2022.

[20] F. Yasmeen and M. S. Uddin, "An Efficient Watermarking Approach Based on LL and HH Edges of DWT–SVD," SN Comput Sci, vol. 2, no. 2, pp. 1–16, Apr. 2021, doi: 10.1007/s42979-021-00478-y.

[21] E. E. D. Hemdan, "An efficient and robust watermarking approach based on single value decompression, multi-level DWT, and wavelet fusion with scrambled medical images," Multimed Tools Appl, vol. 80, no. 2, pp. 1749–1777, Jan. 2021, doi: 10.1007/s11042-020-09769-7.

[22] Y. Xue, K. Mu, Y. Wang, Y. Chen, P. Zhong, and J. Wen, "Robust Speech Steganography Using Differential SVD," IEEE Access, vol. 7, pp. 153724–153733, 2019, doi: 10.1109/ACCESS.2019.2948946.

[23] E. A. Sofyan, C. A. Sari, H. Rachmawanto, and R. D. Cahyo, "High-Quality Evaluation for Invisible Watermarking Based on Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD)," Advance Sustainable Science, Engineering and Technology (ASSET), vol. 6, no. 1, 2024, doi: 10.26877/asset.v6i1.17186.

[24] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," Journal of Computer and Communications, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

[25] C. A. Sari, M. H. Dzaki, E. H. Rachmawanto, R. R. Ali, and M. Doheir, "High PSNR Using Fibonacci Sequences in Classical Cryptography and Steganography Using LSB," International Journal of Intelligent Engineering and Systems, vol. 16, no. 4, pp. 568–580, 2023, doi: 10.22266/ijies2023.0831.46.