Transactions on Machine Intelligence 5(4) (2022) 248-255

ISSN Online: 2821-1693

Transactions on Machine Intelligence

Journal Homepage: https://tmachineintelligence.ir/index.php/TMI

Image Steganography of MRI Using 2D Wavelet Transform

M. Sedaghatian [1,*], M.R. Karami-Mollaei [2]

[1] Department of Biomedical Engineering, Faculty of Electrical and Computer Engineering, Babol Noshirvani University of Technology, Babol, Iran

[2] Associate Professor, Department of Biomedical Engineering, Babol Noshirvani University of Technology, Babol, Iran

ARTICLE INFO

Article History:
Received 29 May 2022
Received in revised form 18 July 2022
Accepted 12 December 2022
Available online 13 December 2022

Keywords:
Steganography, Wavelet Transform, MRI Images, Frequency Domain

ABSTRACT

With the increasing use of the internet and the growing volume of exchanged data, it has become possible to store and send medical information about patients. On the other hand, the use of these methods poses significant risks to the privacy of patient information. Therefore, the use of information hiding techniques, in such a way that the information is not easily detectable or alterable, has become essential. One such method is steganography. In this paper, magnetic resonance imaging (MRI) images are used as hosts for steganographic operations. In the proposed method, all wavelet coefficients of the secret image are embedded in the coefficients of the host image using the suggested α relation. In the experiments conducted, the performance of the wavelet-based steganography in embedding the secret image coefficients into the approximation, horizontal, vertical, and diagonal detail coefficients of the host image at four wavelet decomposition levels are compared. The comparison is performed using the Mean Squared Error (MSE) and Signal to Noise Ratio (SNR) metrics. The results show that steganography at the fourth level of wavelet decomposition, with embedding in the diagonal details, provides the best outcome in terms of both visual and statistical quality.

1. INTRODUCTION

Medical image processing techniques are crucial in disease diagnosis, treatment, education, and research. In disease diagnosis using medical images, personal patient information (such as age, medical history, and gender) and notes from medical staff regarding the patient's condition must be communicated to the physician [1].

Medical images are produced in a standard format called DICOM, which collects such patient information in the image header [2]. On the other hand, with the advancement of communication technologies, it is now possible to store and transmit medical information digitally [3]; however, the use of these methods poses serious risks to the privacy of medical data [4]. Since patient information is standardized and transmitted over the open internet network, there is a risk of deliberate alteration of the data, as it can easily be extracted from the image file [2]. Therefore, it is crucial to use information hiding techniques in such a way that the information is not easily detectable or alterable.

* Corresponding Author: Sedaghatian.mohsen@gmail.com
Department of Biomedical Engineering, Faculty of Electrical and Computer Engineering, Babol Noshirvani University of Technology, Babol, Iran

http://dx.doi.org/10.47176/TMI.2022.248

Steganography, the science of hiding information within other data such that the existence of the information is not apparent, is one of these techniques. Steganography methods are generally classified into two categories: 1) Information hiding, and 2) Steganography [5].

In the first method, known as information hiding, the information is encoded in a way that is incomprehensible to a third party. However, the sender and receiver can decrypt the information using a shared key. This method, however, reveals the existence of hidden information to a third party, and since it does not resemble the original image before decryption, it can be replicated and distributed illegally after decryption. Therefore, it is not always sufficient or effective for protecting data in some cases, and encryption is typically used to protect data during transmission from sender to receiver. This is why, instead of encryption, methods like steganography are used [5]. Steganography involves embedding information within an image to transfer it covertly or to prove ownership of the image in a way that does not alter the image in a perceptible way [6]. Therefore, there is a need to improve the security of medical systems. Digital steganography technology embeds personal patient information into medical images as a steganographer [7].

Three important factors in steganography methods are: capacity, security, and reliability. Among these, reliability is the most significant. In the context of image steganography, methods can be categorized based on where the data is added to the image or whether the image is required at the receiver's end. Steganography methods are divided into two categories: spatial domain methods and transform domain methods [8].

2. RELATED SCIENTIFIC RESEARCH

Information can be hidden in an image using various methods. By encoding each bit of information and data, it can be directly embedded in the image. In more advanced methods, information can be placed only in parts of the image with higher complexity to draw less attention. Information can also be distributed randomly within the image [9].

There are various steganographic methods, each utilizing different domains to ensure the protection of medical images and the retrieval of degraded images. Steganographic methods are classified based on the domain in which the steganographer is used, into spatial and frequency domains [10]. Spatial domain methods modify pixel values directly, while frequency domain methods involve transformations either locally or globally [11].

2.1. Spatial Domain Methods

In this method, the key is embedded in the host image by modifying its pixels or features. The algorithm must carefully weigh the number of bits altered in the pixels to minimize the visibility of the embedded key [12].

2.1.1. LSB Insertion Method

One of the most well-known spatial domain methods is the LSB (Least Significant Bit) method, in which information is embedded in the least significant bits of the image [13]. The main feature of this method is that it does not cause any visible changes in the image. However, a significant drawback of this method is its low resistance to various attacks or processing, such as compression, scaling, and smoothing [14].

2.2. Frequency Domain Methods

Frequency domain methods are more commonly used than spatial domain methods. The goal of these methods is to embed information into the frequency coefficients of the image. The most commonly used transforms in this method are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT). Both Discrete Wavelet Transforms and Discrete Cosine Transforms have been effectively used in digital image steganography. Additionally, Singular Value Decomposition (SVD) is also effectively used in image steganography [15].

2.2.1. Discrete Fourier Transform (DFT) Method

The DFT method has an advantage over spatial domain methods. First, this method is invariant to translation and resistant to rotation, which provides high resistance against geometric attacks [16]. On the other hand, Fast Fourier Transform (FFT) methods introduce rounding errors, which can lead to a loss of quality and errors in key extraction [17].

2.2.2. Discrete Cosine Transform (DCT) Method

The Discrete Cosine Transform (DCT) is similar to the Discrete Fourier Transform (DFT) and is a technique for converting a signal into its primary frequency components. The 2D DCT of a given matrix produces frequency coefficients in another matrix. The upper-left corner of the matrix represents the lowest frequency components, while the lower-right corner represents the highest frequency components. Steganography using DCT methods is more resistant compared to spatial domain methods. Such algorithms are resistant to image processing operations such as low-pass filtering, brightness and contrast adjustment, blurring, and so on. However, they are weak against geometric attacks like rotation, scaling, cropping, and others. DCT-based steganography can be divided into global DCT steganography and block-based DCT steganography. In global DCT steganography, the transform is applied to the entire image, and the image is divided into separate spectral regions based on their energy [18].

3. PROPOSED METHOD

The Discrete Wavelet Transform (DWT) is a mathematical tool used for hierarchical decomposition of an image. This method is widely applied in signal processing applications such as audio and video compression, noise removal from sound, and wireless antenna simulation. The wavelet transform provides both frequency and spatial representations of the image.

In the two-dimensional DWT, the image is decomposed into four sub-images: CA, CH, CV, and CD. CA represents the approximation of the image, i.e., the low-frequency components (approximation coefficients). CH, CV, and CD represent the details of the image, i.e., the high and mid-frequency components. Specifically:

- **CH** denotes horizontal details (horizontal coefficients, mid-frequency),
- **CV** denotes vertical details (vertical coefficients, mid-frequency),
- **CD** denotes diagonal details (diagonal coefficients, high-frequency).

The size of each of these matrices is half that of the original image.

This transform decomposes the image into a lower-resolution image (LL) and detail components: horizontal (HL), vertical (LH), and diagonal (HH) components, creating a multi-resolution representation (as shown in Figure 1). Due to this feature, the key can be placed in any frequency band, and during the inverse transform, the key will be distributed across both high and low-frequency domains, much like in the time domain.

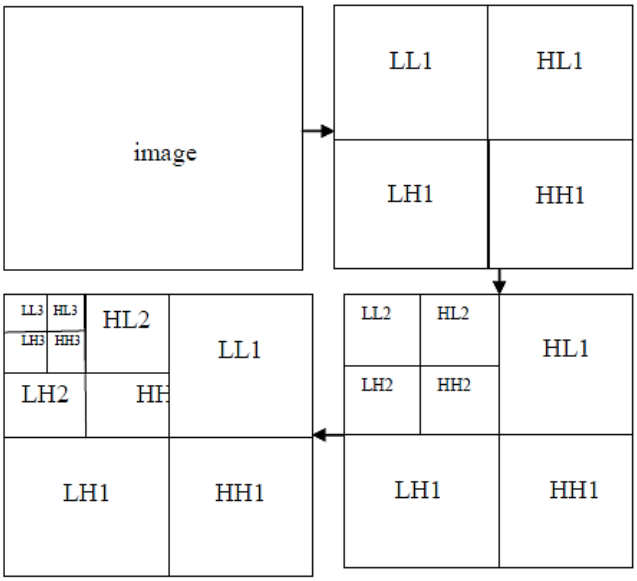

Fig. 1. Discrete Wavelet Transform Scaling

Placing information in low frequencies causes a noticeable degradation in image quality, which becomes perceptible to the human eye. On the other hand, low frequencies are not suitable for embedding information due to their sensitivity to noise. Thus, the ideal choice for embedding data lies in the mid-frequencies. Mid-frequency bands modify the appearance of the image only slightly and are less susceptible to noise [19].

In our approach, for steganography, we first apply a multi-level discrete wavelet transform (DWT) to the host image and extract its approximation and detail coefficients. This process is repeated for the key image as well.

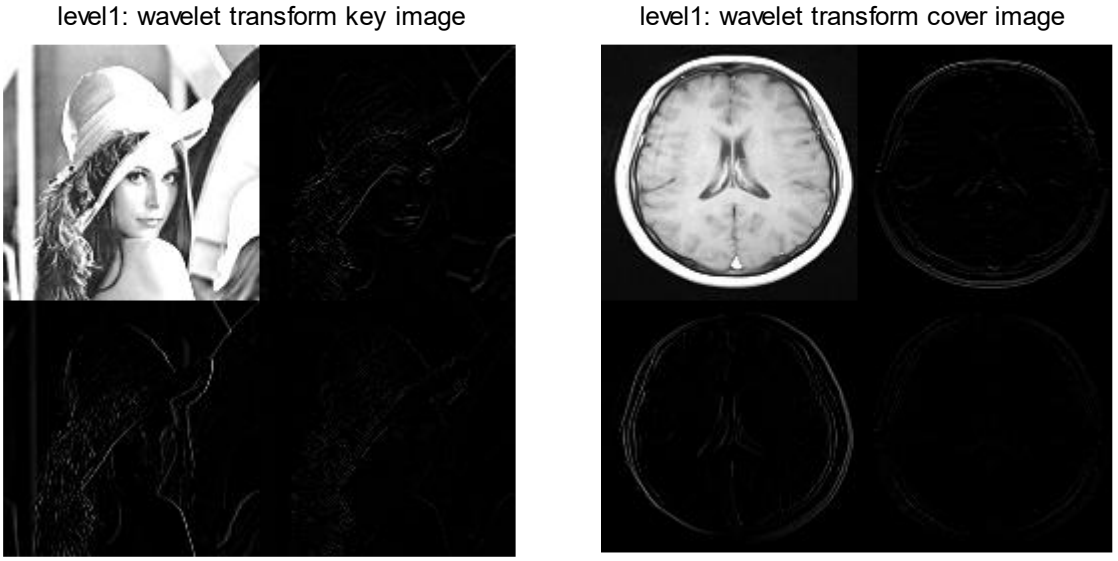

Fig. 2. Overview of the image below the band. a) Host image, b) Key image.

The holography process is then carried out using the alpha blending method [20]. This relationship is expressed as follows:

$$WMI = X \times (LLn) + Y \times (WMn) \quad (1)$$

The WMI is the holographed image, LLn is the approximation of the host image, WMn is the approximation of the key image, and x, y are the scaling coefficients.

After holography, the image is transformed back to the spatial domain using the inverse wavelet transform. In order to recover the hidden message in the host image, we take the wavelet transform of the existing image and use the following relationship to extract the desired key:

$$RW = \frac{(WMI - X \times LLn)}{Y} \quad (2)$$

RW is the extracted key image in the frequency domain.

To obtain the message image in the spatial domain, we apply the inverse wavelet transform to RW.

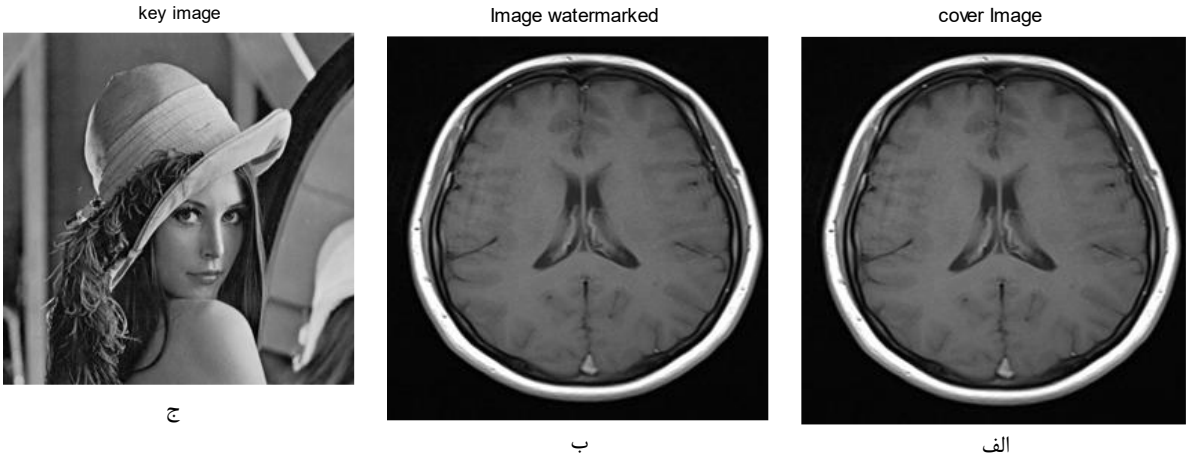

Fig. 3. Illustration of the proposed method for holography applied to a database image. a) Host image, b) Holographed image, c) Key image.

4. RESULTS

In this paper, MRI images have been used as the host image in the holography method. The database images are available for online access. To evaluate the quality of the holographed image, two criteria were used: mean squared error and signal-to-noise ratio. The relationship between these two criteria is as follows:

$$MSE = \frac{\sum_{M,N}[I1(m,n) - I2(m,n)]^2}{M \times N} \quad (3)$$

Here, M and N represent the number of rows and columns, respectively.

$$PSNR_{dB} = 10\, log_{10} \frac{(2^n - 1)^2}{MSE} \quad (4)$$

The results obtained using the above criteria for holography in each of the wavelet coefficients are shown in the tables below. Analyzing the results reveals that holography in the diagonal detail component yields lower error and higher signal-to-noise ratio. Additionally, by examining the above criteria for different wavelet transform levels, we concluded that increasing the level also leads to better holography quality. The results regarding this matter are presented in the tables below.

Table 1. Evaluation of the Proposed Holography Method Using MSE and PSNR Criteria at Four Wavelet Levels for the Approximation Matrix and Horizontal Detail Components

Approximation	PSNR	MSE
Level 1	95.311	1.914046e-05
Level 2	95.377	1.885963e-05
Level 3	95.485	1.838792e-05
Level 4	95.628	1.779377e-05
Horizontal Details	**PSNR**	**MSE**
Level 1	121.679	4.424e-08
Level 2	127.535	1.146e-08
Level 3	133.810	2.704e-09
Level 4	139.794	6.814e-10

Table 2. Evaluation of the Proposed Steganography Method Using MSE and PSNR Criteria at Four Wavelet Levels for the Vertical and Diagonal Detail Matrices

Vertical Details	PSNR	MSE
Level 1	117.94	1.043e-07
Level 2	121.88	4.216e-08
Level 3	126.82	1.349e-08
Level 4	132.19	3.920e-09
Diagonal Details	**PSNR**	**MSE**
Level 1	126.10	1.59394e-08
Level 2	128.99	8.20338e-09
Level 3	136.75	1.37344e-09
Level 4	142.55	3.60668e-10

5. CONCLUSION

With the expansion of the ability to send patients' medical information through virtual space, the need to protect medical data has increased. One way to prevent malicious alteration of patient information is through holography. In this paper, wavelet transform was used for holography of MRI images. The alpha blending relationship was used to embed the key image within the wavelet coefficients of the host image. Analysis of the results based on the MSE and PSNR criteria showed that holography in the diagonal coefficients and higher wavelet levels provides better quality both visually and statistically.

Transparency Statement

The data supporting this study are available upon reasonable request to the corresponding author, subject to ethical and confidentiality considerations.

Acknowledgments

We would like to express our gratitude to all individuals who contributed to this project.

Declaration of Interest

The authors declare that they have no competing interests.

Funding

This research received no specific grant from any funding agency, commercial, or not-for-profit sectors.

REFERENCES

[1] Ahsan, M., & Siddique, Z. (2021). Machine-learning-based disease diagnosis: A comprehensive review. *Healthcare, 10*. https://doi.org/10.3390/healthcare10030541

[2] Li, X., Morgan, P., Ashburner, J., Smith, J. C., & Rorden, C. (2016). The first step for neuroimaging data analysis: DICOM to NIfTI conversion. *Journal of Neuroscience Methods, 264*, 47-56. https://doi.org/10.1016/j.jneumeth.2016.03.001

[3] Kaur, S., Singhal, R., Farooq, O., & Ahuja, B. S. (2010). Recent trends in information, telecommunication and computing (ITC). *International Conference on 2010, 140-144.* https://doi.org/10.1109/ITC.2010.96

[4] Navas, K., & Sasikumar, M. (2007). *Proceedings of the International Conference on Sciences of Electronics, Technologies of Information and Telecommunications*, 25-29.

[5] Pastorfide, E., & Flores, G. (2008). An image steganography algorithm for 24-bit color images using edge-detection filter.

[6] Li, H., Song, W., & Wang, S. (2006). *18th International Conference on Pattern Recognition (ICPR'06)*, 639-642.

[7] Abdulla, A. A., Sellahewa, H., & Jassim, S. (2019). Improving embedding efficiency for digital steganography by exploiting similarities between secret and cover images. *Multimedia Tools and Applications, 78*, 17799-17823. https://doi.org/10.1007/s11042-019-7166-7

[8] Thangavel, P., & Kumaran, T. (2007). *IEEE International Symposium on Industrial Electronics*, 1755-1760. https://doi.org/10.1109/ISIE.2007.4374871

[9] Wu, Y., & Wu, W. (2021). Combinations of superior inorganic phosphors for level-tunable information hiding and encoding. *Advanced Optical Materials, 9.* https://doi.org/10.1002/adom.202100281

[10] Zain, J. M., & Fauzi, A. R. (2007). *29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 5661-5664. https://doi.org/10.1109/IEMBS.2007.4353631

[11] Hassan, M. H., & Gilani, S. (2006). *World Academy of Science, Engineering and Technology, 19*, 39-43. https://doi.org/10.1088/2058-7058/19/11/38

[12] Arnold, M., Schmucker, M., & Wolthusen, S. D. (2002). *Techniques and applications of digital watermarking and content protection*. Artech House.

[13] Johnson, N. F., & Katzenbeisser, S. (2000, May). A survey of steganographic techniques. *Information Hiding*, 43-78.

[14] Zain, J. M., & Clarke, M. (2011). Reversible region of non-interest (RONI) watermarking for authentication of DICOM images. *arXiv preprint arXiv:1101.1603*.

[15] Singh, Y. S., Devi, B. P., & Singh, K. M. (2013). A review of different techniques on digital image watermarking scheme. *International Journal of Engineering Research, 2*(3), 194-200.

[16] Poljicak, A., Mandic, L., & Agic, D. (2011). *Journal of Electronic Imaging, 20*, 033008-033008-033008. https://doi.org/10.1117/1.3609010

[17] Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2010). *Signal Processing, 90*, 727-752. https://doi.org/10.1016/j.sigpro.2009.08.010

[18] Wu, C.-F., & Hsieh, W.-S. (2000). *IEEE Transactions on Consumer Electronics, 46*, 87-94. https://doi.org/10.1109/30.826385

[19] Langelaar, G. C., Setyawan, I., & Lagendijk, R. L. (2000). *IEEE Signal Processing Magazine, 17*(5). https://doi.org/10.1109/79.879337

[20] MaruthuPerumal, S., & VijayaKumar, V. (2011). *International Journal of Computer Applications, 15*, 29-36. https://doi.org/10.5120/1926-2571