HIDING PATIENT INFORMATION INTO MAGNETIC RESONANCE IMAGES USING DNA BASED WAVELET TRANSFORM

Rukiye Karakis, Kali Gurkahraman, Burhanettin Cigdem, Ibrahim Oztoprak and A. Suat Topaktas

Cumhuriyet University, Turkey

Steganography techniques for medical images are alternatives to cryptology, which embed the patient personal information, health reports or other biological signals into the medical images. These methods can be categorized into the least significant bit (LSB) based, the region of non-interest (RONI) based, and the reversible steganography. LSB based method in the spatial domain has high imperceptibility and embedding capacity but it is vulnerable against steg-attacks. RONI based steganography is performed in the spatial or transform domain, whose capacity depends on the RONI area size of a medical image. Reversible steganography in spatial domain reconstructs the original medical image after embedding patient data. This study aims to secure patient personal information in the file headers of medical images against steg-attacks with a new stego system. In the message preprocessing, it is encrypted by DNA encoding and then it is compressed by Huffman compression to increase complexity and the embedding capacity. The message is embedded by Discrete Wavelet Transform and Singular Value Decomposition. 20 patients' cover and stego Magnetic Resonance Images (MRIs) with different size are compared by structural similarity measure (SSIM), universal quality index (UQI), and peak signal-to-noise ratio (PSNR) to determine the quality of the proposed stego system.

Keywords: Medical image steganography, Wavelet transform, DNA encryption, Huffman.

Introduction

An electronic personal health record (EPHR) includes a lot of information about the patient such as personal data, medical history, diagnosis and medications, and medical test reports etc. As a result of technological advances in health, patient's EPHR is made easily accessible on open networks. Since patient data is so valuable to cyber-criminal, there is a life-threatening risk for patients [1-7].

Medical image (X-ray, computed tomography (CT), magnetic resonance imaging (MRI), ultrasound, etc.) is used as a non-invasive method to assist diagnosis or treatment of an illness. In a picture archiving and communication system (PACS) system, medical images are stored and exchanged by a Digital Imaging and Communications in Medicine (DICOM) file format standard which has a file header and image pixels [1, 8-11]. The file header of DICOM has patient information such as name, ID, birth date, age, gender, weight, and address with other image information details. There are many non-commercial applications to process and preserve medical images in DICOM format. A DICOM viewer also demonstrates patient information into the file header of DICOM. According to health standard, patient personal data into DICOM file needs to be protected against cyber-attacks [8-11].

For this reason, DICOM files are encrypted by a symmetric, asymmetric, or hashing encryption when transferring in local or open networks. Furthermore, steganography is also an alternative method to ensure the security of medical images [1, 6-7].

Steganography is a data hiding science which uses a text, image, or video file as a cover object to embed a secret message [1, 12]. The achievement of the steganography is related to the imperceptibility of the message, the capacity, and robustness of the system [1, 6-7, 12]. In image steganography, the embedding process is performed in the spatial domain or transform domain. Spatial domain techniques (LSB embedding, palette sorting, histogram shifting methods, and etc.) are vulnerable to compression, filtering, and geometric distortion. However, transform domain techniques (Discrete Cosine Transform-DCT, Discrete Fourier Transform-DFT, and Discrete Wavelet Transform-DWT) are quite robust against the same attacks [1,12-19].

In medical image steganography, patient personal information, health reports or other biological signals are embedded into the medical images. In literature, medical image steganography methods can be categorized into the least significant bit (LSB) based, the region of non-interest (RONI) based, and the reversible steganography. LSB based method in the spatial domain has high imperceptibility and embedding capacity but it is vulnerable against steg-attacks. RONI based steganography is performed in the spatial or the transform domain, whose capacity depends on RONI area size of the medical image. Reversible steganography in spatial domain reconstructs the original medical image after embedding patient data, and the high embedding message capacity affects its imperceptibility [1, 6-7, 13-19].

This study aims to secure patient personal information into the file headers of medical images with a new stego system to ensure imperceptibility and robustness against steg-attacks. First, the embedding message is encrypted by DNA encoding and then it is compressed by Huffman compression to increase complexity and the embedding capacity. Second, DICOM images are decomposed into four subbands which are LL (approximation), LH (horizontal), HL (vertical) and HH (diagonal). Singular values of LL band are used to hide the message.

Material and Methods

In this study, 20 patients' three MR images with 512x512 and 16 bit were obtained from the Medicine Faculty of Cumhuriyet University (Project No: Tekno-017). Matlab Platform was used to code and test the proposed method. The embedding message was each gathered from the file headers of DICOM images separately. It included patient's personal information (name, id, birth date, sex, age, weight, and address), study information (date, time, id, modality, and description), and series information (date, time, and description).

The embedding stage of the proposed method can be shown in Figure 1. First, the message was encoded by DNA encryption with a 128-bit stego-key of expert doctor and then the encrypted message was compressed by Huffman lossless compression method. Second, the embedding message was converted into two-dimensional matrices by using the size of the cover image. Third, the cover DICOM image file and the message were decomposed into subbands by DWT method. The embedding was generated by adjusting the singular values LL subbands of the cover image with the message's singular values. In the proposed stego system, patient personal information was deleted from the header of the stego DICOM image.

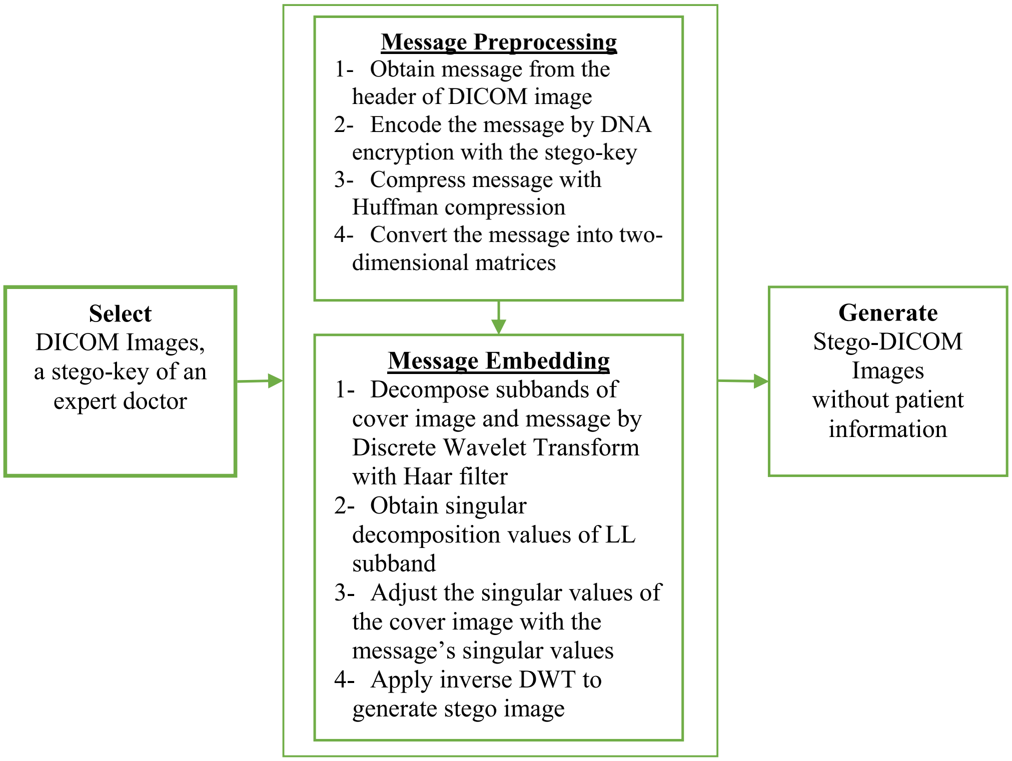
Select
DICOM Images,
a stego-key of an
expert doctor
Message Preprocessing
1- Obtain message from the header of DICOM image
2- Encode the message by DNA encryption with the stego-key
3- Compress message with Huffman compression
4- Convert the message into two-dimensional matrices
Message Embedding
1- Decompose subbands of cover image and message by Discrete Wavelet Transform with Haar filter
2- Obtain singular decomposition values of LL subband
3- Adjust the singular values of the cover image with the message's singular values
4- Apply inverse DWT to generate stego image
Generate
Stego-DICOM
Images
without patient
information

Figure 1. Message embedding stage of the proposed method

The extracting message stage can be shown in Figure 2. First, the subbands were obtained from stego DICOM image by DWT. The singular values of LL subband were decomposed and then they were used to extract the hidden message with inverse DWT. The extracted message was decompressed by Huffman compression and it was decrypted by DNA decoding. Expert doctor with the stego-key can only analysis patient information after the extracting message.

The quality of the proposed system is determined by structural similarity measure (SSIM), universal quality index (UQI), and peak signal-to-noise ratio (PSNR) between the cover and stego DICOM images. The details of these methods can be found in [1, 19].

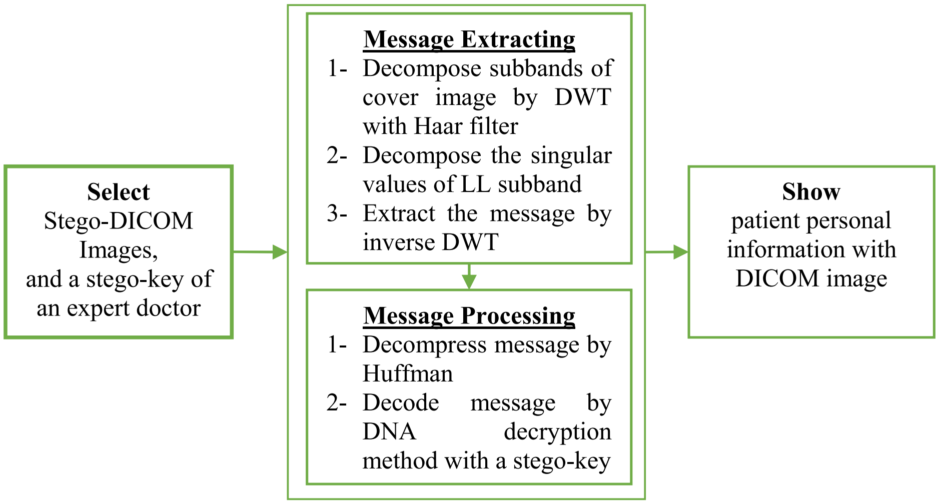
Select
Stego-DICOM
Images,
and a stego-key of
an expert doctor
Message Extracting
1- Decompose subbands of cover image by DWT with Haar filter
2- Decompose the singular values of LL subband
3- Extract the message by inverse DWT
Message Processing
1- Decompress message by Huffman
2- Decode message by DNA decryption method with a stego-key
Show
patient personal
information with
DICOM image

Figure 2. Message extracting stage of the proposed method

1. Discrete Wavelet Transform (DWT)

DWT gives both temporal and frequency information with using multiple filters. In DWT, the detail coefficients of the image are found by the high-pass filter (H), and the approximation coefficients of the image are extracted by the low-pass filter (L), as it can be shown in Figure 3. Two level decomposition of the DWT gives four subbands which are LL (approximation), LH (horizontal), HL (vertical) and HH (diagonal). LL subband ensures to reconstruct the image by inverse DWT. The formula of DWT is represented in Eq. 1 and Eq.2 for an image [19-20].

$$W_{\varphi}(j_0,m,n)=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\varphi_{j_0,m,n}(x,y) \tag{1}$$

$$W_{\psi}^{i}(j,m,n)=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\psi_{j_0,m,n}^{i}(x,y) \tag{2}$$

Where f is an image with m x n size. In Eq.1, $W_{\varphi}(j_0,m,n)$ represents the approximation of the image. $W_{\psi}^{i}(j,m,n)$ gives the horizontal, vertical and diagonal details [19-20].

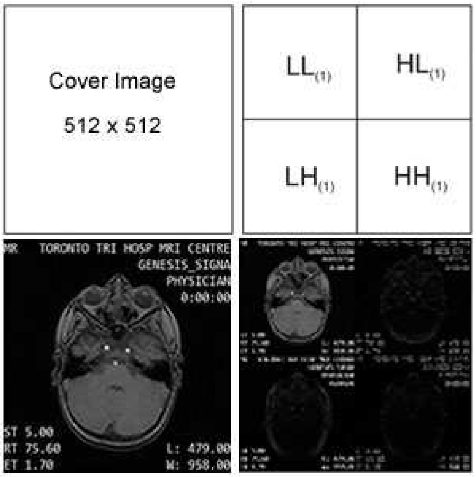

Figure 3. Two level decomposition process of DWT with low and high-pass filters

2. DNA Encryption

DNA encryption is a hiding data in terms of DNA sequence. A human deoxyribonucleic acid (DNA) has four bases which are adenine (A), cytosine (C), guanine (G), and thymine (T). In DNA encryption, each letter of a message is converted into four bases of DNA [21-22].

The steps of the DNA encryption used in the study are given below.

i. Encode bit values of the message as A (00), T (01), C (10) and G (11).
ii. Create the one-time key (OTP) by using stego key of expert doctor and convert it into DNA bases.
iii. Generate the bit values of the message
iv. Encrypt the message with OTP key:

If binary data is ‘0’, transfer the first base of OTP without changing.

If binary data is ‘1’, transfer the first base of OTP with changing (A pairs with T, G pairs with C)

OTP key is	: TCAGAGTT
Message bits	: 01010101…
Encrypted Message	**: TGACACTA**

The steps of the DNA decryption used in the study are given below.

i. Convert encrypted message into DNA bases.
ii. Convert the OTP key into DNA bases.
iii. Compare encrypted message with the OTP key:

If the base of message and OTP key is the same, the bit of the decrypted message is assigned as 0.

If the base of message and OTP key is the difference, the bit of the decrypted message is assigned as 1.

OTP key is	: TCAGAGTT
Encrypted Message	: TGACACTA
Decrypted Message bits	**: 01010101**

Results and Discussion

The differences between cover and stego MR images can be given in Figure 4, Figure 5 and Figure 6. The proposed stego system ensures the imperceptibility. Furthermore, patient personal information was deleted from stego DICOM images, and expert doctor with a stego-key can only analyze it. As it can be seen in Figure 3, 4 and 5, there is no significant difference between the histograms of cover and stego images.

The performance of the proposed stego system was evaluated by PSNR, SSIM, UQI metrics. The mean PSNR values of 20 patients are given in Figure 6. These values changed between 55.18 and 56. 81 dB (decibel). In literature, PSNR values have to be higher than 35 dB to achieve imperceptibility [1, 19].

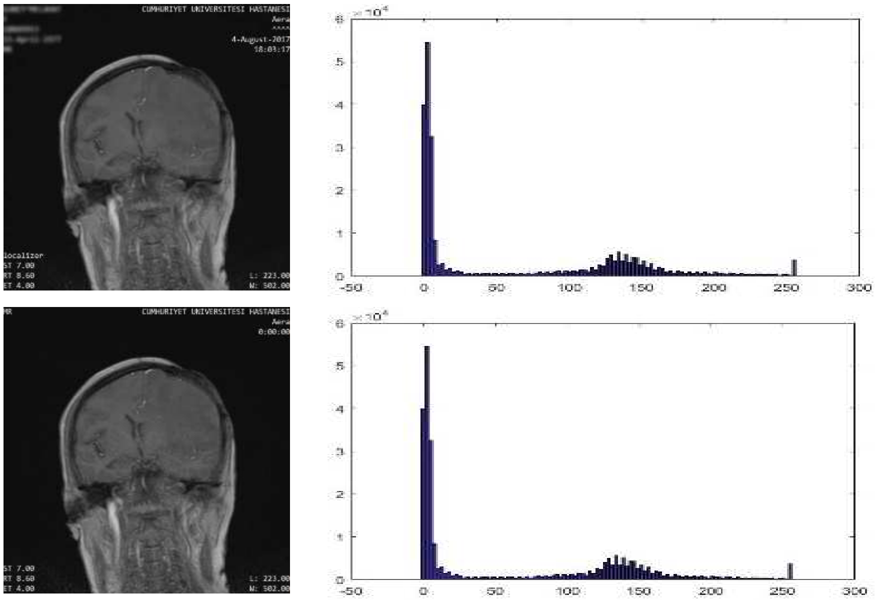

Figure 3. (a) Cover image and its histogram (b)Stego image and its histogram

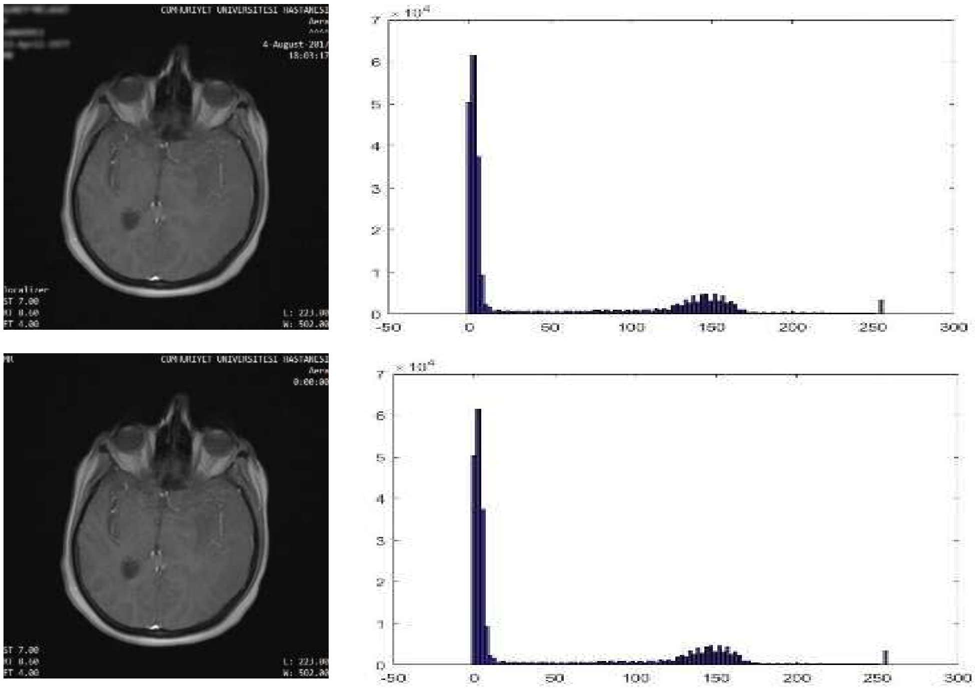

Figure 4. (a) Cover image and its histogram (b)Stego image and its histogram

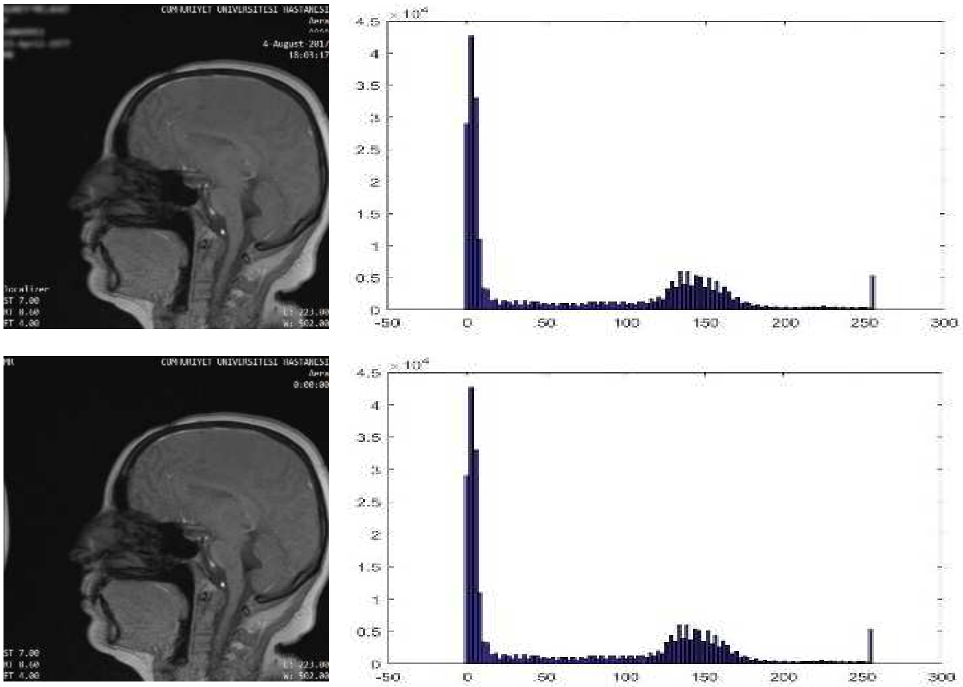

Figure 5. (a) Cover image and its histogram (b)Stego image and its histogram

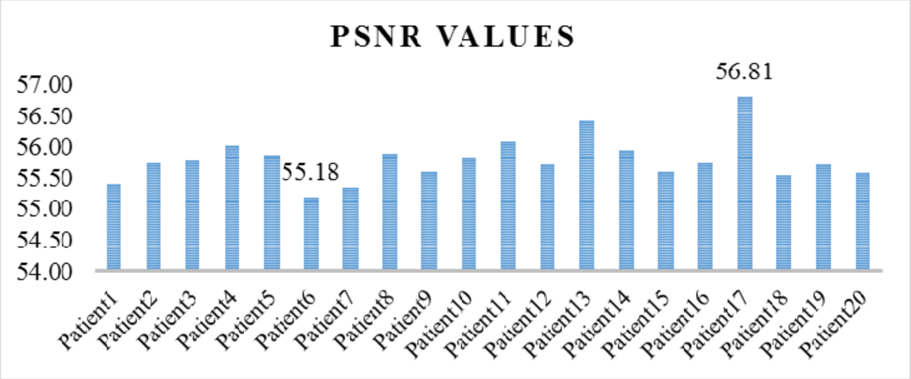

Figure 6. The mean of PSNR values between stego and cover MR images.

The mean UQI values of the proposed stego system ranged between 0.82563 and 0.99996, as it can be seen in Figure 7. The mean SSIM values of DICOM images in Figure 8 are found between 0.999879 and 0.999989. According to the obtained performance results, the proposed stego sytem has high imperceptibility and robustness against the steg-attacks because the embedding process is generated in the transform domain with discrete wavelet.

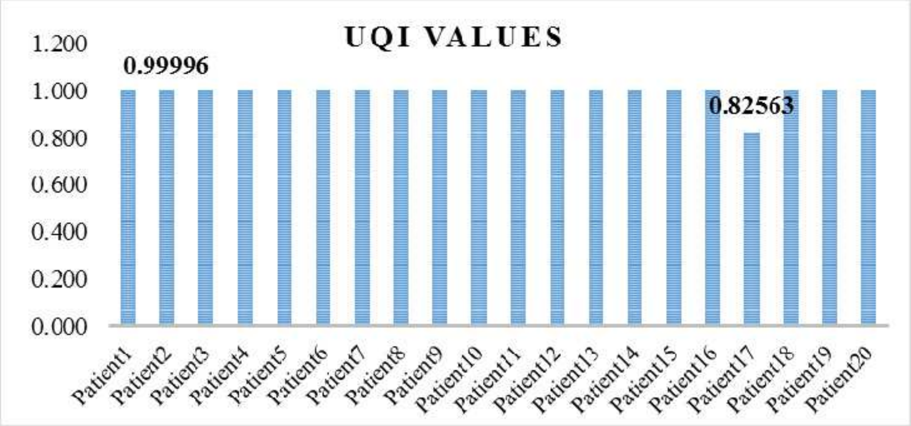

Figure 7. The mean of UQI values between stego and cover MR images.

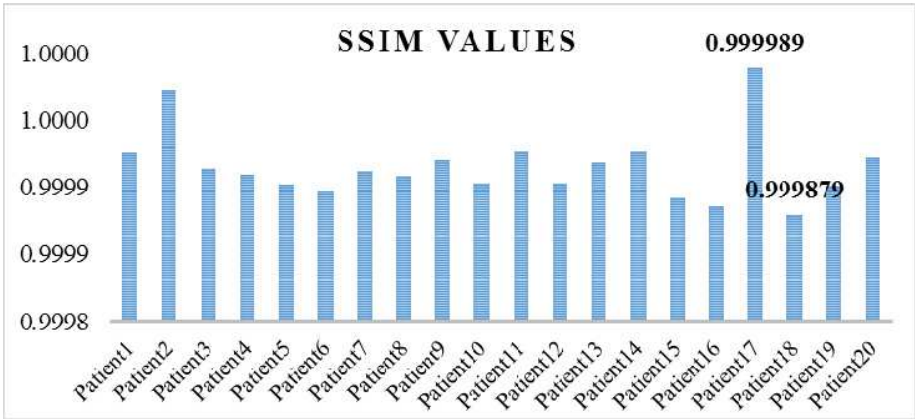

Figure 8. The mean of SSIM values between stego and cover MR images.

Conclusion

In this study, a new stego system is proposed to ensure the patient personal information in the header of DICOM images. For this reason, DWT and SVD methods were combined to embed the message into images. It also assured the robustness of the embedding process. The message was encoded by DNA encoding to develop an unbreakable system and it was compressed by Hufmann to increase the message complexity. Three MR images of 20 patients are used to evaluate the proposed stego system with the performance metrics as PSNR, UQI, and SSIM values. According to the obtained results, the proposed stego system can be used to secure patient personal information into DICOM images.

Acknowledgement

This study has been supported by Cumhuriyet University Scientific and Research Project Fund (Project No: TEKNO-017).

References

1. Karakış, R., Güler, Çapraz, İ., Bilir, E. (2015). A Novel Fuzzy Logic-Based Image Steganography Method to Ensure Medical Data Security, Computers in Biology and Medicine, 67: 172–183, 2015.
2. Internet: Electronic Health Record, http://en.wikipedia.org/wiki/Electronic_health_record (2018, July 31).
3. Internet: Electronic Health Records Overview, http://www.himss.org/files/HIMSSorg/content/files/Code%20180%20MITRE%20Key%20Components%20of%20an%20EHR.pdf (2018, July 31).
4. Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y., Collorec, R. (2000). Relevance of Watermarking in Medical Imaging, Information Technology Applications in iomedicine, 2000. Proceedings. 2000 IEEE EMBS International Conference on, 250-255.
5. Internet: https://www.benton.org/headlines/medical-data-has-become-next-cybersecurity-target (2018, July 31).
6. Nyeem, H., Wageeh Boles, W., Colin Boyd, C., (2013). A Review of Medical Image Watermarking Requirements for Teleradiology, J. Digit. Imaging, 26, 326-343.
7. Coatrieux, G., Lecornu, L., Sankur, B., Roux, C. (2006). A Review of Image Watermarking Applications in Healthcare, Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE, 4691-4694.
8. Internet: About DICOM, The National Electrical Manufacturers Association (NEMA), http://medical.nema.org/Dicom/about-DICOM.html (2018, July 31).
9. Haidekker, M. (2011). Image Storage, Transport, and Compression, Wiley-IEEE Press, Edition: 1, 386-412.
10. Kuang, L.-Q., Zhang, Y., Han, X. (2009). Watermarking Image Authentication in Hospital Information System. Information Engineering and Computer Science, 2009. ICIECS 2009, 1-4.
11. Internet: Oosterwijk, H. (2010). The DICOM standard, overview and characteristics, http://www.ringholm.com/docs/02010_en.htm (2017, April 19).
12. Cheddad, A., Condell, J., Curran, K., McKevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, 90, 727–752.
13. Navas, K. A., Sasikumar, M. (2007). Survey of Medical Image Watermarking Algorithms. SETIT 2007 4rth International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, TUNISIA, 1-6.
14. Golpira H., Danyali, H. (2010). Reversible blind watermarking for medical images based on wavelet histogram shifting, IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), 31–36.
15. Fallahpour, M., Megias, D., Ghanbari, M. (2011). Reversible and high-capacity data hiding in medical images, Image Processing, IET, 5 (2), 190-197.
16. Raul, R.-C., Claudia, F.-U., Trinidad-Bias, G.J., (2007). Data Hiding Scheme for Medical Images, Electronics, Communications and Computers, 2007. CONIELECOMP '07. 17th International Conference on, 32-37.

17. Ravali, K., Kumar A.P., Asadi, S., (2011). Carrying Digital Watermarking for Medical Images using Mobile Devices, IJCSET, 1 (7), 366-369.
18. Karakis R., Gurkahraman K. (2017). An Implementation of DNA based Security Model in Medical Data. The 3th International Conference on Engineering and Natural Sciences (ICENS 2017), 1105-1110.
19. Karakis R., Guler I. (2018). Steganography and Medical Data Security, Cryptographic and Information Security Approaches for Images and Videos (Ed. S. Ramakrishnan, CRC Press, ISBN 9781138563841.
20. Gonzales, R., Woods, R. E., (2008). Digital Image Processing, Pearson Prentice Hall, USA.
21. Wang, Z., Zhao, X., Wang, H., Cui G. (2013). Information hiding based on DNA steganography. 2013 IEEE 4th International Conference on Software Engineering and Service Science, 946- 949.
22. Thiruthuvadoss, A.P. (2012). Comparison and Performance Evaluation of Modern Cryptography and DNA Cryptography, Royal Institute of Technology, Masters of Science.