Biomedical & Pharmacology Journal, June 2018. Vol. **11**(2), p. 863-870

Joint Digital Water Marking for Medical Images for Improving Security

K.J. Kavitha[1]* and Priestly B Shan[1,2]

[1]Department of ECE, Jain Institute of Technology, Davangere, VTU,Karnataka & Research Scholar,CSE Dept,Sathyabama University, Chennai, India.
[2]Principal, Eranad Knowledge City-Technical Campus, Manjeri, India.
*Correspondence author E-mail: kavithakj192@gmail.com

http://dx.doi.org/10.13005/bpj/1443

(Received: 04 May 2018; accepted: 16 May 2018)

Digital watermarking is one of the most efficient techniques to provide the highest secureness to the transmission of data like images or videos over the internet. Quite over the medical data which incorporates the EHR (Electronic Health Record) and medical images and conjointly the military data are crucial whose protection and privacy is extremely a lot of essential issues. To secure this data, the Digital watermarking plays a major role so that it will guarantee authentication, integrity, confidentiality and reliability. In the case of medical images, even a small change or modifications are strictly prohibited as it might lead to the incorrect diagnosis of the disease. Therefore, securing medical image is extremely essential. So as to provide high security for each patient's data and also the various medical scanning images, we can employ the Digital Water Marking (DWM) technique. The DWM technique may be implemented in two ways: Spatial domain technique and Frequency domain technique. Although the spatial implementation is extremely straightforward and a very simple method, most of the implementations are done using frequency or transform/remodel domain strategies since it provides additional details and high effectiveness. The DWM may be implemented using numerous transform/remodel techniques like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), also with the combination of these remodel techniques. Nowadays the work is also extended using a combination of transforming/remodel and spatial domain techniques. In this article the Digital Water Marking is being implemented by employing a combination of a transform technique DWT and a spatial domain technique SVD to provide security to the medical images and also the system efficiency is checked for numerous attacks.

Keywords: DCT, DWT, IWT, SVD, Encryption.

Telemedicine is playing a vital role as it made easy for everybody to transfer the EHR (Electronic Health record) which may include the medical scanned images from any remote places. This technology made easy for the doctors to ask for higher diagnosis details and for the patients to save time and money. During the transmission of the information over the network, the data may undergo malicious attacks and modifications. The malicious attacks may include geometrical variations, various noises such as Gaussian, salt & pepper, etc. and the modifications may be regionally or globally. In some of the cases this information may be used for making money. And more over a small change in the medical report of a patient may lead to the disastrous decisions even by the expertise doctors. Therefore, there is a need for providing security to the medical information and much research work is being done by many of the researchers to provide high security to the medical information.

Information security methods

There are several methodologies available for protecting the information and some of them are: Steganography, Cryptography and Digital Water Marking.

The function of these hiding techniques and their diagrams are given below:

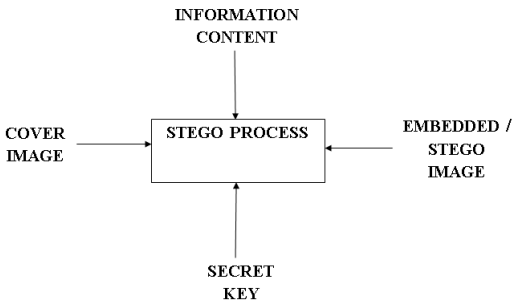

Fig. 1. Block Diagram of Steganography

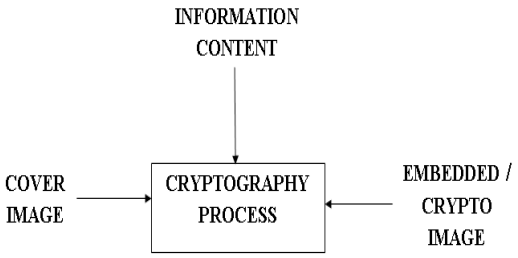

Fig. 2. Block Diagram of cryptography

- Steganography is one of the data embedding techniques in which case we may hide the information content into another cover image and this embedded information is not seen by the human eye.
- Cryptography is another hiding technique in which case the information is embedded in the non-readable format.
- Digital Water Marking technique is another hiding technique where we may embed information into another cover image without much distortion. The embedded information may in any form like text, image, barcode, QR code etc.

As this technique mostly employed on the digital data, it is named as Digital Water Marking. This technique provides not only the security for the information, but also provides authenticity, copyright protection and integrity

Among the three embedding techniques

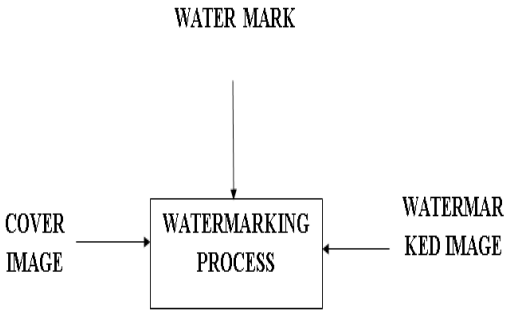

Fig. 3. Block Diagram of Watermarking

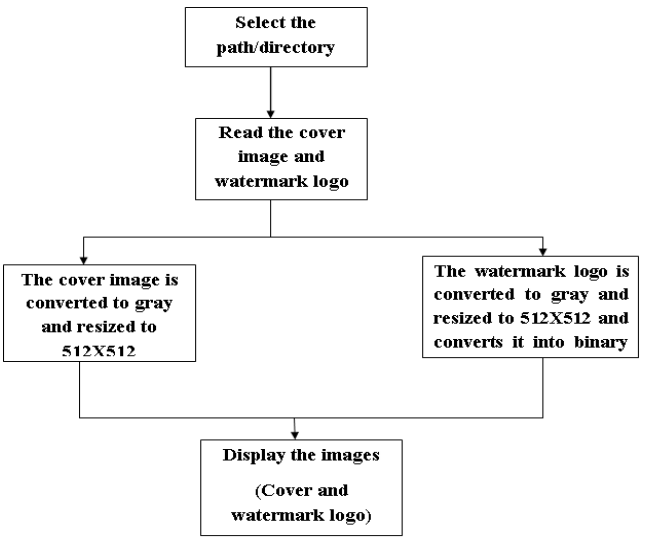

Fig. 4. Initial steps for selecting the cover image and watermark

mentioned above, the most appropriate methodology for securing the medical image is Digital Water Marking [6]. Digital Water Marking (DWM) for medical scanned images is implemented in numerous ways, but no complete algorithm is available to satisfy all the necessities for securing the medical image or information. Therefore till today there exist a space for digital watermarking for medical images and also the medical videos for improving security, reliability, credibility and privacy. Therefore a novel approach is anticipated here to improve the quality, reliability, authenticity and confidentiality [1] & [4] to the medical image.

DWM implementation methods

The Digital Water Marking is primarily implemented in two ways:

- Pixel level domain
- Frequency domain

The pixel level technique often referred as the spatial domain technique is a technique in which the watermark is directly embedded in the pixels, whereas in the latter case, often referred as the transform domain, the pixels are transformed into frequency values and then in these newly formed signals the information is embedded.

Some of the spatial domain methods are as follows [7]:

- *Least Significant Bit method (LSB)*
- *Correlation based technique*
- *Text mapping coding technique*
- *Patch work technique*
- *Additive watermarking*

Some of the transform domain methods are as follows:

- Discrete Fourier Transform
- Fast Fourier Transform
- Discrete Cosine Transform (DCT)
- Discrete Wavelet Transform (DWT)

The digital watermarking may be implemented by any of the mentioned techniques

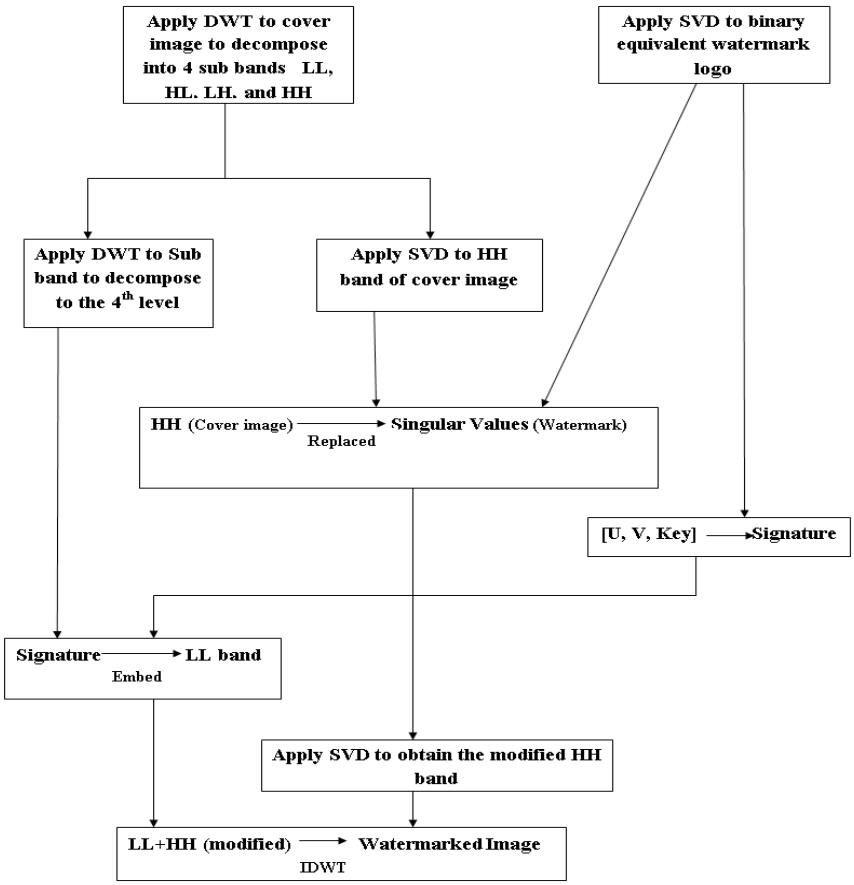

Fig. 5. Flow chart for showing Water mark embedding process

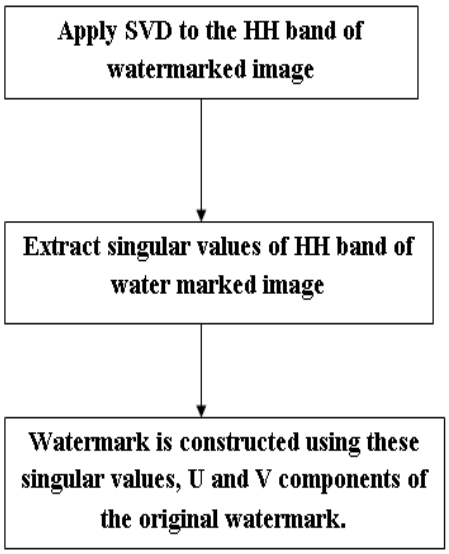

Fig. 6. Flow chart showing the watermark construction process

and also the watermarking for medical images may be implemented by combining the spatial methods with transforming methods [3] & [10]. To increase the security effectiveness, these methods are jointly used with encryption technologies. Most commonly used techniques among the above is DWT. There are other variations of DWT are also available such as Lifting Wavelet Transform (LWT) and Integer Wavelet Transform (IWT). The IWT technique is substituting DWT technique [2] as it has many advantages over DWT. The first and foremost advantage of IWT over DWT is:

In IWT function, the losses are not ensured and coding tasks may be performed very easily, whereas DWT provides the fractional value of filter and loss could also be inevitable. Both spatial and transform domain methods have advantages and disadvantages. The positives of both the methods may be combined to enhance

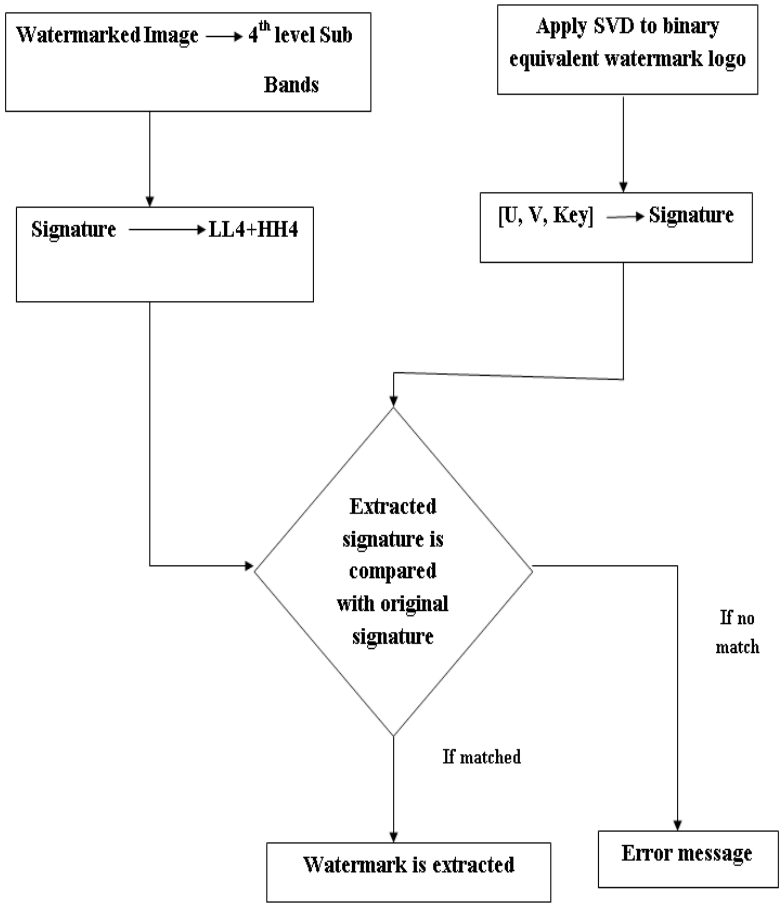

Fig. 7. The flow chart for showing the watermark extraction process

the potential of the system. Also the malicious attacks may be avoided by implementing strong and efficient algorithms [14].

To enhance the security, multiple watermarks may be embedded in the medical images [13] and to reduce the distortion the size of the watermark may also be reduced. In other words, we can say that the data payload should be less to avoid the damage to the information which may achieved by converting the watermark information into barcode or Quick Response (QR) code.

Since this article is mainly on medical images [MI], the DWM for MI may classified as:

- DWM in Region of Interest (ROI)
- DWM in Region of Non Interest (RONI)
- DWM in ROI & RONI

Implementation

In this article the DWM technique is implemented by combining the spatial method: Singular Value Decomposition (SVD), the frequency domain method: DWT and cryptography technique: symmetrical key generation [11] & [12]. This technology is popularly known as Joint watermarking (JDWM). The proposed flow diagram for the implementation of Digital water marking for medical pictures is shown in **Figure4**, **Figure5**, **Figure6** and **Figure7**.

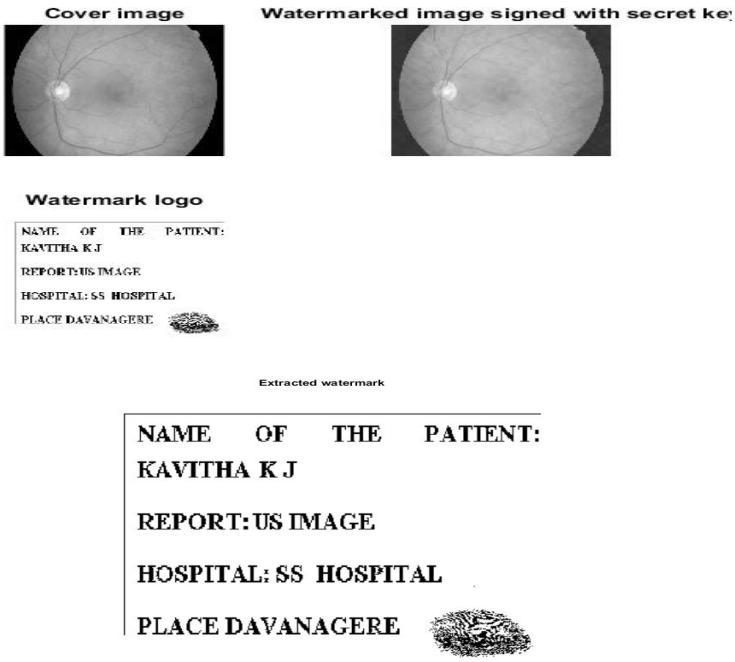

Fig. 8. Cover Image, Watermark image (Patient information, thumb impression), Watermarked image and the Extracted image for the correct key

Fig. 9. Error image for the wrong key

Initial steps

In the flow chart shown below, primarily the cover medical image and the watermark image are read from the database of a hospital. The watermark information may include the details or thumb impression of a patient. If the cover medical image is color image, then it is transformed in to grey medical image and resized to the specified size, for ex. 512×512 and additionally the watermark image is also changed in to binary image and resized to the size of the cover medical image, for ex. 512×512.

After reading the information from the database, the watermark embedding and watermark extraction process are carried out. In Figure4 and Figure5 the image selection and the watermark embedding process are shown.

Watermark Embedding process

In the flow diagram shown above, we can see that the embedding method is carried out by combining the spatial and frequency domain watermarking technique which incorporates DWT, SVD and cryptography [5] & [9] techniques.

The embedding method at the transmitter aspect is described below:

a. Decompose the cover medical image in to four sub-bands by applying 4-level DWT.

b. Apply SVD to the 4th level HH band of the cover image and also to the watermark image.

c. In the above steps three components are generated U, S and V for both original and watermark image. The singular value of both the images is exchanged to generate the modified 4th level HH band.

d. The U and v components of the watermark image may be used with a pseudorandom number to generate the signature.

e. This generated signature may be used as a secret key and hidden in the original image before transmission.

f. Now the modified 4th level HH band and LL band are combined along with the remaining

Table 1. SSIM, PSNR and MSE values for 20 secret keys

Keys	SSIM	PSNR
1	0.8967.	45.0040085890353
2	0.8905.	44.9493032016019
3	0.8997.	44.9961087866195
4	0.8908.	44.8809336492430
5	0.8889.	44.7503321653980
6	0.8938.	45.0119376851504
7	0.8920.	44.8438605723110
8	0.8990.	44.8146511899554
9	0.8963.	45.0040085890353
10	0.8903.	44.8660283799648

Keys	SSIM	PSNR
11	0.8941.	45.0198955683894
12	0.8913.	44.9262733386379
13	0.8962.	44.9415994102162
14	0.8895.	44.7362941294795
15	0.8859.	44.8219167831058
16	0.8933.	45.0682652055501
17	0.8899.	44.9493032016019
18	0.8920.	44.8512247252954
19	0.8974.	44.9339228531879
20	0.8877.	44.9961088786195

Keys	MSE	Keys	MSE
1	2.07051816370031	11	2.06295794097041
2	2.09676428484771	12	2.10791258505017
3	2.07428794197260	13	2.10048695930560
4	2.13003414672462	14	2.20216835555615
5	2.19506160875109	15	2.15917703447701
6	2.06674150928773	16	2.04010917997368
7	2.14829478103283	17	2.09676428484771
8	2.16279228457402	18	2.14465509259948
9	2.07051816370031	19	2.10420304776248
10	2.13735712182427	20	2.07428794197259

two bands and inverse DWT is applied to get the watermarked image.

In this work, twenty secret keys are used for evaluating the performance of the algorithm. To check the efficiency of the algorithm, various quality metrics like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), false positive, false negative, and mean of decoding are evaluated.

During the embedding process, a secret key was hidden in the medical image [8] to provide security while transmitting the data over the network. At the receiver, we will receive watermarked image and in order to retrieve this image, no original image is required; instead it requires the secret key to extract the information. If the input secret key on the receiver is wrong, then it is not possible for us to proceed with the further steps. This ensures increased security for the information.

Table 2. False positive and false negative value for 20 keys

Keys	Pfa	Pfr	Keys	Pfa	Pfr
1	0.5	0.320	11	0.396	0.412
2	0.489	0.329	12	0.385	0.422
3	0.478	0.338	13	0.375	0.431
4	0.468	0.347	14	0.365	0.441
5	0.458	0.356	15	0.356	0.451
6	0.447	0.365	16	0.346	0.460
7	0.437	0.374	17	0.336	0.470
8	0.426	0.384	18	0.327	0.480
9	0.416	0.393	19	0.317	0.490
10	0.406	0.403	20	0.308	0.500

Watermark construction and extraction process

The flow chart for watermark construction and extraction are as shown below.

At the receiver the watermarked medical image is received and using this data, the watermark is extracted and compared with the original watermark and the system robustness is evaluated. In order to construct the watermark, the following steps are performed:

1. Read the watermarked image.
2. Apply 3-level DWT to the watermarked image.
3. Apply SVD to the HH band of 3rd level decomposition.
4. Extract the singular values from the HH band.
5. Use these singular values along with the U and V components of the original watermark.

The detailed diagram of watermark extraction is shown in the below figure. The extracted signature is compared with the original signature. If match is found, then the watermark is extracted otherwise an error message will be displayed.

RESULTS

In this experiment the watermark embedding and watermark retrieval algorithm

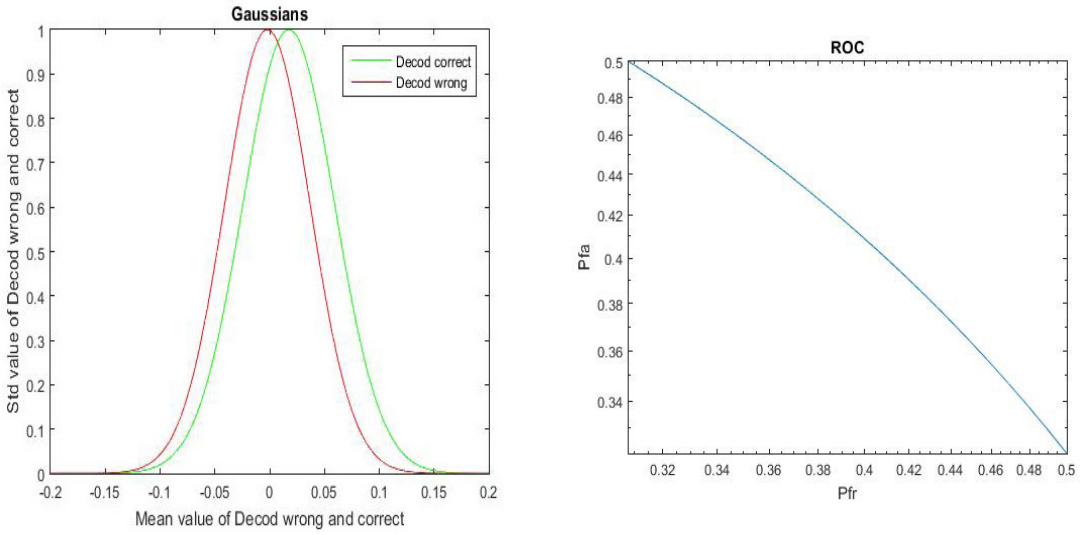

Fig. 10. Graphs showing Standard vs Mean and false positive vs False negative

is executed using MATLAB 2015a. The various quality metrics of the system are calculated so as to assess the performance of the technique being utilized. The Peak to signal noise quantitative relation (PSNR) which can be used for examination of the initial and watermarked medical image, mean sq. error (MSE) to examine the error distinction between the 2 pictures, mean of correct and wrong secret writing, variance, false acceptance and false rejection of the system are evaluated to investigate the enforced system. The below figure shows the results obtained:

The below tables shows the results obtained for twenty different keys.

In this procedure the maximum value obtained are listed as below:

Mean for decoding Correct: 0.01743, Mean for decoding wrong: — 0.002116, SSIM (Max)=0.8997, PSNR(Max)=45.0199, Standard deviation for Correct decoding :0.041898, Standard deviation for Wrong decoding :0.039029, false positive=/0.17, false rejection=0.5 and the maximum time taken for performing embedding and extraction process is minimum of 138.25 and a maximum of 217.46 seconds.

DISCUSSION

In this paper, Joint digital watermark for medical images is proposed. The PSNR, SSIM, MSE, is achieved to the optimum value. The authentication of the system is verified by cryptography technique. Still the more efficiency may be obtained by using the advanced versions of the watermarking embedding and extraction algorithms and also we may look for the techniques in order to reduce data payload so that we may avoid the much damage to the medical image.

REFERENCES

1. R.lakshmi priya, v.sadasivam. A survey on watermarking techniques, requirements, applications for medical images. *Journal of Theoretical and Applied Information Technology*; **65**(1), ISSN: 1992-8645 (2014).
2. Chih-ChinLai, et.al. A Robust Feature-based Image Watermarking Scheme. 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, *IEEE* . Pp 581-586 (2013).
3. V. Pandey. Secure Medical Image Transmission using Combined Approach of Data-hiding , Encryption and Steganography. *International Journal of Advanced Research in Computer Science and Software Engineering;* **2**(12), pp. 54–57 (2012).
4. T. Chen, M. Hwang, and J. Jan. A Secure Image Authentication Scheme for Tamper Detection and Recovery 2011;
5. M. M. Abd-eldayem. ORIGINAL ARTICLE A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine. *Egyptian Informatics Journal*; **14**(1): pp. 1–13 (2013).
6. Chitla and C. M. M. Authenticating Medical Images with Lossless Digital Watermarking. No; pp. 291–296 (2014).
7. P. N. Faoziyah, F. P. Permana, T. A. B. Wirayuda, and U. N. Wisesty. Tamper Detection and Recovery of Medical Image Watermarking using *Modified LSB and Huffman Compression;* pp. 129–132 (2013).
8. Novel Algorithms for Secure Medical Image Communication Using Digital Signature with Various Attacks. (2013).
9. S. Bhatnagar, S. Kumar, and A. Gupta. An Approach of Efficient and Resistive Digital Watermarking using SVD. 2014 pp. 2470–2475.
10. K. Pal, N. Dey, S. Samanta, A. Das, and S. S. Chaudhuri. A Hybrid Reversible Watermarking Technique for Color Biomedical Images. 2013.
11. F. Wen-ge. SVD and DWT Zero-bit Watermarking Algorithm. 2010; pp. 4–7.
12. H. Nyeem. Utilizing Least Significant Bit-Planes of RONI Pixels for Medical Image Watermarking. 2013.
13. N. Mohananthini and G. Yamuna. A Study of DWT-SVD Based Multiple Watermarking Scheme for Medical Images; **17**(5), pp. 558–568 (2015).
14. B. Han and J. Li. Watermarking algorithm for medical volume data anti-geometric attacks.; **2**: pp. 345–349 (2016).