



# AN ALGORITHM FOR SECURING THE BINARY IMAGE VIA ADVANCED ENCRYPTION AND WATERMARKING METHODS

<sup>1</sup>Reshu, <sup>2</sup>Ms. Jyoti Sharma

<sup>1</sup>M.Tech Scholar, <sup>2</sup>Assistant Professor

<sup>1</sup>Computer Science Engineering,

<sup>1</sup>South Point Institute of Technology and Management Sonepat (Hr.), India

**Abstract:** There is an urgent need for copyright enforcement technologies which is increasing day by day in networked multimedia systems. These technologies can protect copyright possession of multimedia content. Image Watermarking is one of the technologies which have advanced to save digital images from illegal access. Content service transmission is a vital field of research to protect the ownership of the content. Also, Robustness against distortions and attacks is a crucial issue in watermarking. This issue has been taken care of greatly in this work. There are various methods to safe medical images, widely used are encryption, steganography, and watermarking, etc. Because of the watermarking benefits, it has gained great importance in the image security field. In this work, an advanced and improved method is proposed for hiding and the extraction of the binary watermark. This approach is proposed to watermark the biomedical information into a biomedical cover image. Along with the watermark extraction, the cover image is also extracted at the end of the receiver. A color image ".jpg" and binary image ".png" is taken as host and watermark image respectively. To increase the size of the security, firstly, the encryption of the watermark image is done by pseudo-random code and embedded in an RGB color cover image. The cover image is also decomposed by using discrete wavelet transform (DWT) and Singular Value Decomposition (SVD) methods. Both of the methods combined enhance the safety level of the proposed method. In short, the new SVD-DWT algorithm for the blind image is powerful in the fight against various attacks. DWT and Inverse DWT conversions were used to obtain four types of frequency images. To measure the efficiency of the proposed method, the test metrics are used such as MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio), and NC (Normalized Correlation).

**Index Terms** – Watermark, Discrete wavelet transform (DWT), Singular value decomposition (SVD) etc.

## I. INTRODUCTION

Development in information technology led to the proliferation of the medical profession, especially in the imaging area [2]. As a result of tele-radiology, telepathy is very popular these days. Teleradiology permits the exchange of medical images for clinical analysis between different hospitals via the Internet or through electronic media and better health care delivery. While such a long-distance image transfer raises new and complex issues, like image retention and fraud, privacy, liability for negligence, etc. Dealing with these problems often ensures an investigation into the safety measures of their limited performance and the scope of continuous self-processing. Watermarking is the process of hiding or inserting certain information into the original media is called the cover image [3]. After watermarking, an image is found is known as a watermarked image. Watermarking is performed on a variety of domains namely spatial and on a modified domain [1] [9].

Medical information is very important and sensitive because of its importance in medical diagnosis, education, treatment, research, and other application, both for private and public [4] [6]. Those types of systems offer easy access, effective distribution, and manipulation of medical data in between the hospitals. There are many reasons for this exchange of medical data, i.e. applications of telemedicine to distant learning of medical employees [4].

## II. RELATED WORK

SHANG Yv-fan et.al presented a powerful watermarking algorithm for medical imaging based on Arnold's transformation and DCT targeting the chronic security problems in today's medical system. It first uses encryption technology to encrypt data of watermark and then combines it with the vector of the visual image feature to produce a series of binary logic. A sequence is considered key and saved by a third party to retain ownership of the real image. The simulation test shows that the algorithm is very simple in operation and very good for durability and invisibility [5].

Ritesh Patel et.al have discussed two different watermarking schemes depends on DCT-DWT-SVD. One watermarking system depends on DC coefficients of SVD by using the second phase of DWT decomposition and the other system depends on SVD for all second-level DCT values for DWT cover image composition [7]. Charles Way Hun Fung et.al, proposed a basic model for watermarking and explained some of the latest image watermarking algorithms and their features. Digital watermarking can be used for many purposes such as copyright protection, broadcast monitoring, and proprietary identification [10].

Ms. Anchal Gupta et.al has researched available video watermarking techniques and provides critical reviews on a variety of available techniques. Video watermarking is a new technology proposed to resolve the illegal use problem and distribution of the digital video. It is a process of inserting information of copyright into video bit broadcasts. Most of the suggested video watermarking programs are based on image watermarking techniques [8].

## III. PROPOSED METHODOLOGY

In this work, a high-quality and improved method of embedding and extraction of the watermark is proposed. This approach is proposed to convert the biomedical information of the watermark into a biomedical cover image. Along with the watermark extraction, the cover image is also extracted at the end of the receiver. Color image ".jpg" and binary image ".png" is taken as host and watermark image respectively. To increase the security level, firstly, the encryption of the watermark image is done by a random pseudo-code and then inserted into a single layer of RGB color cover image. Then, the cover image is also decomposed with the help of DWT and SVD methods. Both of these methods maximize the security level of the proposed method. In short, new SVD-DWT algorithm for the blind image watermarking is robust against various attacks. DWT and Inverse DWT transforms have been used to obtain four different frequency images. To test the efficiency of the proposed method, the test metrics used are MSE, PSNR, and NC.

The following are the steps to start the experiment:

First of all, call and enter the input of the cover image and then convert the cover image into the matrix. Compute the cover image matrix size. Call and read binary watermark image and convert watermark image into binary one then calculates the watermark image matrix size. Now, calculate total elements in the watermark and demand ciphering key from the user.

### ENCRYPTION AND HIDING OF WATERMARK

Declare the loop as per the total elements of watermark & generate random sequence as per the watermark image size. Convert random matrix into binary one and declare external and internal loop as per the rows and columns of matrix of watermark. Application of logical XOR operation on the binary random sequence and binary watermark to encrypt the watermark. Display the original watermark and encrypted watermark

### SINGULAR VALUE DECOMPOSITION (SVD)

Decomposition of the cover image into approximation coefficients with detailed coefficients using DWT. Do SVD of approximation coefficients. Calculate the size of the approximation coefficients matrix and make a dummy matrix (All elements are zero) as per the size of approximation coefficients. Declare external and internal loop as per the rows and columns of watermark matrix & put the encrypted elements of the watermark into dummy matrix. Mix decomposed singular value of approximation coefficients of cover image with watermark. Again, perform the SVD of mixed elements and the generation of new decomposed values. Mix new decomposed values with old decomposed values and also mix newly mixed values with detail coefficients of the cover image using inverse wavelet transform. Lay the cover image with a hidden watermark. Generate and mix different types of attacks to be put on watermarked images. Various types of attacks are:

- white patch on image
- change in black color contrast
- change in white color contrast
- increase of contrast
- decrease of contrast
- addition of speckle noise
- addition of gaussian noise
- rotation by 45 degree
- equalization of image histogram
- Display the attacked watermarked image.

### DECRYPTION AND EXTRACTION OF WATERMARK

With the help of digital wavelet transforms, decompose the newly attacked image and get approximation and detail coefficients. Perform the SVD of approximation coefficients and combine diagonal matrix  $s_2$  with non-negative diagonal elements and unitary matrices  $u_2$  and  $v_2$  that were obtained before. Extract encrypted watermark from the mixed matrix and create dummy matrix (All elements are zero) as per the watermark matrix size. Declare external and internal loops as per the rows and columns of the watermark matrix and put the extracted elements of the watermark into the dummy matrix. Extract the watermark from the cover image and convert the watermark into a binary image. Calculate the size of a new matrix of watermark image & also calculate total elements in the watermark. Request deciphering key from user & declare loop as per the total elements of the watermark. Make a random sequence as per the watermark image size & convert the random matrix into a binary one. Declare external and internal loop according to rows and columns of watermark matrix & XOR binary random sequence and binary watermark to encrypt the watermark. Display the decrypted watermark & calculate the normalized correlation value between the decrypted watermark and the original watermark. Calculate MSE & calculate PSNR.

### RESULTS

In this work, a high-quality and improved method of embedding and extraction of the watermark is proposed. This approach is proposed to convert the biomedical information of the watermark into a biomedical cover image. Along with the watermark extraction, the cover image is also extracted at the end of the receiver. Color image ".jpg" and binary image ".png" is taken as host and watermark image respectively. To increase the security level, firstly, the encryption of the watermark image is done using a random pseudo-code and then inserted into a single layer of RGB color cover image. Then, the cover image is also decomposed with the help of DWT and SVD methods. Both of these methods maximize the security level of the proposed method. In short, the new SVD-DWT algorithm for blind image watermarking is robust against various attacks. DWT and Inverse DWT transforms have been used to obtain four different frequency images. To test the efficiency of the proposed method, the test metrics used are MSE, PSNR, and NC. PSNR is well-defined by equation (1). The error between the actual watermark and the watermark extracted from the attacked image is estimated by using MSE given by the eqn. (2). The similarity between the actual watermark and the watermark extracted from the attacked image is estimated by using NC given by the eqn. (3).

$$\text{PSNR} = 10 \log_{10}(255^2/\text{MSE}) \quad (1)$$

Where,

$$\text{MSE} = \frac{1}{M \times N} \sum_{m=1}^M \sum_{n=1}^N [(m, n) - w(m, n)]^2 \quad (2)$$

$$\text{NC} = \frac{\sum_i \sum_j w(i, j) w'(i, j)}{\sum_i \sum_j |w(i, j)|^2} \quad (3)$$

The above three parameters are calculated for the Watermark image and Cover image for all kinds of attacks that are given in table 1. Table 1 is the proof of the improved performance of the proposed method. Some screenshots of different steps of the proposed method have been given below. Figure 1 is the screenshot of the original cover image. Figure 2 is the screenshot of the watermark image. Figure 3 is the screenshot of the encrypted watermark image. Figure 4 is the screenshot of the cover image with the encrypted watermark or watermarked image. Figure 5 is the screenshot of gray watermarked with attacks. Figure 6 is the screenshot of the color watermarked with the attack. Figure 7 is the screenshot of the extracted encrypted watermark from watermarked image. Figure 8 is the screenshot of the decrypted watermark. Figure 9 is the screenshot of the recovered RGB color cover image, original cover image and color watermarked with the attack.

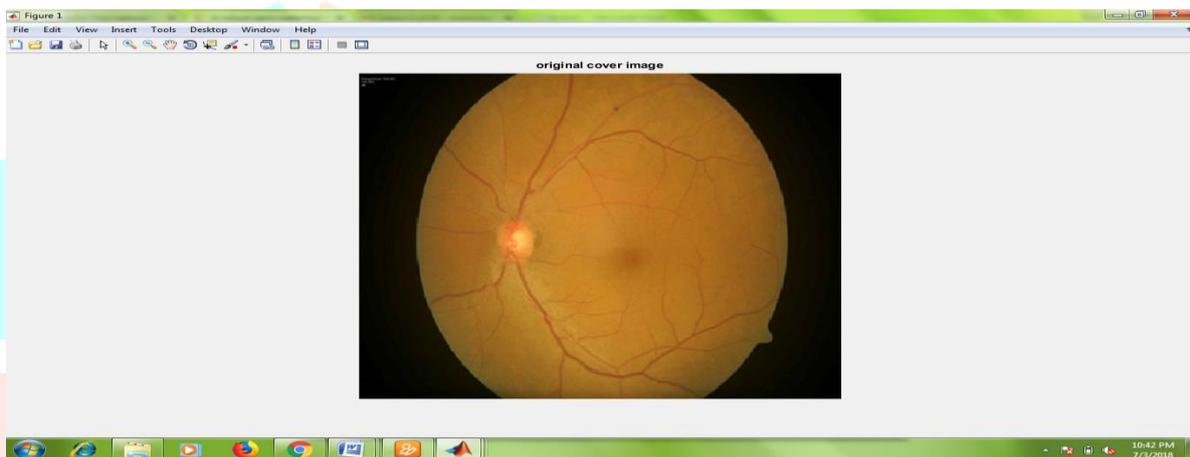


Figure 1 original cover image

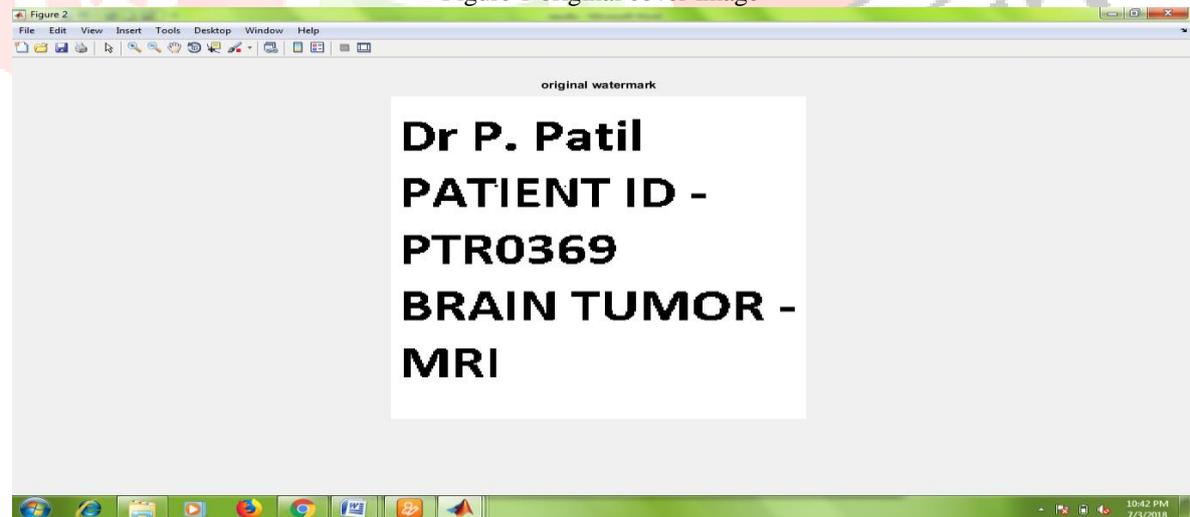


Figure 2 watermark image

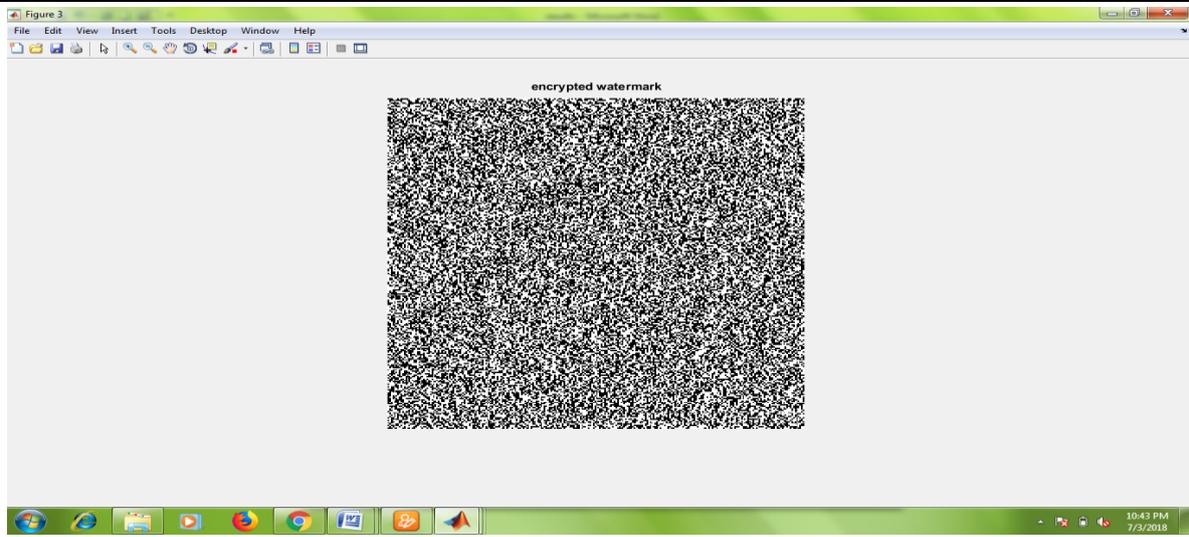


Figure 3 encrypted watermark image



Figure 4 cover image with encrypted watermark or watermarked image



Figure 5 gray watermarked image with attack

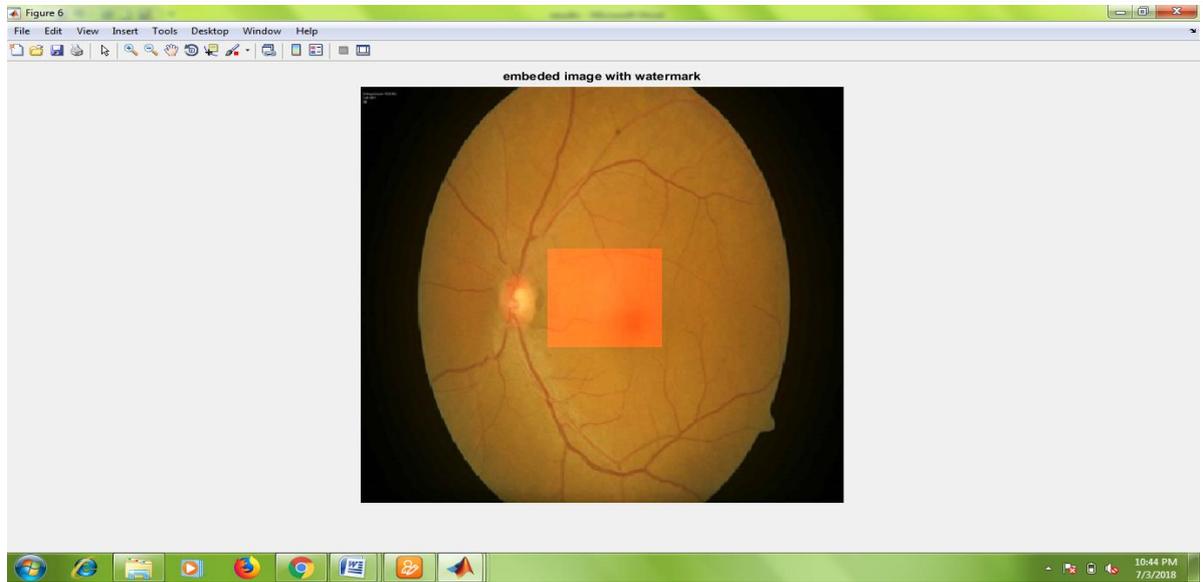


Figure 6 color watermarked image with attack



Figure 7 extracted encrypted watermark from watermarked image

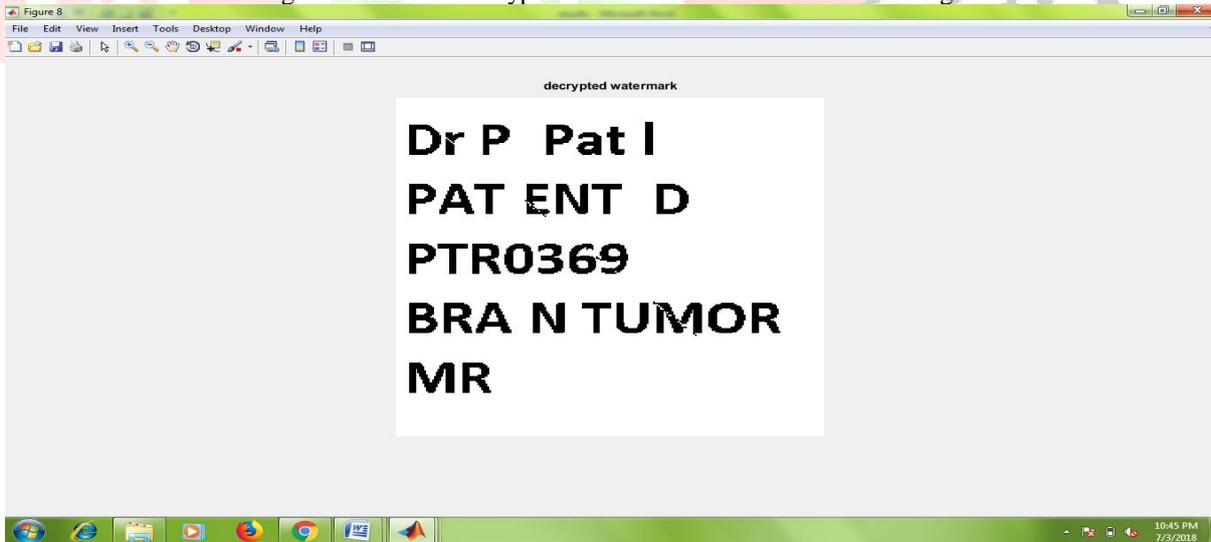


Figure 8 decrypted watermark image

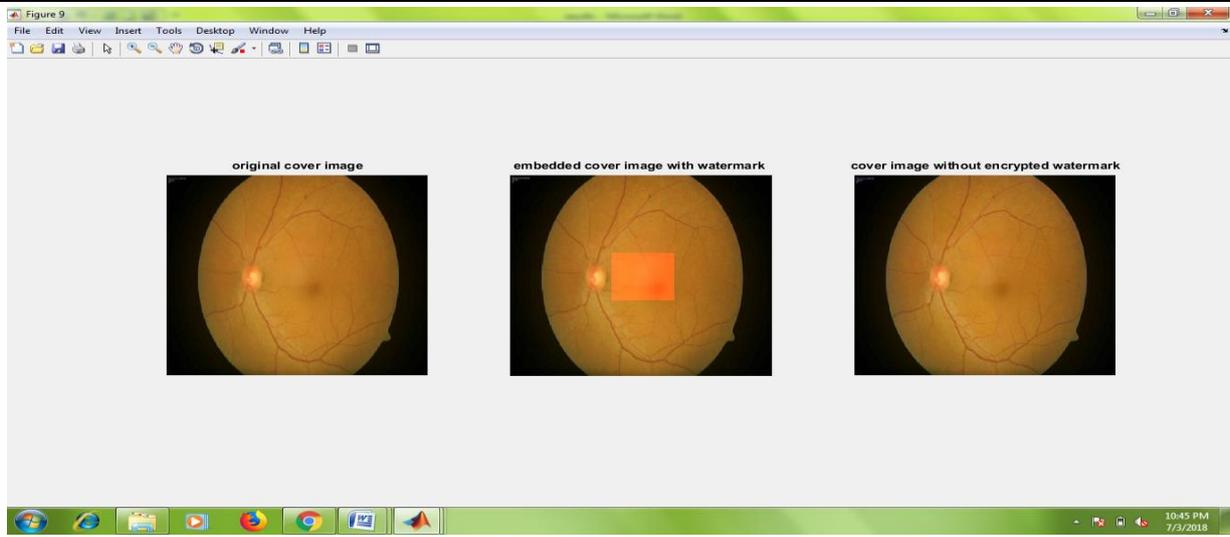
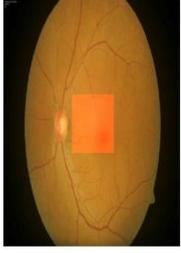
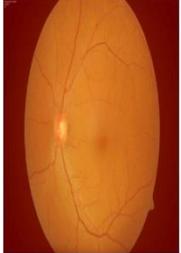
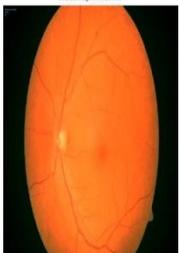
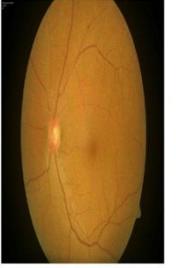
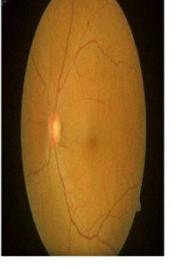


Figure 9 recovered RGB color cover image, original cover image and color watermarked with attack

Table 1 Performance Parameters of Proposed Method with Different kinds of Attack

Type of Attack	Attacked image	MSE		PSNR		Correlation Value	
		Water mark	Cover image	Water mark	Cover Image	Water mark	Cover image
<b>PATCH ON IMAGE</b>		0.0097	2.6532	68.332	43.927	0.9523	0.962
<b>CHANGE IN BLACK COLOR CONTRAST</b>		0.0123	1.4076	67.500	46.680	0.9397	0.981
<b>CHANGE IN WHITE COLOR CONTRAST</b>		0.0096	2.5472	68.367	44.104	0.9531	0.965
<b>INCREASE OF CONTRAST</b>		0.1319	1.7070	56.956	45.842	0.5553	0.971

<b>DECREASE OF CONTRAST</b>		0.0122	1.3884	67.280	46.739	0.9401	0.981
<b>ADDITION OF SPECKLE NOISE</b>		0.0322	4.5865	63.082	41.550	0.8512	0.945
<b>ADDITION OF GAUSSIAN NOISE</b>		0.0104	6.8404	67.675	39.814	0.9493	0.910
<b>ROTATION BY 45 DEGREE</b>		0.0098	2.7843	68.263	43.717	0.9523	0.957
<b>EQUALIZATION OF HISTOGRAM OF IMAGE</b>		0.0106	3.2225	67.930	43.082	0.9484	0.957

### CONCLUSION AND FUTURE SCOPE

A high-quality and improved method of embedding and extraction of the watermark is proposed. This approach is proposed to convert the biomedical information of the watermark into a biomedical cover image. Along with the watermark extraction, the cover image is also extracted at the end of the receiver. Color image ".jpg" and binary image ".png" is taken as host and watermark image respectively. To increase the security level, firstly, the encryption of the watermark image is done using a random pseudo-code and then embedded to a single layer of RGB color cover image. With the help of SVD, the watermark is embedded in a high-frequency band. The presented method is performing much better as compared to existing methods in terms of PSNR, MSE, and Correlation co-efficient for watermark and cover image. Experimental results are the proof of the above statement. The PSNR value of the proposed method is between 57db-72db and the average Correlation coefficient value is 0.9733, which shows that the watermark extracted from the attacked image is near to the actual watermark. The value of PSNR and Correlation coefficient is much higher than that of the existing method for all the attacks. Also, both methods (SVD-DWT)

combinedly increase the security level of the proposed method. In short, a secure and robust blind image watermarking algorithm is presented which is robust against numerous attacks. By comparison with other algorithms, the proposed algorithm can increase watermark data security with second encryption, make it easier to calculate, improve accuracy and consistency, and increase resistance to geometric attacks and common attacks. Besides, since it does not require automatic ROI options, it can increase the speed of embedding. In addition, it does not disturb the quality of the actual medical image, and therefore boasts of the high importance of health care. Finally, the algorithm applies to medical imaging as well as to other fields.

There are three frequency images (low-frequency image, middle-low frequency image, middle high-frequency image) which have not been used for embedding purpose. So, three more watermarks can be embedded into them in the future.

## REFERENCES

- [1] Thabit, Rasha, and Bee Ee Khoo 2015. A new robust lossless data hiding scheme and its application to color medical images. *Digital Signal Processing* 38 (2015): 77-94.
- [2] Kumar, E.P., Philip, R.E., Kumar, P.S. and Sumithra, M.G., 2013, July. DWT-SVD based reversible watermarking algorithm for embedding the secret data in medical images. In 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.
- [3] Saxena, P., Garg, S. and Srivastava, A., 2012, April. Dwt-svd semi-blind image watermarking using high frequency band. In 2nd International Conference on Computer Science and Information Technology (ICCSIT'2012) Singapore April (pp. 28-29).
- [4] Das, S. and Kundu, M.K., 2013. Effective management of medical information through ROI-lossless fragile image watermarking technique. *Computer methods and programs in biomedicine*, 111(3), pp.662-675.
- [5] Yv-fan, S. and Yi-ning, K.A.N.G., 2013. Medical Images Watermarking Algorithm Based on Improved DCT. *Journal of Multimedia*, 8(6).
- [6] Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O. and Toval, A., 2013. Security and privacy in electronic health records: A systematic literature review. *Journal of biomedical informatics*, 46(3), pp.541-562.
- [7] Ritesh Patel and Prof.A.B.Nandurbarkar 2015, Implementation of DCT DWT SVD based watermarking algorithms for copyright protection , *International Research Journal of Engineering and Technology (IRJET)*, Volume: 02 Issue: 02 | May-2015, pp(340-344).
- [8] Ms. Anchal Gupta and Er. Rimanpal kaur, A Study of Video Watermarking Techniques Based on Energy Model, *International Research Journal of Engineering and Technology (IRJET)* Volume: 02 Issue: 01 | Mar-2015, pp (116-121)
- [9] Rajpoot, M.S., 2014. A Review paper on Hybrid Watermarking Approach for Higher Imperceptibility and Robustness by using DWT-SVD-SWT.
- [10] Charles Way Hun Fung, Antonio Gortan and Walter Godoy Junior 2011, A Review Study on Image Digital Watermarking , *ICN 2011 : The Tenth International Conference on Networks* pp(24-28)