Reversible Watermarking and Encryption Method for Safe Transfer Of Medical Images Using Hybrid DWT-SVD Technique

Pravin savaridass.M[1], Ameena bibi.N[2]

[1]PG Scholar, Department of ECE, Government College of Technology, Coimbatore, India.
[2]Assistant Professor, Department of ECE, Government College of Technology, Coimbatore, India.

---***---

Abstract - *This paper is the combination of reversible watermarking and encryption method for better security, robustness and confidentiality of medical images. In watermark embedding process, two level Digital Wavelet Transform (DWT) is applied to original cover image. LH1 and LH2 sub band coefficients obtained after applying DWT is selected for watermarking. Both the sub bands are sub divided into 4x4 matrices and Singular Value Decomposition (SVD) is applied. Watermark in the form of image or text is converted into binary form and encrypted. Encrypted watermark bits are embedded by modifying the singular value (SV) matrix. Then inverse SVD and inverse DWT is applied to form the watermarked image and then image is encrypted for further security. In watermark extraction process, watermark is extracted from SV matrix by reversing the embedding process. Cover image is reconstructed after extraction without using original cover image. The proposed system is simulated and results are analyzed using various performance metrics. The experimental results shows that proposed system has better robustness and imperceptibility under various attacks such as noise, crop and compression attacks.*

Key Words: **watermarking, DWT-SVD, medical image, reversible watermarking, encryption, security.**

1. INTRODUCTION

The digital communication system made easier way of transmitting digital data through communication network. This ease of manipulations does not ensures the security issues. To make highly secured transfer of those digital data are popularly made by embedding a secret data within those original data. This process is especially popular in images, known as watermarking. The watermarking scheme mainly used for providing ownership of data, confidentiality and reliability. The reliability of images plays major role in military and medical applications. Especially in medical applications the medical images are transferred for opinions and tele -diagnosis, during the transmission the patient details are confidential, so the patient ID, hospital logo or some other important information can be embedded in the image in the form of text or image (binary image). The watermarking can be visible or invisible. The basic characteristics of watermarking method are robustness, capacity, imperceptibility and security.

Most importantly watermarking methods should not alter the original image information. Robustness is the measure of immunity of inserted watermark against various image modifications like filtering, noise attacks, compression, rotation, resizing, cropping. Imperceptibility is a quality of input medical image should not be modified due to insertion of watermark. Capacity is the measure of quantity of data inserted as watermark. Extraction of watermark from the watermarked image without using original image is achieved by reversible watermarking. Reversible watermarking method is useful in medical images transfer, because it is possible to recover the original image and watermark without any loss or distortion without using original image at the receiver end. Encryption algorithms are considered as a protection technique. Encryption technique is additionally used to enhance the robustness of watermarking process. Proposed scheme's goal is to join the robustness of watermarking technique with the security offered by the encryption algorithm.

The rest of this paper is organized as follows. Section-II presents the various works related to our scheme and an overview of the methods utilized in the proposed scheme. Section-III illustrates the proposed watermark embedding, encryption and extraction procedures. Section-IV presents the experimental setup and results. Finally, the conclusions are stated in Section-V.

2. RELATED WORKS BASED ON OUR SCHEME AND OVERVIEW OF THE METHODS USED

In this section, the different works related to watermarking algorithm by applying the Singular Value Decomposition and Discrete Wavelet Transform is summarized. In [3] a robust watermarking method for images by combining SVD, DCT and SVD technique is proposed. HL the middle frequency band after applying DWT to the input image is selected to embed the watermark. Kumar et al. in [4] have proposed a watermarking method based on SVD and DWT. In this method, 3 level of DWT have been used. Then the watermark is embedded into diagonal elements of the singular matrix of original input image. Medium (LH or HL) frequency bands chosen for watermark embedding process. In [2] Amith et al. proposed a robust watermarking method by combining DWT, DCT and SVD. The first step consists to decompose the original image into 1st level DWT transformation of LL (Low frequency band).Next step is to watermarking the transformed image by using SVD and DCT. After that the values of watermark is embedded in the singular matrix values of original cover image. To obtain the watermarked image, the inverse SVD on V, U vectors and modified S vector is applied then inverse DWT and inverse DCT is applied. Currently, establishing block-based image watermarking techniques is of interest because of their advantages, one of which is the ability to process each block individually and it increases capacity. The basis of this technique is to embed the watermark into the selected blocks, which are the blocks or regions bearing the basic character information of the image, such as the texture and edges.

The overview of the techniques used in proposed system like DWT, SVD is explained in following sections. Wavelet transform decompose a signal to a set of basis functions, it is called as wavelets. Wavelet transform provide both spatial and frequency information of an image. Unlike other conventional transforms like Fourier transform, temporal information is retained in wavelet transformation technique. Wavelet transform is a multi-resolution analysis, it decomposes the images into coefficients of wavelets and scaling function. The 2D-DWT is popular nowadays and play key role in image processing. DWT is suitable for identifying the areas in the original image where we can embed a secret watermark image. This property helps to achieve imperceptibility of watermarking process, if a DWT co-efficient is altered, it modifies the region corresponding to that particular coefficient only. Embedding the watermark in low frequency bands may degrade the input image because most of the image information is stored in lower sub-bands. However it is more robust than high frequency bands. The high frequency band contains the edge information of the image, this high frequency sub-band is generally used for watermarking because the human eye is less sensitive to changes in edges, but has less robustness to attacks. So in the proposed system medium frequency band is selected for embedding the watermark to satisfy both imperceptibility and robustness property.
Singular Value Decomposition (SVD) is a unique technique used to factorize the matrices for numerical analysis [8]. The important properties of SVD in image processing applications are: (1) singular values (SV) of an image have good stability, i.e., when a tiny perturbation is added to the image, its SVs does not change considerably. (2) SV shows the inherent algebraic image properties. In this section, a watermark casting and revealing scheme based on the SVD is described. In linear algebra we can observe that an image is an array of non-negative scalar values which may be a matrix. Given the matrix I which represents an input image, singular value decomposition (SVD) can be used to decompose I into I = U*S*V' where U and V' are orthogonal matrices and S is a singular, diagonal matrix. In applications, SVD method has been applied to image compression, image hiding [8] and image watermarking. Chung et al. presented an SVD and vector quantization-based image hiding algorithm for embedding the secret data into the S component of the SVD. Using a different way, Liu and Tan [8] presented a well-organized SVD-based algorithm to modify the coefficients in D component for embedding watermark into the cover image. Chang et al. [9] presented a block-based watermarking algorithm by partitioning the image into several blocks and changed the coefficients in U component for each block to achieve the watermarking effect. SVD can also be used for watermarking by changing the singular values of the input image and replacing the singular values with the watermark.

3. PROPOSED WATERMARKING AND ENCRYPTION METHOD

In this section we explain our proposed schema of combined Discrete Wavelet Transform with block based Singular Value Decomposition for medical image watermarking. The patient's data or hospital logo (watermark) and watermarked image are encrypted for further security.

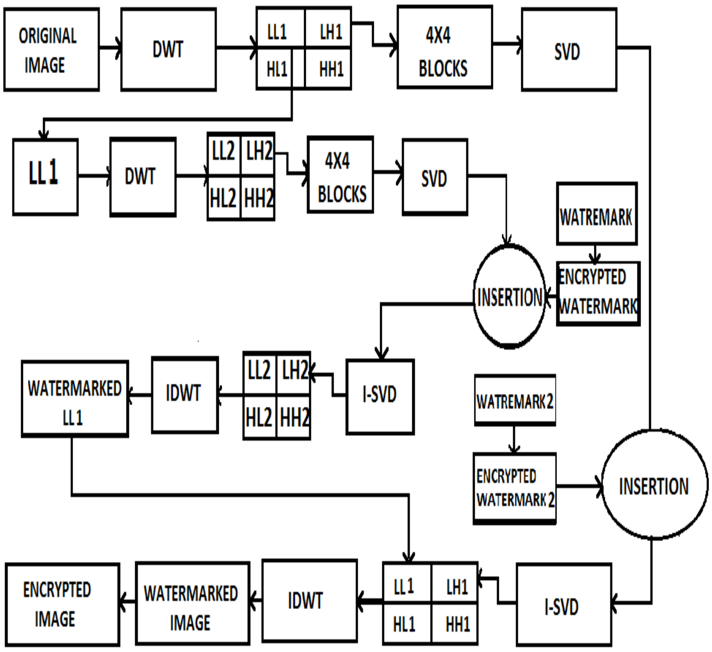


Figure -1: BLOCK DIAGRAM OF PROPOSED METHOD

Watermark embedding process

Step1: Take the input image (CT or any type of medical image)
Step2: Two level Discrete Wavelet Transform ('Daubechies') is applied on the input image.
Step3: For better imperceptibility and robustness we choose LH1 and LH2 sub bands and divide it into non overlapping 4x4 sub blocks.
Step4: On each 4x4 block Singular Value Decomposition (SVD) is applied to obtain singular matrix.
Step5: Watermark (text or image) to be inserted is converted into binary form and encrypted.

Step6: The watermark bit (W) is inserted in the diagonal elements of singular value (SV) matrix as per insertion process.

INSERTION PROCESS

```
S-Singular matrix of size 4x4 obtained after applying SVD
W-Watermark bit
If W==1
  q=(S(1,1)+(3,3))/2;
  if S(2,2)<=q;
    qq=q-S(2,2);
    S(2,2)=S(2,2)+qq+1;
  else
    S(2,2)=S(2,2);
  end
else if W==0
    if S(2,2)>q
      qp=S(2,2)-q;
      S(2,2)=S(2,2)-qp-1;
    else
      S(2,2)=S(2,2);
    end
```

Step7: Inverse SVD is applied including modified singular matrix.
Step8: Inverse DWT applied to obtain the watermarked image.
Step9: Watermarked image is encrypted for further security.

Watermark extraction process

Step1: Watermarked image is decrypted and two level Discrete Wavelet Transform ('Daubechies') is applied on watermarked image.
Step2: LH1 and LH2 sub bands are chosen and divide it into non overlapping 4x4 sub blocks.
Step3: On each 4x4 block Singular Value Decomposition (SVD) is applied to obtain singular matrix.
Step4: Watermark is extracted from the diagonal elements of singular matrix as per extraction process.

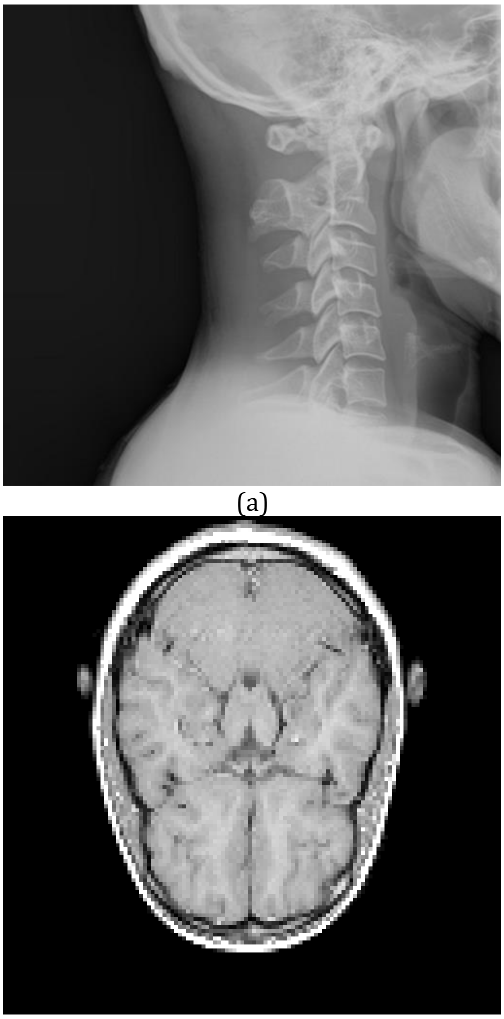
EXTRACTION PROCESS

```
S-Singular Matrix
W-Watermark bit
q=(S(1,1)+S(3,3))/2;
  if S(2,2)>q
    qq=S(2,2)-q;
    S(2,2)=S(2,2)-qq-1;
    W=1;
  else if S(2,2)<=q
    qp=q-S(2,2);
    S(2,2)=S(2,2)+qp+1;
    W=0;
  End
```

Step5: The watermark (W) extracted in each block is concatenated and decrypted, obtained watermark (binary form) is converted to original form.
Step6: Inverse SVD is applied using singular matrix after extraction.
Step7: Inverse Discrete Wavelet Transform is applied to obtain retrieved image.

4. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed scheme is simulated in MATLAB2013a by using two medical images as test images shown in Figure 2 and watermark (image and text) shown in Figure 3. The experiment is carried out by inserting watermark into the input medical images. The result watermarked image, extracted watermark and reconstructed images are shown in Figure 4 & 5 with their PSNR, and BCR values. It is essential to obtain good values of PSNR and BCR regardless of the domain and method of the watermarking. Indeed, this is essential in the medical image sector. Various performance metrics that are calculated in proposed system is explained below.



(a)

(b)

Figure -2: (a) & (b) INPUT MEDICAL IMAGES

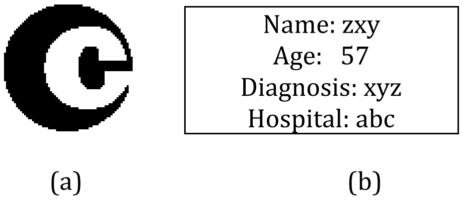


Figure -3:(a) WATERMARK (IMAGE)
(b) WATERMARK 2 (TEXT)

A. PSNR

The PSNR is used to estimate and analyze the imperceptibility. Imperceptibility is the term used to evaluate the similarity level between the input image and watermarked image. It is defined as follows

$$\mathrm{PSNR} = 10\log_{10}\left[\frac{\max(x(i,j))^2}{\mathrm{MSE}}\right]$$

Where i, j are the coordinates of each pixel of the input image X and mean-square error (MSE) value between the input image X and the watermarked image Y , and MSE is defined as

$$\mathrm{MSE} = \frac{1}{m*n}\sum_{i=1}^{m}\sum_{j=1}^{n}[x(i,j) - y(i,j)]^2$$

Where m and n are number of rows and columns, x(i,j) and y(i,j) are pixel values of original and extracted images respectively. When good imperceptibility is achieved, the watermarked image appears nearly identical to the host image, in other words, we can say that the host image is not affected by the watermarking process.

B. BCR

BCR is a criterion used to measure the robustness by evaluating the similarity between the original watermark and the extracted watermark with or without attacks. BCR ranges from 0 to 1. When the BCR value is close to 1 under applicable attacks, the scheme is robust against those attacks. The BCR can be estimated as follows

$$\mathrm{BCR}(w,\bar{w}) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\overline{w_{ij}\otimes\bar{w}_{ij}}}{M*N}$$

Where N and M represent the number of rows and columns pixels in the watermark and w, $\bar{w}$ indicate the original and the extracted watermarks respectively. The input images are tested by our proposed scheme without any attack and they result better PSNR and BCR values. Most importantly watermarking scheme is tested against several types of attacks to check its robustness.

C. ENTROPY

Entropy is a magnitude characterizing the quantity of data contained in an image. In fact, the information entropy is the most important feature of randomness and encryption. In fact, if the dispensing of grey values is very uniform, the information entropy is greater. The entropy *E(s)* is defined as follows:

$$E(s) = -\sum_{i=1}^{N}\left[P(Si)\log_2\left(P(Si)\right)\right]$$

P(Si) is the histogram count of an image

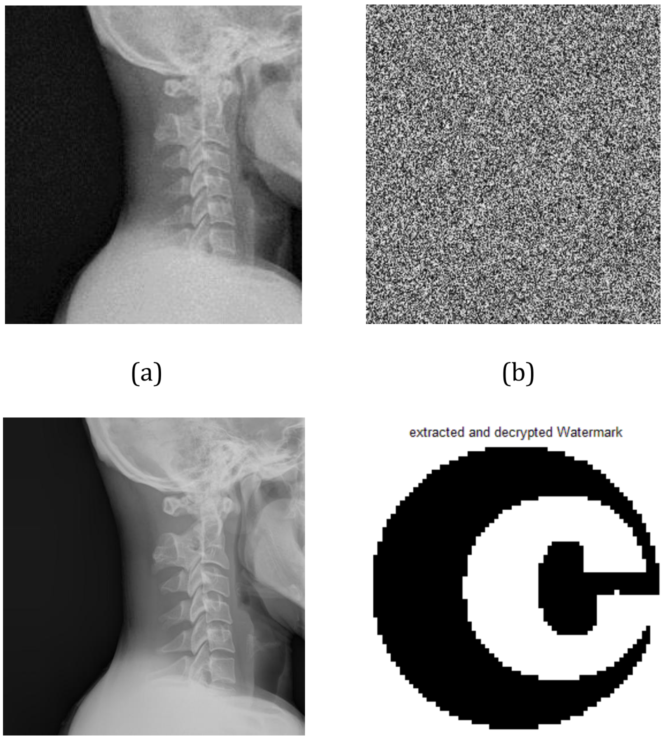
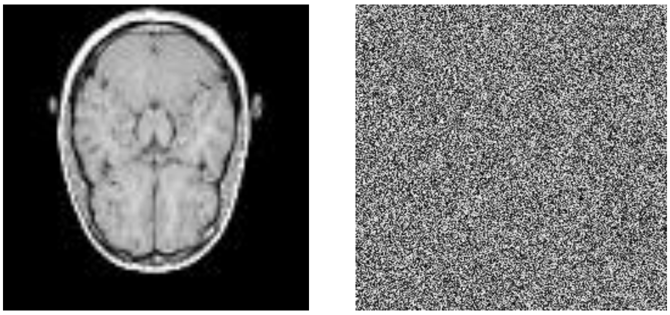
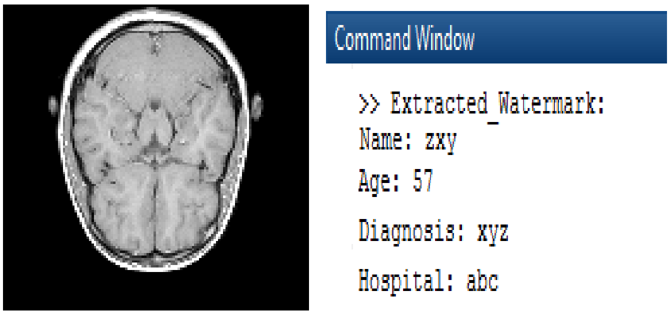


Figure -4:(a) WATERMARKED IMAGE (PSNR=55.67dB) (b) ENCRYPTED IMAGE (Entropy=7.89 (c) EXTRACTED IMAGE (PSNR=61.03dB) (d) EXTRACTED WATERARK (BCR=0.9998)





```
>> Extracted_Watermark:
Name: zxy
Age: 57
Diagnosis: xyz
Hospital: abc
```

(c) (d)

Fig -5: (a) WATERMARKED IMAGE (PSNR=53.67dB) (b) ENCRYPTED IMAGE (ENTROPOY=7.68) (c) EXTRACTED IMAGE (PSNR=60.14dB) (d) EXTRACTED WATERMARK (BCR=1)

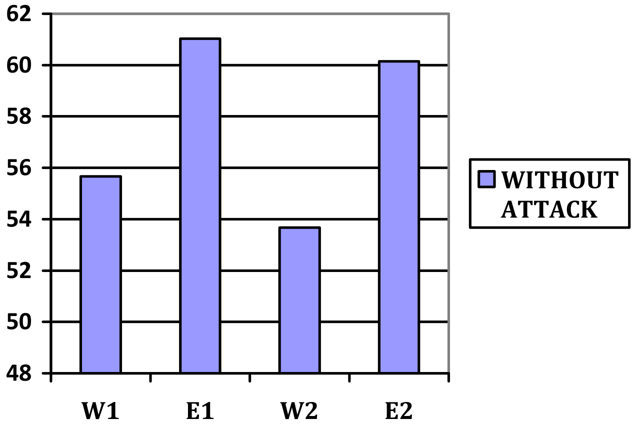


Chart -1: PSNR VALUES OF WATERMARKED (W) AND EXTRACTED (E) IMAGES WITHOUT ANY ATTACK W1 & E1 - FIGURE 2 a , W2 & E2 - FIGURE 2 b

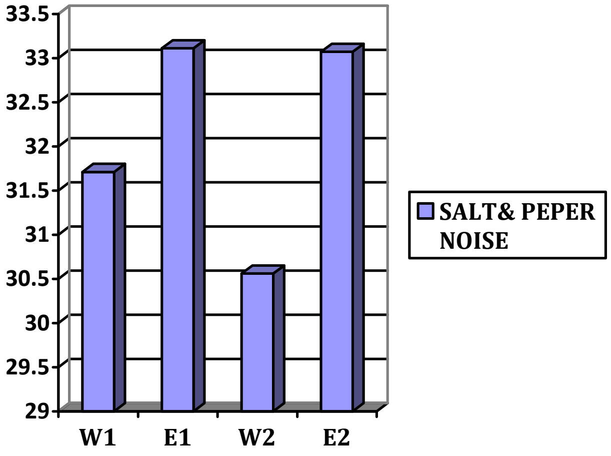


Chart -2: PSNR VALUES OF WATERMARKED AND EXTRACTED IMAGES AGAINST SALT & PEPPER NOISE ATTACK

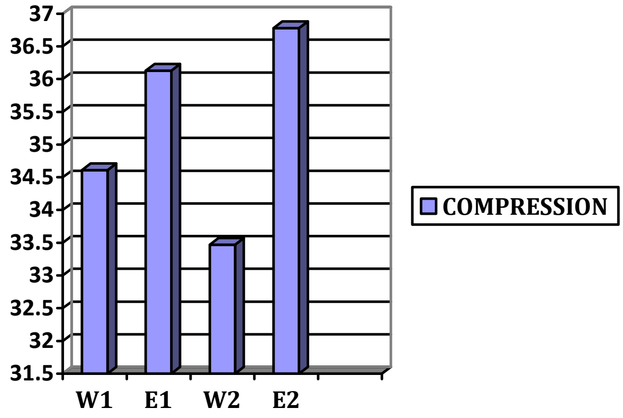


Chart -3: PSNR VALUES OF WATERMARKED AND EXTRACTED IMAGES AGAINST COMPRESSION ATTACK

Most common attacks are chosen to analyze the robustness of proposed system. They are JPEG compression attacks, Salt & Pepper noise and Cropping. After attacking the same medical images, we attempt to extract our watermark and to reconstruct the original image. PSNR and BCR values of simulated results are shown as charts in CHART 1-4.

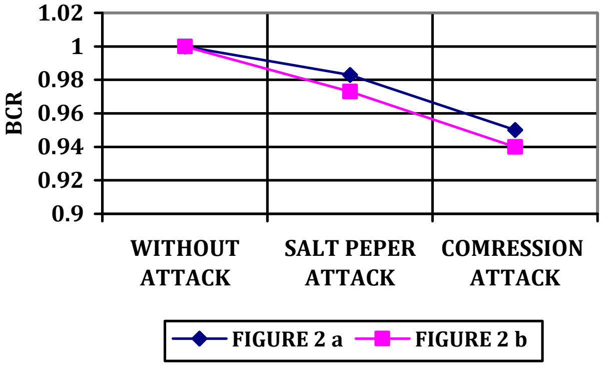


Chart -4: BCR VALUES OF WATERMARK AGAINST VARIOUS ATTACKS

The goal of this calculation is to determine the degree of robustness of our algorithm to resist to several attacks. Based on the results our proposed algorithm has a higher robustness against various attacks with better BCR values and the cover images are reconstructed with good PSNR values.

5. CONCLUSIONS

In this paper, a hybrid DWT–SVD block based reversible watermarking and encryption scheme is presented to ensure the confidentiality, robustness and security of medical images during transmission. The result shows that the robustness is high in our proposed scheme against various attacks. Cover image is reconstructed with better quality without using the original cover image unlike most of watermarking schemes. Capacity of watermark is increased by proposed block based SVD method and security level of watermarked image is improved by encryption technique. Future works aims to improve the capability, robustness of watermark and quality of reconstructed image against high level of attacks.

REFERENCES

[1] Sondes, Mohamed, and Abdellatif "Hybrid SVD- DWT watermarking technique using AES algorithm for medical image safe transfer" 16th international conference on Sciences and Techniques of Automatic control & computer engineering - STA'2015, Monastir, Tunisia, December 21-23, 2015

[2] Singh, Amit Kumar, Mayank Dave, and Anand Mohan. "Hybrid Technique for Robust and Imperceptible Image Watermarking in DWT–DCT–SVD Domain. "National Academy Science Letters 37.4, pp. 351-358, 2014.

[3] S. Murty, Dr. Rajesh Kumar, "A Robust Digital Image Watermarking Scheme using Hybrid DWT-DCT-SVD Technique", IJCSNS,Vol.10,No.10, pp. 185-192, Oct 2010.

[4] Satendra Kumar, Ashwini Saini, Papendra Kumar, " SVD based Robust Digital Image Watermarking using Discrete Wavelet Transform", IJCA,Vol. 45No. 10, pp.7-11, May 2012.

[5] Makbol, N.M., Khoo, B.E.: Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. Int. J. Electron. Commun.(AEU) 67(2), pp. 102–112, 2013.

[6] Ray, Arun Kumar, et al. "Development of a new algorithm based on SVD for image watermarking." Computational Vision and Robotics. Springer India, pp.79-87, 2015.

[7] Zhou, Yaxun, and Wei Jin. "A novel image zero-watermarking scheme based on DWT-SVD." Multimedia Technology (ICMT), 2011 International Conference on.IEEE, pp. 2873-2876, 2011.

[8] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Trans. Multimedia, vol. 4, no. 1, pp. 121–128, Mar. 2002.

[9] Chang, C.C., Tsai, P., Lin, C.C.: 'SVD-based digital image watermarking scheme', Pattern Recognit. Lett, 2005, 26, (10), pp. 1577–1586

[10] Nasrin M. Makbol1, Bee Ee Khoo1, Taha H. Rassem "Block-based discrete wavelet transform singular value decomposition image watermarking scheme using human visual system characteristics" IET Image Processing Journal. ISSN 1751-9659.

[11] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Processing Letters, vol. 18, no. 4, 2011.

[12] W. Hong, T.-S.Chen, and H.-Y. Wu, "An improved reversibledata hiding in encrypted images using side match," IEEE Signal Processing Letters, vol. 19, no. 4, pp. 199–202,

[13] Singh AK, Dave M, Mohan A, "Hybrid technique for robust and imperceptible image watermarking inDWT-DCT-SVD domain", NatlAcadSciLett 37(4), pp. 351–358, 2014.

[14] Kannammal, A., and S. Subha Rani. "Authentication of medical images using integer wavelet transforms." International Journal of Emerging Technology and Advanced Engineering 2.9, pp. 104-108, 2012.

[15] Habiba Loukil,HadjKacem and Mohamed Salim Bouhlel. Mesure de la qualité des images par l'utilisation de la loi de weber. In International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, 2005.

[16] Federal Information Processing Standards Publication, "Secure Hash Standard," 180-2, 2002.

[17] S. Gastan, Codage de canal pour les communications optiques [M.S. thesis], 2009.