International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

COPY RIGHT

2018 IJIEMR. Personal use of this material is permitted. Permission from IJIEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper, all copy right is authenticated to Paper Authors

IJIEMR Transactions, online available on 20th January 2018. Link :

http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-01

Title: ECG Steganography for Protecting Patient Confidential Information in Point Of Care System by SVD.

Volume 07, Issue 01, Page No: 74 – 81.

Paper Authors

*** D. ANUDEEPTHI, N. NAGARAJU.**

* Department of ECE, Sai Tirumala Nvr Engineering College.

International Journal for Innovative Engineering and Management Research ★

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative
Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ECG STEGANOGRAPHY FOR PROTECTING PATIENT CONFIDENTIAL INFORMATION IN POINT OF CARE SYSTEM BY SVD

***D. ANUDEEPTHI, **N. NAGARAJU**

*M.Tech [DECS] PG Scholar, Department of ECE, Sai Tirumala Nvr Engineering College, Narasaraopet, Ap, India.
** M.Tech [DECS] Associate Professor, Department of ECE , , Sai Tirumala Nvr Engineering College, Narasaraopet , Ap, India.

derangulaanudeepthi@gmail.com nagaraju.433@gmail.com

ABSTRACT:

The patient's confidential data should be safe and secure this is Act by Health Insurance Portability and Accountability Act (HIPAA). At the same time, there is a significantly growth in population. Numbers of patient care centers are used usually around the world in a Point - Of - care (PoC) applications in hospitals around the, huge amount of ECG signal collected by Body Sensor Networks (BSNs) from remote patients at homes will be transmitted such as blood pressure, temperature, glucose level etc along with other physiological readings. If the diagnosed by those remote patient monitoring systems are important that patient confidentiality it is protected while data is being transmitted over the public network as well as when they are stored in hospital servers used in this paper by remote monitoring systems and the wavelet based steganography technique has been introduced which combines encryption and scrambling technique to protect patient confidential data to be allows ECG signal to hide its corresponding patient confidential data and other physiological information thus guaranteeing the integration between ECG and the effectiveness of the proposed techniques for the two distortion measurement metrics have been used:. It is found that the proposed technique provides high security protection for patients data with low (less than 1%) distortion and ECG data remains diagnosable after watermarking and as well as after watermarks are removed from the watermarked data.

I.INTRODUCTION:

Hiding the confidential data in to other form of data is call as data steganography. The HIPAA regulations act says that, there should be a protection and security is provided to the patient's confidential information which is sent through the public network. As the patient privacy is important so patient can control his/her confidential health information that if anyone can access or control the information like name, age, gender, ID no., address, telephone number. Monitoring patients at their home can reduce due to increasing rush at hospitals and care centers like medical. Hiding patient's confidential information and other physiological data in ECG signal is the main goal. Provide secrecy, integrity, and accessibility to confidential information. The main branch of cryptography is steganography that involves hiding information in other secondary information. Hiding the information decrease the chance of the information being detected. Medical images has smaller size were the ECG signal has greater size. Therefore instead of medical image ECG signal is used in steganography process. The ECG signal of the patients is used to hide physiological data of patient like temperature, glucose level, blood pressure, position, etc., which are collected by using Body Sensor Networks (BSNs) at home and stored on hospital server by transmitted via network. Then that data is diagnosed by monitoring systems at hospital. At the same cost that the patient privacy is protected against intruders while data navigate in open network and stored in hospital servers. This technique allows hiding the confidential information of the patient in to ECG signal and thus gives guarantees the patient's privacy and discretion.

The main objective of steganography is to put the undisclosed message in the other coated media so that nobody can see that and both doctor and patient can communicate in secret way. The data security has improved by combining the more number of methods of steganography and the other techniques related to data hiding. The first steganography method is on hiding patient data which is confidential, inside ECG signal of patient which can be called as host signal. Additionally, the proposed method uses model which involves encryption to allow extracting the data which is hidden. That data can be extracted by only the authorized persons like doctors. In this paper, for the host signal, the ECG signal of patient is used and the patient private information and other physiological reading are hiding inside it. The main fact is that the ECG signal which is used here as a host signal because ECG information will collect by many of the healthcare systems. As compare to other host signal, ECG signal has large size thus it can hide more data than hiding data in other host signal. Therefore, for the small size secrete data the ECG signal will be right as a host. The proposed technique fallows the HIPPA, by providing open access for ECG signal and provides security for patient's confidential information from unauthorized access. In this method the ECG signal with temperature, blood pressure and glucose level are collected by using body sensor network. By using Bluetooth the physiological readings collected from sensor are transfer to patient's PDA device. The patient's PDA device contains steganography technique and embedding operation which embed the patient secret information and patient physiological data inside the. ECG signal i.e. host signal.

II.LITERATURE SURVEY:

To provide security to patient confidential data, there is no. of methods [4], [1], [5]. However, one approach proposed which is on using steganography. Were, to protect confidential information of the patient it used medical image to stored secret information. How much data can be stored in medical image are the challenging factors of this method and up to which level this method is safe. Kai-meiZheng and XuQian [8] proposed a fresh technique for data hiding which is reversible and depending on wavelet transform. Furthermore, this method dose not used user define key, so in this algorithm the security is depends only on algorithm. At last, this algorithm is not useful for the abnormal ECG signal because in it QRS complex is absent. However this algorithm is depending only on normal ECG signal were QRS complex can be easily find. H. Danyali and H. Golpira [7] proposed a new technique where medical images are used like host signal. So this technique is not useful for ECG signal. Moreover, this algorithm has low capacity. Additionally, the encryption key is not concerned in its watermarking process. In our approach to use ECG signal in data hiding process. To decompose the ECG signal DWT technique is used. Then the patient's confidential information is embedded with share key inside decomposed ECG signal. XOR ciphering method is used with a shared key which is an ASCII coded. Here first security is provided with a shared key which is an ASCII coded. Second security is provided at the time of embedding operation by applying inimitable scrambling matrix. And third security is providing by selection steganography level vector at the time of inverse wavelet transform. So here three tier securities are provide to the patient's confidential information.

III ARCHITECTURE:

The proposed architecture for the system as shown in Figure.1 first collects the patient's ECG signal and other physiological readings using different body sensors. The signals are then sent to the smart phone via Bluetooth on which the secret data of the patient is stored. The secret data is encrypted in the smart phone using some encryption technique. The signals are then transformed into discrete wavelets using Discrete Wavelet Transformation (DWT). The five-level DWT applied on the host signal results into 32 sub-bands. The encrypted data is then embedded into the sub-band's coefficient using LSB substitution.

The 32 steganographed sub-bands are recomposed using inverse wavelet re-composition into a single steganographed ECG signal. The smart phone then sends the signal to the hospital server through Internet. The hospital server extracts the data from the host signal which can then be accessed by authorized personnel. Only the authorized people have the security key to access the hidden data.

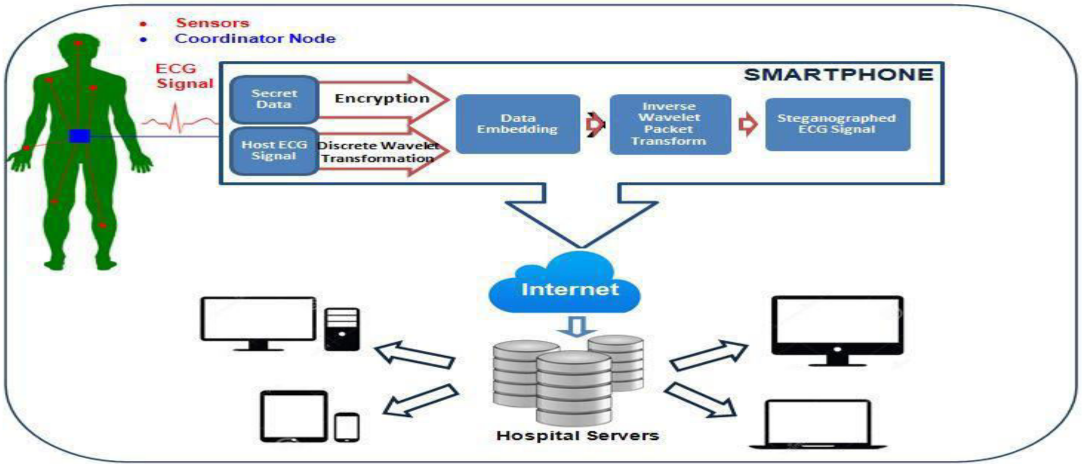

Figure.1: Architecture for ECG steganography and transmission of steganography ECG signal

This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. In image steganography the information is hidden exclusively in images. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret . Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of Steganography is partly defeated. The strength of Steganography can thus be amplified by combining it with cryptography. In the process of Steganography, cover image is used to hide the watermark image and it is transmitted over the channel. At the receiving side, the watermark is extracted by leaving the cover image. In this process some details of watermark image is lost as we are not considering cover image. To overcome the disadvantage of Steganography we go for watermarking technique. DWT AND SVD

IV.PROPOSED SYSTEM METHODOLOGY

A. DWT

Wavelets are special functions which, in a form analogous to sines and cosines in Fourier analysis, are used as basal functions for representing signals [7]. For 2-D images applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL1, LH1, HL1 and HH1. The sub-band LL1 represents the coarse-scale DWT coefficients while the sub-bands LH1, HL1 and HH1 represent the fine-scale of DWT coefficients. According to the character of HVS, human eyes are sensitive to the change of smooth district of image, but not sensitive to the tiny change of edge, profile and streak. Embedding the watermark in the higher level sub bands increases the robustness of the watermark. However, the image visual fidelity may be lost, which can be measured by PSNR. With the DWT, the edges and texture can be easily identified in the high frequency band .Therefore it’s hard to conscious that putting the watermarking signal into the big amplitude coefficient of high-frequency band of the image DWT transformed. Then it can carry more watermark signal and has good concealing effect. Whenever an image is subjected to dwt transform the details of watermark image is observed on the cover image. So that any person viewing at the channel can have information that something is there behind the cover image.

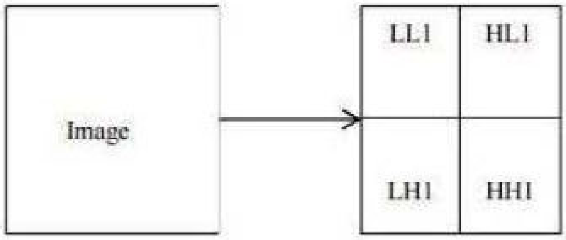

Fig-1: Single Level DWT

Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In particular, this property allows the exploitation of the masking effect of the human visual system such that if a DWT coefficient is modified, only the region corresponding to that coefficient will be modified. In general most of the image energy is concentrated at the lower frequency sub-bands LLx and therefore embedding watermarks in these sub-bands may degrade the image significantly. Embedding in the low frequency sub bands, however, could increase robustness significantly. On the other hand, the high frequency sub-bands HHx include the edges and textures of the image and the human eye is not generally sensitive to changes in such sub-bands. This allows the watermark to be embedded without being perceived by the human eye. The compromise adopted by many DWT based watermarking algorithm, is to embed the watermark in the middle frequency sub-bands LHx and HLx where acceptable performance of imperceptibility and robustness could be achieved. to overcome the disadvantage of dwt we are going for the combination of dwt-svd domain.

B. SVD

SVD is an effective numerical analysis tool used to analyze matrices. In SVD transformation, a matrix can be decomposed into three matrices that are of the same size as the original matrix. From the view point of linear algebra, an image is an array of nonnegative scalar entries that can be regarded as a matrix. The singular value decomposition of a matrix is a factorization of the matrix into a product of three matrices. Given an m×n matrix A, where m ≥ n, the SVD of A is defined as $A = U\sum V^T$ where U is an m×n column-orthogonal matrix whose columns are referred to as left singular vectors; Σ =diag (σ1, σ2, . . . , σn) is an n×n diagonal matrix whose diagonal elements are nonnegative singular values arranged in descending order; V is an n×n orthogonal matrix whose columns are referred to as right singular vectors. SVD efficiently represents intrinsic algebraic properties of an image, where singular values correspond to brightness of the image and singular vectors reflect geometry characteristics of the image. Since slight variations of singular values of an image may not affect the visual perception, watermark embedding through slight variations of singular values in the segmented image has been introduced as a choice for robust watermarking .

Proposed DWT-SVD Based Watermarking

A. Watermark Embedding

The proposed watermark embedding algorithm is shown in Figure 2.

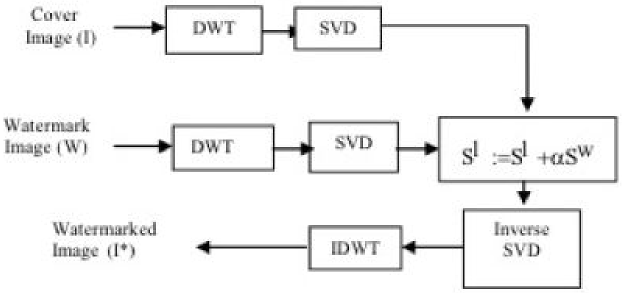

Fig-2: Block Diagram of the proposed watermark Embedding Algorithm

The steps of watermark embedding algorithm are as follows:

1. Apply DWT to the cover image to decompose it into LL, HL, LH, and HH sub bands.

2. Apply SVD to the low frequency sub band LL of the cover image:

$$I^l = U^l S^l V^l$$

3. Apply DWT to the visual watermark.

4. Apply SVD to the low frequency sub band of watermark:

$$w \quad = U^w S^w V^w$$

5. Modify the singular values of the cover image with the singular values of watermark image

$$S^{*l} = S^l + \alpha S^w$$

Where □ is scaling factor, Sl and Sw are the diagonal matrices of singular values of the cover and watermark images, respectively.

6. Apply inverse SVD on the transformed cover image with modified singular values

$$I^{*l} = U^l S^{*l} V^l.$$

.

7. Apply inverse DWT using the modified coefficients of the low frequency bands to obtain the watermarked image.

1. Flow chart for the above Algorithm

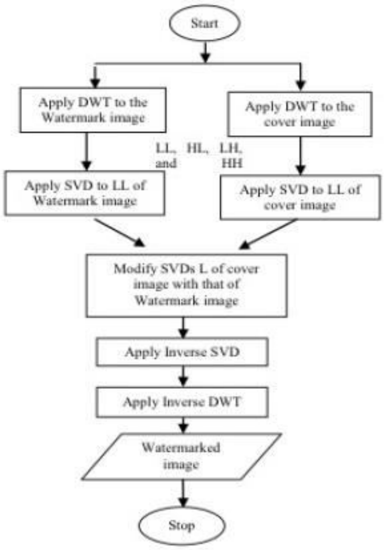
Start
Apply DWT to the Watermark image
Apply DWT to the cover image
LL, HL, LH, and HH
Apply SVD to LL of Watermark image
Apply SVD to LL of cover image
Modify SVDs L of cover image with that of Watermark image
Apply Inverse SVD
Apply Inverse DWT
Watermarked image
Stop

Fig-3: Flow Chart of Watermark Embedding

B. Watermark Extraction

The proposed watermark extracting Algorithm is shown in Figure 4.

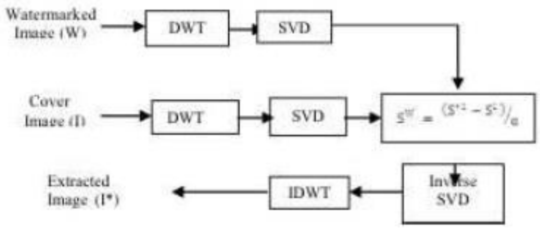

Fig-4: Block diagram of the proposed Watermark Embedding Algorithm

The steps of watermark extracting algorithm are as follows and the flow chart will as same as shown for watermark embedding:

1. Using DWT, decompose the watermarked image I* into 4 sub bands: HH, HL, LH and LL.

2. Apply SVD to low frequency sub band LL: I∗ = U∗ S∗ V∗

3. Extract the singular values from low frequency sub band of watermarked and cover image S_ = (S∗ −S) ÷ α where S contains the singular of the cover image.

4. Apply inverse SVD to obtain low frequency coefficients of the transformed watermark image.

5. Apply inverse DWT using the coefficients of the low frequency sub-band to obtain the watermark image.

RESULTS

In this study, we used gray scale image as our host image of size252 × 252, and the watermark image is of same size. In our experiments, we used the scaling factor □ □ 0.1. Below figure shows cover image, watermark, watermarked image and the extracted watermark.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

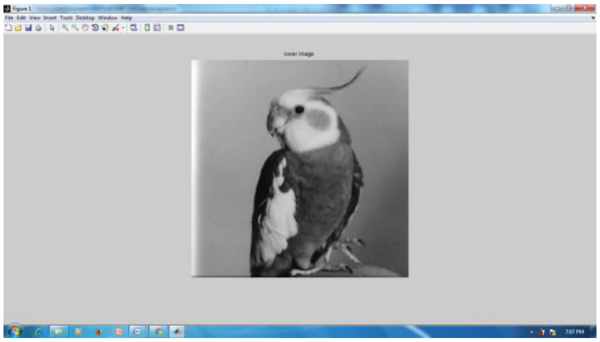

Fig: cover image

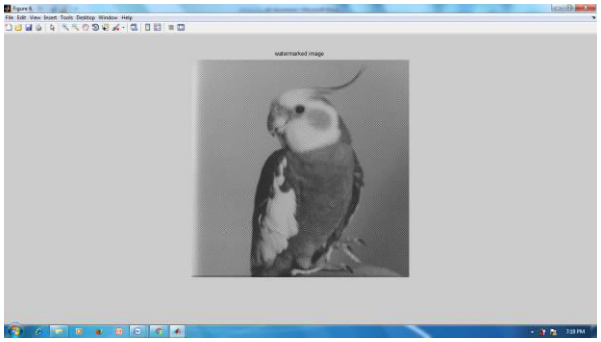

Fig: Watermark image

Dwt operation cover image

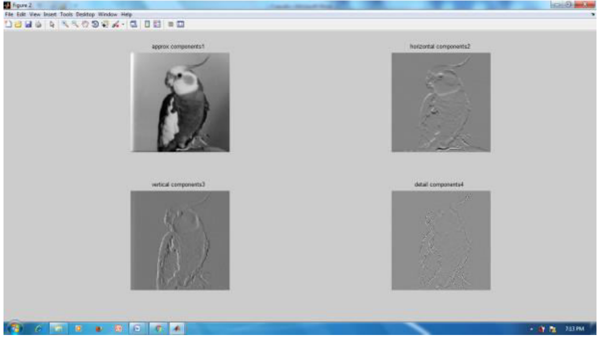

Fig: Dwt operation cover image

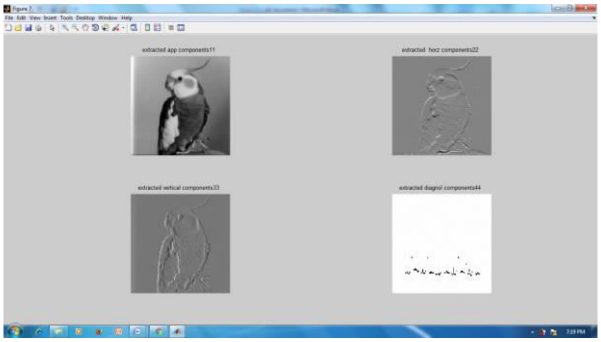
Figure 7
File Edit View Insert Tools Desktop Window Help
extracted app components11
extracted horz components22
extracted vertical components33
extracted diagnol components44

Fig: Extracted dwt operation

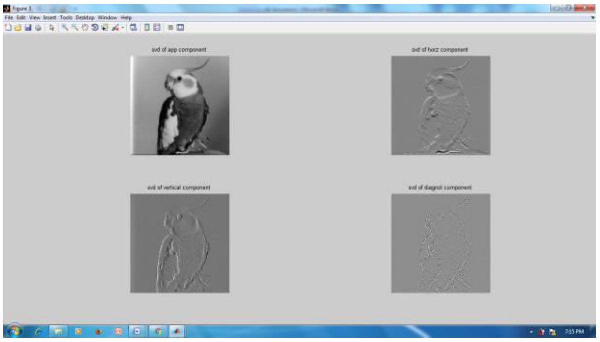

Fig: SVD operation cover image

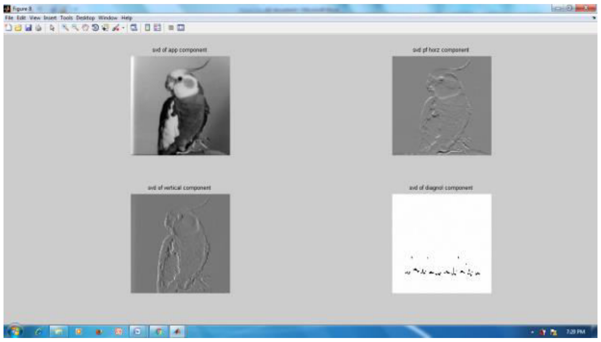

Fig: Extracted SVD operation

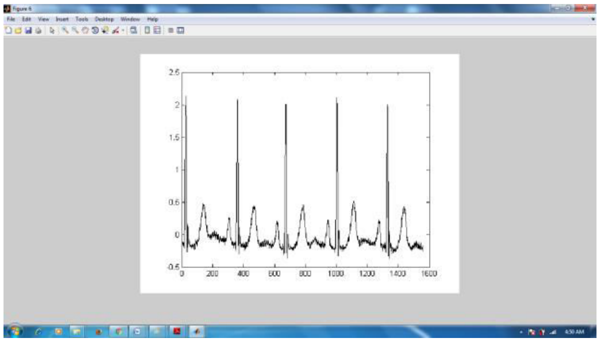

Fig: Input ECG signal

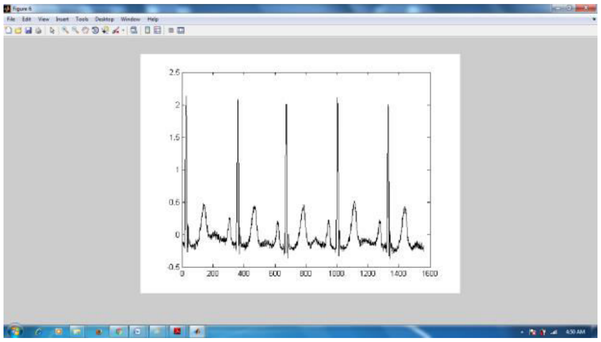

FIG: Output extract ECG signal

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

When watermarks are extracted, similarity of the watermarked and cover image can be defined by the PSNR (Peak Signal to Noise Ratio) criterion:

$$PSNR = 10log_{10}(255^2 \div MSE)$$

where MSE (Mean Square Error) is defined as:

$$MSE = (1 \div M \times N)\sum_{x=1}^{M}\sum_{y=1}^{N}(P(x,y) - P'(x,y))^2$$

where m and n are the dimensions of the images X and Y. PSNR is measured in Db The PSNR value obtained in DWT-SVD domain is higher than that of DWT.

CONCLUSION

We introduced another watermarking technique in view of DWT-SVD to insert a watermark picture which can be as huge as the cover picture. Changing particular estimations of the cover picture in DWT space gives high strength against regular assaults. High PSNR also, connection coefficient of watermarked picture is another useful purpose of the calculation as the outcome of DWT usage. Another preferred standpoint of this technique is the likelihood to implant a vast watermark in the cover picture. This work can be additionally broadened with variety in DWT like RDWT.

REFERENCES

[1] D. Kundur, D. Hatzinakos, Towards robust logo watermarking using multiresolution image fusion, IEEE Transactions on Multimedia 6 (2004) 185–197.

[2] Q. Li, C. Yuan, Y.Z. Zong, Adaptive DWT-SVD domain image watermarking using human visual model, ICACT-2007, 2001, pp. 1947–1951.

[3] D.S. Chandra, Digital image watermarking using singular value decomposition, Proceedings of the 45th Midwest Symposium on Circuits and Systems (MWSCAS'02), vol. 3, 2002, pp. 264–267.

[4] Liu, R. and Tan, T. (2002) An SVD-based watermarking scheme for protecting rightful ownership, IEEE Transactions on Multimedia, Vol.4, No.1, Pp. 121-128.

[5] A. Sverdlov, S. Dexter, A.M. Eskicioglu, "Robust DCT-SVD Domain Image Watermarking For Copyright Protection: Embedding Data In All Frequencies", Proceedings of the 13th European Signal Processing Conference (EUSIPCO2005), Antalya, Turkey, September 2005.

[6] L. Liang, S. Qi, "A new SVD-DWT composite watermarking", Proceedings of IEEE International Conference on Signal Processing (ICSP) , 2006.

[7] V. Santhi, A. Thangavelu, "DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space", International mJournal of Computer Theory and Engineering, vol. 1, no. 4, pp. 424-429.

[8] C.C. Chang, C.C. Lin, Y.S. Hu, "An SVD oriented watermark embedding scheme with high qualities for the restored images", International Journal of Innovative Computing, Information and Control (ICIC), vol. 3, no. 3, pp. 609-620.

[9] P. B. Paul, and X. Ma, "Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition", IEEE Transactions on Circuits and Systems for Video Technology, vol.15, no.1, pp.96-102