IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-3, Mar 2019 E-ISSN: 2347-2693

Digital Image Watermarking Based on DWT and SVD for Fingerprint Security

Komal Ramteke[1*], Akhil Anjikar[2], Sushil Chavhan[3]

[1,2] Department of Information Technology, Rajiv Gandhi College of Engineering and Research, Nagpur, Maharashtra, India
[3]Department of Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra ,India

Corresponding author: komalramteke03@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i3.10731078 | Available online at: www.ijcseonline.org

Accepted: 15/Mar/2019, Published: 31/Mar/2019

Abstract— Protection of biometric data is gaining interest and digital watermarking techniques are used to protect the biometric data from either accidental or intentional attacks. Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. The information used for identification or verification of a fingerprint, mainly lies in its minutiae. Advanced image watermarking is a valuable answer for the issue of data security, copyright and system security. The proposed algorithm is based on Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT) to improve the recognition performance as well as the security of fingerprint based biometric system which will provide adequate security to fingerprint data without degrading visual quality. The algorithm converted the minutiae into binary watermark, increasing embedded information capacity. Different experiments are performed to test the effectiveness and robustness of proposed algorithm and the experimental results shows that the scheme is effective and robust against various image processing attacks. Results shows higher PSNR and NC values under general image processing.The algorithm can satisfy the transparency and robustness of the watermarking system very well and the useful information can be extracted accurately even if the fingerprint is severely degraded.

Keywords— Arnold transform, Digital Watermarking, DWT, Fingerprint minutiae, Normalized coefficient, Peak signal to noise ratio, SVD

I. Introduction

With the development of network and multimedia technologies, multimedia copyright protection and content authentication have become serious problems that need to be solved urgently. Multimedia and network security issues are classically handled through cryptography; however, cryptography ensures confidentiality, authenticity, and integrity only when a message is transmitted through a public channel such as an open network. It does not protect against unauthorized copying after the message has been successfully transmitted. Digital watermarking is an effective way to protect copyright of multimedia data even after its transmission. Among the various biometrics, fingerprints are more famous in the authentication area, as they are unique to each person and are widely used in identification and verification of personal individuality. However, they are susceptible to accidental and intentional attacks, when transmitted over network. Thus, a defensive scheme is needed which will preserve fidelity and prevent modifications. Digital watermarking technology provides strong solution for it. DWT and SVD are two most popular tools used in watermarking algorithm. With the increasing use of SVD, the digital watermarking technology in transform domain has been greatly developed.

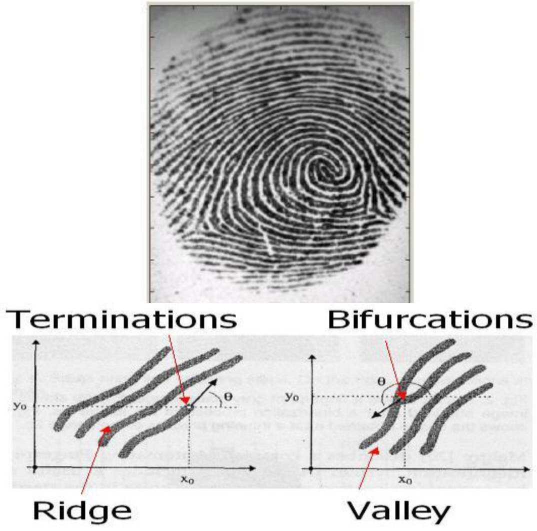
Digital watermarking is the process of embedding or hiding digital information called watermark into a multimedia product such as an image, audio or video. Digital watermarks should be imperceptible, difficult to remove, i.e., robust to common attacks, and of large capacity. Existing watermarking schemes can be divided into two categories: spatial domain schemes and transform domain schemes. Spatial domain schemes embed data by directly modifying pixel values of the host image, while transform domain schemes embed data by modifying transform domain coefficients. The major advantage of transform domain methods is their superior robustness to common image distortions.

The typical Transformation-Domain Methods are mostly based on the domain of Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), etc. Wavelet transform is superior to time-frequency transform for its inner predominance. For example, wavelet has the character of multi-resolution, which can avoid the rectangle brought by DCT. As DWT decomposes images into four bands, DWT-based watermarking schemes can embed data in all frequencies. This result in robustness to a wide range of attacks for embedding in low and high frequency bands are complementary. Recently, some researchers began to make use of spatial domain technique Singular Value Decomposition (SVD) to embed a Watermark. SVD is a compression technique that can be used in a wide range of applications where data may be organized in a matrix representation. SVD is suitable for watermarking applications since some largest singular values are sufficient to embed instead of using all singular values.

A. Fingerprint minutiae

Fingerprints are the patterns formed on the epidermis of the fingertip. It is believed with strong evidences that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have being used for identification and forensic investigation for a long time. A fingerprint is composed of many ridges and furrows.

However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by Minutia, which are some abnormal points on the ridges [9]. Among the variety of minutiae types reported in literatures, two are mostly significant and in heavy usage: one is called termination, which is the immediate ending of a ridge; the other is called bifurcation, which is the point on the ridge from which two branches derive.



(a) (b)

Figure 1-(a) Typical fingerprint image (b) Minutiae. (Valley is also referred as Furrow, Termination is also called Ending and Bifurcation is also called Branch)

B. Discrete Wavelet Transform

In DWT transformation the image is divided into four multi resolution sub-bands LL, LH, HL and HH using DWT. Fine-scale DWT coefficients are represented by LH, HL, HH sub-bands and coarse-scale DWT coefficients are represented by LL sub-bands. LL sub-band is further decomposed into four multi resolution sub-bands to obtain next coarser wavelet coefficients [12-14]. This process is repeated several times determined by application for which it is used. For k level DWT, there are (3*k) + 1 sub-bands available. Wavelet transform is a time-frequency domain combined analysis method. It has multi-resolution analysis features. After wavelet decomposition, many signal processing, such as compression and filter are likely to change the high frequency wavelet coefficients. If the watermark sequence is embedded into this part, its information may be lost in the processing in sequence, which will reduce the robustness of the watermark [3]. In order to ensure the watermark has a better imperceptibility and robustness, the approximation sub-image LL_3 coefficients are chosen to embed watermark. The three level 2-D DWT decomposition of an image is shown in figure as below-

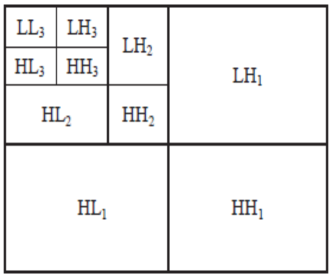


Figure 2-Three level wavelet decomposition

C. Singular Value Decomposition

SVD is one of the effective tool to analysis the matrices. While using the SVD transformation a matrix is decomposed into three matrices U, S, V. U and V are the unitary matrices and S is a diagonal matrix .If a m× n image is represented as a real matrix A , it can be decomposed as: A =USVT . It is called a singular value decomposition of A . Where U is a m×m unitary matrix, S is a m×n matrix with nonnegative numbers on the diagonal and zeros on the off diagonal, and VT denotes the conjugate transpose of V, an n× n unitary matrix. The nonnegative components of S represent the luminance value of the image [7].Changing them slightly does not affect the image quality and they also don't change much after attacks, watermarking algorithms make use of these two properties.

$$I= U.S.V^T =\Sigma^N_{K=1}\, \mu_k.\ s_k.\ v_k^T$$

$$\text{With } U=[u_1,u_2,u_{3,\dots\dots}] \text{ and } V=[v_1,v_2,v_{3,\dots\dots}] \quad \dots\dots\dots (1)$$

D. Arnold Transform

To confirm the security and improve the robustness of the proposed watermarking scheme, the watermark should be pre-processed before embedded into the original image. Arnold Transform is commonly known as cat face transforms and is only suitable for N×N images digital images. Arnold transform can be expressed as-

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} \text{ Mod N} \quad \ldots\ldots\ldots\ldots\text{.. (2)}$$

Where (x, y) is the location coordinates of the original image pixels, and $(x^{'}, y^{'})$ is the location coordinates of image pixels that after transform[9].Arnold Transform is periodic in nature. The decryption of image depends on transformation periods. Period changes in accordance with size of image. Iteration number is used as the encryption key. When Arnold Transformation is applied, the image can do iteration, iteration number is used as a secret key for extracting the secret image.

Rest of the paper is organized as follows, Section I contains the introduction of Digital watermarking scheme ,DWT,SVD and Fingerprint Minutiae , Section II contain the related work of DWT and SVD watermarking systems, Section III contain the proposed approach to protect biometric watermarking scheme, Section IV describes the Experimental results, and Section V concludes research work with future directions.

II. Related Work

Early work of digital watermarking is done in spatial domain [6].Recent developments are mostly focused on frequency domain and wavelet domain watermarking techniques [1-4]. R.Chouhan, A. Mishra, P. Khanna proposed DWT based Digital Watermarking in [3], uses a wavelet-based blind watermarking scheme has been proposed as a means to provide protection against false matching of a possibly tampered fingerprint by embedding a binary name label of the fingerprint owner in the fingerprint itself. Khalil Zebbiche, Lahouari Ghouti, Fouad Khelifi [4], introduce an application of wavelet based watermarking method to hide the fingerprint minutiae data in fingerprint images. The application provides a high security to both hidden data (i.e. fingerprint minutiae) that have to be transmitted and the host image (i.e. fingerprint). The original unmarked fingerprint image is not required to extract the minutiae data. The method is essentially introduced to increase the security of fingerprint minutiae transmission and can also used to protect the original fingerprint image. Weimin Yang, Xiaoning Zhao [7], introduce a new watermarking algorithm is based on Singular Value Decomposition (SVD) and discrete wavelet transform (DWT). The algorithm uses a gray image as a watermark, increasing embedded information capacity. The algorithm can satisfy the transparence and robustness of the watermarking system very well. . Here 3-level wavelet transformation is performed on original image and intend to embed watermark in LL_3 also the Arnold transform for watermark image is done before embedding process.

III. Proposed Watermarking Scheme

In the proposed approach, initially the watermark image is produced by extracting the minutiae points (ending, bifurcation) from fingerprint image and then converted to binary watermark image. Next the cover fingerprint image is decomposes into 3-level two-dimensional DWT coefficients and the approximation sub-band LL3 is opted to embed watermark .The produced watermark image is additionally undergo Arnold transformation before embedding process is perform. After that by applying SVD concept on watermark image and selected sub-band of cover image, the watermarked image coefficients are produced. Then inverse DWT is apply to determinately generate the watermarked image in which the watermark is embedded. The watermark extraction process is performing in precisely the inversion order of watermark embedding process.

The proposed watermarking scheme for fingerprint images has been shown in fig. The cover image is the fingerprint while the watermark is a binary image identically equal to the minutiae of the cover fingerprint. The scheme has been divided into two sections:

A. Watermark Embedding
B. Watermark Extraction.

A. *Watermark embedding scheme*

The steps of minutiae watermark embedding as are follows:

Step 1: The fingerprint image is decomposed into its 3-level two-dimensional DWT coefficients. Out of the all sub-bands, only LL_3 approximation sub-band is selected.

Step 2: Fingerprint Pre-processing
A real fingerprint might have discontinuities that might lead to erroneous minutiae. Therefore, minutiae extraction is preceded by fingerprint pre-processing. This step involves normalization, ridge orientation and frequency estimation. The filtered output is then binaries and thinned to one-pixel width.

Step 3: Minutiae Extraction
Minutiae points such as end points and bifurcation points are identified by calculating Crossing number (CN). The Crossing Number method extracts the ridge endings and bifurcations from the skeleton image by examining the local neighbourhoods of each ridge pixel using a 3×3 window. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight neighbourhoods.

$$CN = 0.5 \sum_{i=1}^{8} | \;P_i – P_{i+1}\; |, \quad P_1 = P_9 \quad \ldots\ldots\ldots \text{(3)}$$

If crossing Number is 1, 2 and 3 or greater than 3 then minutiae points are classified as Termination, Normal ridge and Bifurcation respectively.
The minutiae thus extracted have the following information: x and *y* coordinates and the type of minutiae (ending or bifurcation). All these information is converted to binary form by 8-bit representation and a binary watermark is generated by concatenating the eight individual bit planes.
Step 4: Perform Arnold transform for watermark image W.
Step 5: We obtain the watermarked image coefficients matrix A_w through the following three steps:

1. $A = USV^T$
2. $S + W = U_W S_W V_W^T$
3. $A_W = US_W V^T$ ……………….(4)

Apply inverse wavelet transform for original image, and then altering the double-precision real number to unsigned 8-bit integer. Thus, obtain the watermarked image in which watermark are embedded.

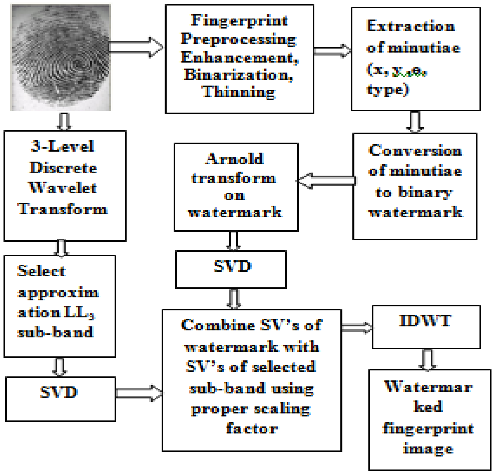

Fingerprint Preprocessing Enhancement, Binarization, Thinning
Extraction of minutiae (x, y, θ, type)
3-Level Discrete Wavelet Transform
Arnold transform on watermark
Conversion of minutiae to binary watermark
SVD
Select approximation LL3 sub-band
Combine SV's of watermark with SV's of selected sub-band using proper scaling factor
IDWT
SVD
Watermarked fingerprint image

Figure 3. Diagram of embedding watermark

B. *Watermark extraction scheme*

We can extract the watermark by the inverse calculation of watermark embedding:
Step 1: Perform a 3-level wavelet transform using haar wavelet for watermarked image, and obtain low-frequency wavelet coefficient LL_3 (denotes as A*).
Step 2: Apply SVD to the A*, such that $A^* = U^* S_1 {}^* V^T{}^*$, and obtain U *,$S_1$* and V^T*.

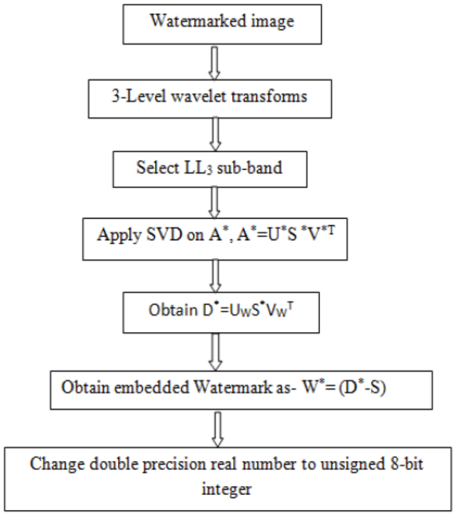

Watermarked image
3-Level wavelet transforms
Select LL3 sub-band
Apply SVD on A*, A*=U*S*V*T
Obtain D*=UWS*VWT
Obtain embedded Watermark as- W*=(D*-S)
Change double precision real number to unsigned 8-bit integer

Figure 4. Diagram of extracting watermark

Step 3: Now by using values of U w, V_W and S_1 *, obtain D* according $D^* = U_W S_1 {}^* V^T$, in the end we can obtain the watermark which is embedded according to W* = (D* −S) /α.
Step 4: Conclusively transmuting the double-precision real number to unsigned 8-bit integer for watermark image, and perform inverse Arnold transform for watermark image.
Step 5: Minutiae points are then regenerated by stacking bit planes and converting them back to decimal system.

IV. Experimental Results and Discussion

The experiments are basically divided into 2 types: test on robustness and test on fidelity. The cover image is 256×256 grayscale host fingerprint image and watermark image is 32×32 binary image equivalent to minutiae of fingerprint image.

A. *Tests on Robustness*

The performance of the proposed fingerprint watermarking scheme is evaluated under various image processing attacks. The extraction of watermark is tested under various attacks, noising attacks (salt and pepper, Gaussian noise), de-noising attacks (median filter), geometric attacks (rotation, cropping) and image processing attack (blurring). The normalized coefficient is used to measure the similarities of extracted watermarks. The NC values are retrieved when the watermarked fingerprint image is facing different attacks. The high correlation value clearly indicates robustness of the algorithm against major attacks.Figure (5) Shows the original host fingerprint, original watermark, watermarked fingerprint and extracted watermark images .The calculated PSNR between host fingerprint and watermarked fingerprint image is 99 and MSE=0. The correlation coefficient between embedded and extracted watermark without performing any attack is 0.9888.

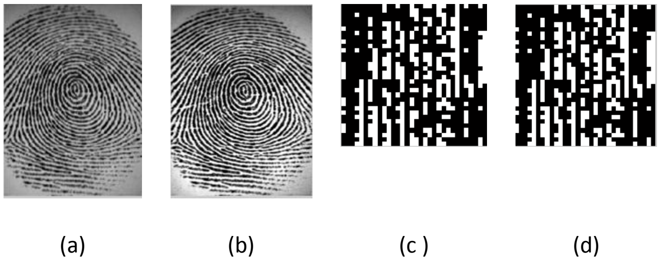


Figure5-(a) Original host fingerprint (b) Watermarked fingerprint with PSNR=99 and MSE=0 (c) original watermark (d) Recovered watermark

Figure(6). shows the various attacked watermarked fingerprint images and extracted binary watermarks from each of them.

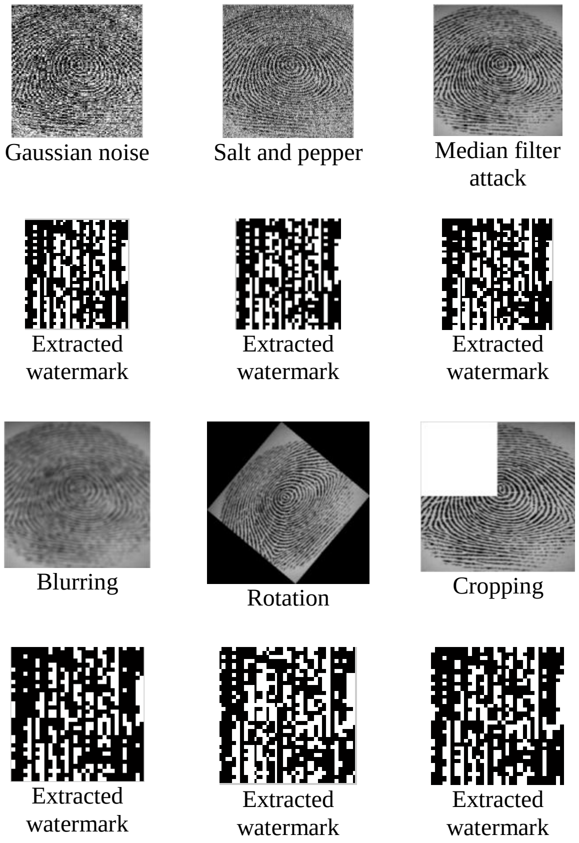


Figure 6. Various attacked watermarked fingerprint images and extracted binary watermarks

Table-1. Shows verification accuracy of extracted watermark when watermarked fingerprint is attacked.

TABLE 1

Sr. No.	1	2	3	4	5	6	7
Attack	No attack	Gaussian noise	Salt and pepper	Median filtering	Blurring	Rotation	Cropping
NC	0.9888	0.9485	0.9409	0.9533	0.9506	0.8559	0.9415

We specified the verification precision of extracted watermark when watermarked fingerprint is attacked by different image processing attacks. The verification precision is calculated in terms of normalized coefficient which is considered as relatives attribute measure between embedded watermark and extracted watermark without any attack and under attacks. The NC under no attack is 0.9888 which proves that the minutiae information i.e. binary watermark is accurately extracted without degrading the visual quality of host fingerprint image.

B. Tests on Fidelity

Fidelity means that the perceived quality of the host fingerprint image should not be distorted by the presence of the watermark. The Peak Signal to Noise Ratio (PSNR) is used as a measure of the quality of a watermarked image. The average PSNR for the all watermarked fingerprints are calculated equals to 99 with MSE=0.At these PSNR values no quality degradation in the watermarked fingerprint was perceived.

V. CONCLUSION AND FUTURE SCOPE

The watermarking scheme is based on hybrid transform domain DWT and spatial domain SVD for fingerprint images. Due to spatio-frequency resolution of DWT, it offers more degrees of freedom as compared with DCT. The main objective of this scheme is to provide security and robustness to fingerprint images. The watermark (i.e. binary equivalent of minutiae) is embedded into LL_3 sub-band because watermark detection at lower resolution is computationally effective. Also in order to ensure watermark has better imperceptibility and robustness, the approximation sub-image LL_3 coefficient are chosen to embeds watermark. Applying Arnold transform to watermark image makes result even better. Subsequently the embedded watermark can be extracted from watermarked image successfully under normal extraction or even in the presence of various image processing attacks.

Future Scope

- Different combinations of DWT, DCT and SVD may give better results.
- The combination of spatial domain and frequency domain approaches will help to improve the robustness of fingerprint images.

- Use of clear fingerprint database will give improved results.
- The proposed watermarking algorithm can be significantly using for other biometric data such as face template in combination with fingerprints and preserve the integrity of both.

REFERENCES

[1] D. Mathivadhani, C. Meena, "A Comparative Study on Fingerprint Protection Using Watermarking Techniques". In Global Journal of Computer Science and Technology, vol. 9, no. 5, pp. 98-102, 2010.

[2] Rajlaxmi Chouhan, Pritee Khanna, "Robust Minutiae Watermarking in Wavelet Domain for Fingerprint Security". In World Academy of Science, Engineering and Technology 60 2011.

[3] R. Chouhan, A. Mishra, P. Khanna, "Wavelet-based robust digital watermarking scheme for fingerprint authentication". In Proc. International Conference on Intelligent Computational Systems, pp. 29-33, 2011.

[4] Khalil Zebbiche, Lahouari Ghouti, Fouad Khelifi School of Electronics, Electrical Engineering and Computer Science, "Protecting Fingerprint Data using Watermarking". In Proceedings of the First NASA/ESA Conference on Adaptive Hardware and Systems (AHS'06) 0-7695-2614-4/06, 2006 IEEE.

[5] Ms.Jalpa M.Pate1, Mr.Prayag Patel, "A brief survey on digital image watermarking techniques". In International Journal for Technological Research in Engineering Volume 1, Issue 7, March-2014 ISSN.

[6]] S.D. Lin, Chin-Feng Chen, "A robust DCT-based watermarking for copyright protection", (2000) IEEE Transactions on Consumer Electronics, vol. 46, no. 3, pp. 415 - 421.

[7] Weimin Yang, Xiaoning Zhao, College of Computer and Information Engineering Central South University of Forestry & Technology Changsha, Hunan, China," A Digital Watermarking Algorithm Using singular Value Decomposition in Wavelet Domain" 978-1-61284-774-0/11,2011 IEEE.

[8] Sachin Mehta, Rajarathnam Nallusamy, Ranjeet Vinayak Marawar, Balakrishnan Prabhakaran, "A study of DWT and SVD based Watermarking Algorithms for Patient Privacy in Medical Images". In 2013 IEEE International Conference on Healthcare Informatics.

[9]Ravi. J, K. B. Raja, Venugopal. K. R," Fingerprint recognization using minutiae score matching". International Journal of Engineering Science and Technology Vol.1 (2), 2009, 35-42.

[10] Divya Saxena, Department of Applied Science, Vishveshwarya Institute of Engineering and Technology, G.B.Nagar, India," Digital Watermarking Algorithm based on Singular Value Decomposition and Arnold Transform". In International Journal of Electronics and Computer Science Engineering, ISSN-2277-1956.

[11] J. Delaigle, C. De Vleeschouwer, B. Macq, " Psychovisual Approach to Digital Picture Watermarking", Journal of Electronic Imaging, vol. 7, no. 3, pp. 628-640, 1998.

[12] A. Graphs, "An Introduction to Wavelets," IEEE Computational Science and Engineering, vol. 2, no. 2, pp. 50-61, 1995.

[13] R.C. Gonzalez, R.E. Woods, Digital Image Processing. New Jersey: Prentice Hall, Upper Saddle River, 2002.

[14] A. Abu-Errub, A. Al-Haj, "Optimized DWT Based Image Watermarking," (2008) Proc. IEEE First International Conference on Applications of Digital Information and Web Technologies, pp. 1-6.

[15] A. Al-Haj, "Combined DWT-DCT Digital Image Watermarking", (2007) Journal of Computer Science, vol. 3, no. 9, pp. 740-746.

[16] Pooja Chinchmalatpure, Komal. Ramteke, Prashant Dahiwale,"Adaptive DWT and SVD domain digital image watermarking for fingerprint security", (2014) Journal of Emerging Technologies and Innovative Research, Volume 2, Issue 6,DOI/ JETIR1506039.

[17] Komal. Ramteke,Swati Ramteke "Hybrid DWT and SVD based Biometric Watermarking for Fingerprint Authentication", (2017) International Journal of Advanced Research in Computer and Communication Engineering, Volume 7,Issue 1,DOI 10.17148/IJARCCE.2018.717.

[18] Pooja Chinchmalatpure, Komal. Ramteke, Prashant Dahiwale," Finger print Authentication by hybrid DWT and SVD based Watermarking ", (2014) 2nd IEEE International conference on Innovations in Information, Embedded and Communication Systems.

[19] Weimin Yang ; Xiaoning Zhao," A digital watermarking algorithm using Singular Value Decomposition in wavelet domain", (2011) International Conference on multimedia technology.

[20] Ben Wang ; Jinkou Ding ; Qiaoyan Wen ; Xin Liao ; Cuixiang Liu," An image watermarking algorithm based on DWT DCT and SVD", (2007) IEEE International Conference on Network Infrastructure and Digital Content.

[21] Qiang Li ; Chun Yuan ; Yu-Zhuo Zhong," Adaptive DWT-SVD Domain Image Watermarking Using Human VisualModel", (2007) IEEE The 9th International Conference on Advanced Communication Technology.

[22]B.Prasanalakshmi ," Biometric Cryptosystem Involving Two Traits And Palm Vein As Key", (2011) International Conference On Communication Technology And System Design 2011 Published by Elsevier Ltd. DOI:10.1016/j.proeng.2012.01.865.