A Hybrid Technique Using DWT and SVD Watermarking for Multimodal Biometric System

[1]Prachi Dholu, [2]Dr. A. C. Suthar,
[1]PG Student, [2]Director,
[1]Computer Engineering,
[1]L J Institute of Engineering and Technology, Ahmedabad, India

Abstract: Now-a-days, there is a growing usability and accessibility of internet which leads to growing concern over content protection of digital images. Thus to eliminate the traditional use of passwords and to ensure that the access to the image is restricted only to legitimate users, security solutions are increasingly combined with biometrics. Consequently, biometric-based watermarking algorithms, that involve embedding the identity of the owner, are proposed to solve ownership disputes. A multimodal biometric combines two or more biometric data recognition results such as a combination of a subject's fingerprint, face, iris and voice. This increases the reliability of a personal identification system that discriminates between an authorized person and a fraudulent person. The proposed methodology is a hybrid watermarking system which integrates two different techniques i.e. DWT and SVD together to increase the robustness and authentication of a person's identity. Additionally, we use a multimodal biometrics for the purpose of protecting and authenticating biometric data.

Keywords: **Watermarking; DWT; SVD; Biometrics; Multimodal; DCT;**

1. INTRODUCTION

Currently there is a need of biometrics based identification methods because the traditional methods like password (which can be forgotten) and identification card (which can be lost or stolen) has a weakness. Another reason to move towards biometrics is that it has the discriminative ability to discriminate between an authorized and a fraudulent person. Fingerprint, face recognition, iris detection, voice etc are most commonly used biometrics for authorization purposes. A multimodal biometric fusion technology which combines two or more biometrics data recognition results has been also used in order to increase reliability.

To authenticate one's identity one can make use of biometrics. A biometric measures an individual's unique physical or behavioral characteristics to recognize authenticate their identity. Physical biometrics are fingerprints, hand or palm geometry, retina, facial or iris etc [8]. Behavioral biometrics are signature, voice, keystroke pattern etc.

Biometrics is characterized on the basis of following features [8] :

Highly unique- chance of any two people having same characteristics is minimal.

Stable- feature does not change over time.

Easily captured- in order to provide convenience to the user.

Digital watermarking was developed to hide digital information and protect the copyright of multimedia signals such as images, audio, video etc [7]. Robustness of the watermark can be obtained if the watermark embedding is done in transform domain [1]. The number of watermarking techniques has been proposed using DWT to watermark fingerprint images. Besides these, frequency domain techniques such as DCT and SVD based watermarking techniques have gain importance. A hybrid watermarking system is used for ensuring security and integrity of biometric data.

Digital watermarking is an extension of watermarking concept in the digital world. A digital watermark is a pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc). Different kinds of watermarking techniques are: - Spatial Domain- Data is embedded in LSB of each pixel in the cover image. Transform Domain-Data is embedded by modulating coefficients of frequency domain image obtained using some transform such as DCT or DWT.

This paper is organized as follows: In section 2, we described the basic watermarking techniques and the related survey work. Then in section 3, from the analysis of previous work we propose the hybrid multimodal biometric watermarking system. Finally, in section 4, we conclude and discussed about work we proposed.

2. RELATED WORK

In recent years, there have been a few published papers on watermarking of biometric data. Biometric watermarking is a new research field, which is attracting more attention as security is the issue for biometric technology. Below is the brief discussion about the methods used by different researchers for biometric watermarking.

S. Anu H. Nair, P. Aruna [3] stated in their work that from different methods of watermarking such as DCT, SVD and BFOA, according to measured metric parameters BFOA performs better than other watermarking systems. Also they discussed the different methods in which SVD is as follows. The Singular Value Decomposition (SVD) is a factorization of a real or complex matrix. An A matrix can be decomposed into a product of three different matrices with SVD method [3].

Rohit Thanki and Komal Borisagar [4] proposed sparse watermarking technique, in which fingerprint image is taken as watermark information. This fingerprint image is converted into sparse measurements using compressive sensing (CS) theory and embeds these sparse measurements into wavelet coefficients of standard image to generate a watermarked image. Punam Bedi, Roli Bansal and Priti Sehgal [5] has the key idea to watermark an individual's face image with his fingerprint image and demographic data. PSO is used to select best DCT coefficients in the face image for embedding the watermark. The objective function for PSO is based on the human visual perception capability and ability of the watermarked image to sustain image processing attacks. Eko Hari Rachmawanto, Christy Atika Sari, Yani Parti Astuti and Liya Umaroh [1] proposed a hybrid technique using SLT and DCT. The result of SLT has improvement of DWT with multiresolution decomposition and better time localization. Pooja Chinchmalatpure, Komal Ramteke and Prashant Dahiwale [2] paper represents a hybrid DWT and SVD based biometric watermarking algorithm which is useful for embedding watermark i.e. binary equivalent of minutiae of fingerprint into cover fingerprint image. The proposed algorithm can satisfy both the main objectives of watermarking system i.e. transparence and robustness very well and even in the presence of various image processing attacks useful information can be extracted accurately from fingerprint images. Urvi H. Panchal and Rohit Srivastava [6] descried the DWT watermarking technique in the paper. It is a decomposition technique that decomposes given image into set of basic wavelets. DWT is suitable technique to identify the area in the image that contains secret image. DWT decompose given image into low and high frequency components and finds high frequency components and embeds an image into high frequency components [6]. In DWT based method frequency resolution depends on frequency so when frequency is corrupted it decreases robustness. DWT multiresolution technique decomposes given image into four sub bands –LL, LH, HL, HH. It embeds watermark into LH and HL bands. This method does not provide strong robustness against different types of geometric and image processing [6].

3. WATERMARKING TECHNIQUES

3.1 Discrete Wavelet Transform (DWT)

DWT decompose given image into low and high frequency components and finds high frequency components and embeds an image into high frequency components. In DWT based method frequency resolution depends on frequency so when frequency is corrupted it decreases robustness. DWT multiresolution technique decomposes given image into four sub bands –LL (High scale low frequency components), LH (Vertical low scale high frequency components), HL (Horizontal low scale high frequency components), HH (Diagonal low scale high frequency components). It embeds watermark into LH and HL bands. This method does not provide strong robustness against different types of geometric and image processing attacks.

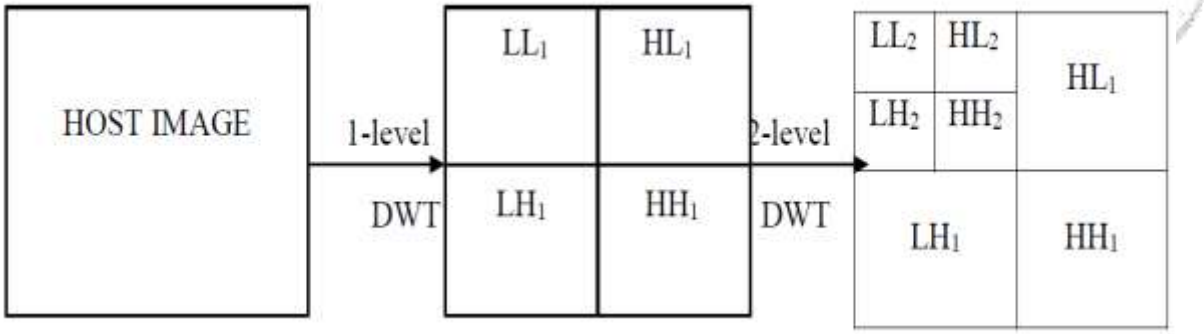

Figure1: DWT Transformation [2]

3.2 Singular Value Decomposition (SVD)

The Singular Value Decomposition (SVD) is a factorization of a real or complex matrix. An A matrix can be decomposed into a product of three different matrices with SVD method. The SVD of an image A with size m · m is given by A — USV^T, where U and V are orthogonal matrices, and S is a diagonal matrix of singular values (SV), i= 1, . . ., m, arranged in decreasing order. The columns of U are the left singular vectors, whereas the columns of V are the right singular vectors of the image A. This process is known as the Singular Value Decomposition (SVD) of A, and can be written as $A = USV^T$.

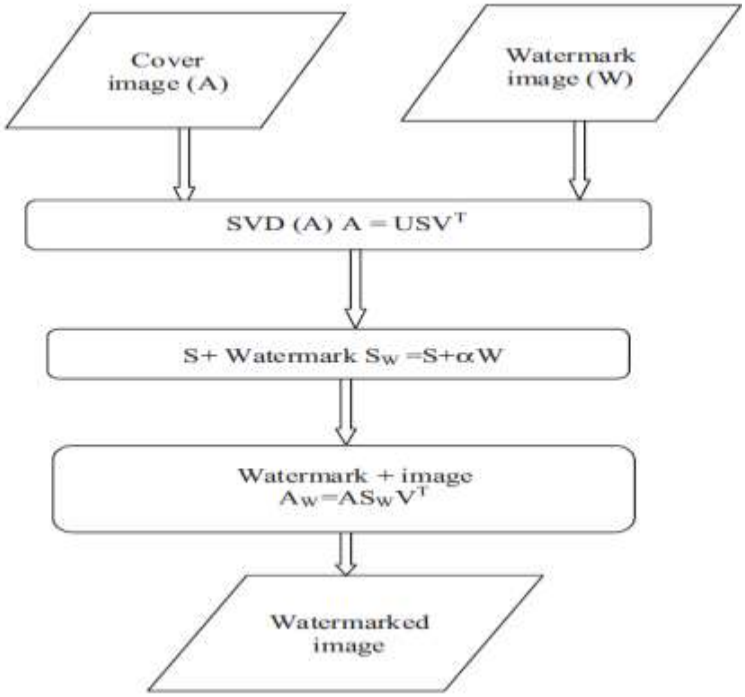

Figure2: SVD Watermarking Technique [3]

3.3 Discrete Cosine Transform (DCT)

In this technique, an image is divided into different frequency band as low (FL), medium (FM) and high (FH). It allows selecting the band to embed data or watermark into the image. Figure 3 represents Discrete Cosine Transform Frequency 8X8 block, where low frequency band FL appears at upper left corner, High frequency band FH lies at lower and right edges, Medium frequency band FM is considered best region for modification, it cannot affect the image quality. Thus, a middle frequency band is the best band to embed watermark.

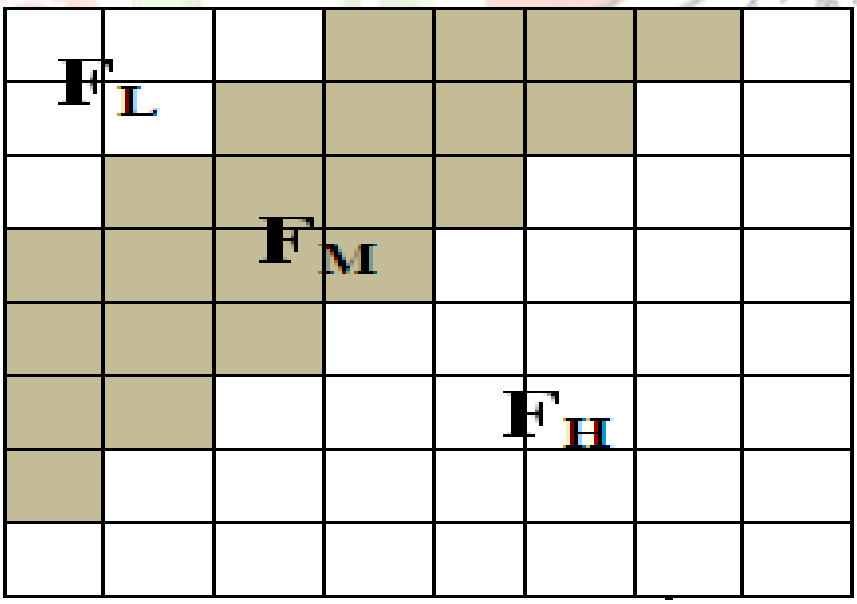

Figure3: DCT Frequency 8x8 block [10]

4. PROPOSED METHODOLOGY

The proposed watermarking system use two forms of biometrics such as fingerprint and a face image i.e. for host image and watermark image respectively. A hybrid technique combining DWT and SVD is utilized to ensure efficient security and robustness to the proposed method. Thus by using two forms of biometrics, a system becomes a multimodal biometric system. The method is divided into two sections: Watermark Embedding Process and Watermark Extraction Process. There is an issue regarding the robustness of the watermarked image to be withstanding various modification attacks. To solve this, issue the proposed technique uses a hybrid concept of two robust watermarking system that is DWT and SVD. Along with robustness the quality parameters are also taken into consideration for comparing the cover image and the watermarked image.

4.1 Watermark Embedding Process

Step1: The host fingerprint image undergoes 2-level decomposition resulting into two-dimensional DWT coefficients. Only LH_2 approximation sub-band is selected for another process.
Step2: Apply SVD matrix transform on LH_2 sub-band of host fingerprint image and by using Face image as the watermark image.
Step3: Applying SVD transform by $A=USV^T$.
Step4: Change the singular values in LH subband with half of the watermark image and then apply SVD to them. i.e. $S+\alpha W = U_w S_w V_w^T$ where α denotes the scaling factor.
Step5: Obtain the set of modified DWT coefficients. i.e. $A=US_WV^T$
Step6: Perform the inverse DWT using the set of modified DWT coefficients and set of non-modified DWT coefficients.
Step7: Thus we obtain the watermarked image in which watermark is embedded.

4.2 Watermark Extraction Process

Step1: Perform a 2-level decomposition DWT transform on watermarked image and obtain low frequency wavelet coefficient LH_2.
Step2: Apply SVD transform to LH_2 sub-band by $A_w=U(S_w^*)V^T$
Step3: Compute $B = U_w(S_w^*) V_w^T$.
Step4: Extract each half of the watermark image from LH subbands. $W^* = (B-S)/\alpha$.
Step5: Add the results from step 4 and obtain the watermark.

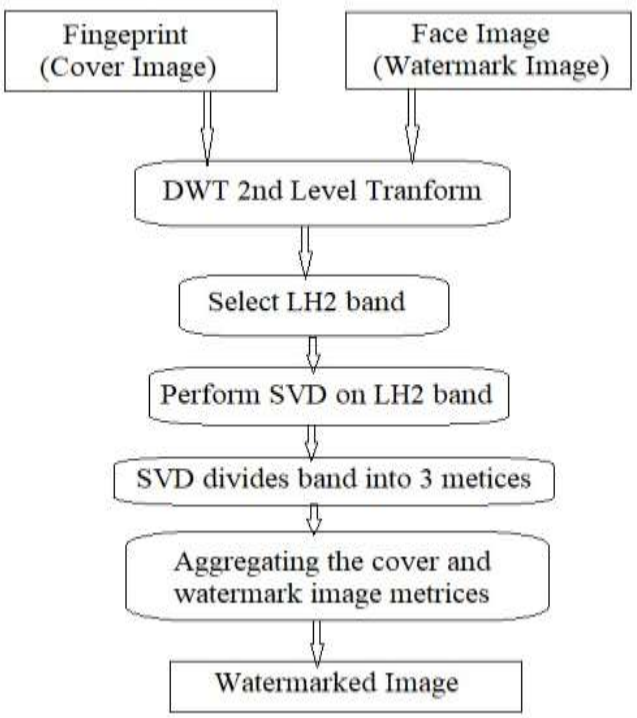

Figure4: Watermark Embedding Process

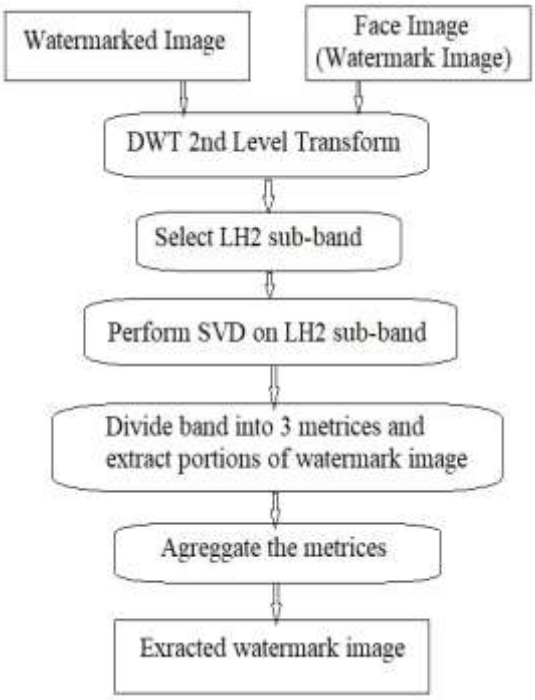

Figure5: Watermark Extraction Process

5. EXPERIMENTAL RESULTS

This experiment uses a fingerprint image and a face image. The host fingerprint image is of size 200x200 pixels and watermark face image is of 256x256 pixels simulated in MATLAB 2016a.

The host fingerprint image and the watermark image both undergoes DWT 2nd level transform. Extracting the LH1 subband from both the images we perform SVD and embedded the watermark on LH subband of host fingerprint image. Thus watermarked image is formed.

Similarly, on extraction of watermark from the watermarked image, we perform DWT and SVD on both the watermark and the host image and the result yields the extracted watermark image.

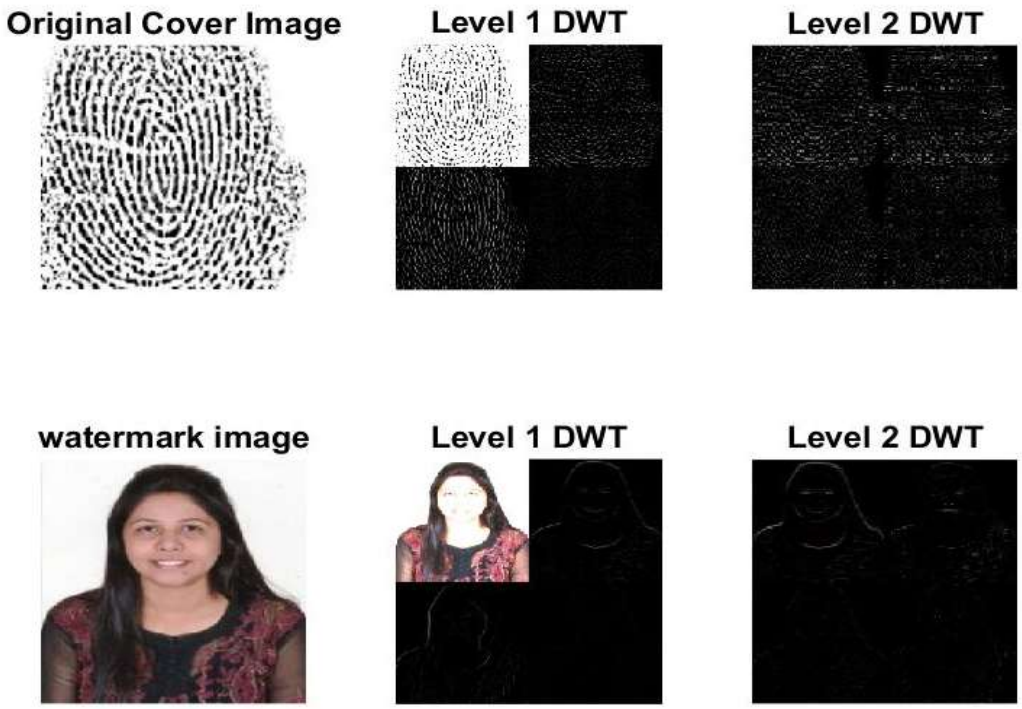

Figure6: Watermark Embedding Process

Figure7: Watermarked Image

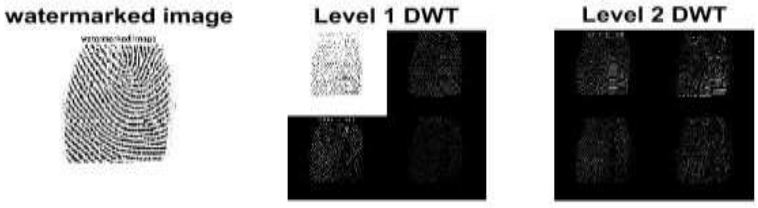

Figure8: Watermark Extraction Process

Figure9: Extracted Watermark Image

MSE and PSNR for the above mentioned experimented is calculated and the result is as below for one image.
MSE (Mean Square Error) = 43.91
PSNR (Peak Signal to Noise Ratio) = 31.7387873 dB

The watermarked values of different watermarking techniques are analyzed with different error metrics such as MSE, PSNR, CC, SSIM etc. The values are referenced with the same cover image and watermark image for all the different techniques so as to make the comparison effective. The face images used for watermark purpose and the fingerprint images used for the host cover image purpose are taken from the standard dataset that is mentioned before.

Error Metrics	DWT	DCT	DWT-SVD on LL subband	Proposed DWT-SVD on LH subband
MSE	87.42	61.47	43.15	**27.46**
PSNR	28.748 dB	24.116 dB	31.467 dB	**33.777 dB**
CC	0.9918	0.9887	0.9927	**0.9934**
SSIM	0.9625	0.9613	**0.9633**	0.9631

Table2: Performance Analysis of Proposed Model

6. CONCLUSION

The proposed watermarking system uses multimodal biometrics and is a hybrid concept that uses a transform domain (DWT) and a spatial domain (SVD) methods. The main motive behind this proposed technique is to provide security and robustness to the fingerprint images. Watermarking techniques are applied to ensure copyright protections, for owner identification, content authentication etc. Some of the real world applications are in the areas of laws, defense, journalism, medical science and others such as smart cards, passports, visa, e-commerce activities etc. After analyzing the performance of the different watermarking techniques we conclude that our proposed watermarking system yields better results than other watermarking techniques. Further along with this proposed method we can also apply arnold transform for better results.

REFERENCES

[1] Eko Hari Rachmawanto, Christy Atika Sari, Yani Parti Astuti, Liya Umaroh "A Robust Image Watermarking Using Hybrid DCT and SLT." 2016 International Seminar on Application for Technology of Information and Communication pp 312- 316.

[2] Pooja Chinchmalatpure, Komal Ramteke and Prashant Dahiwale. "Fingerprint Authentication by hybrid DWT and SVD based Watermarking" 2015 IEEE Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference pp 1-4.

[3] S. Anu H. Nair, P. Aruna "Comparison of DCT, SVD and BFOA based multimodal biometric watermarking systems" 2015 Alexandria Engineering Journal, Volume 54, Issue 4, December 2015, pp 1161-1174.

[4] Rohit Thanki, Komal Borisagar "Sparse Watermarking Technique for Improving Security of Biometric System" Procedia Computer Science, Volume 70, 2015, pp 251-258.

[5] Punam Bedi, Roli Bansal, Priti Sehgal "Multimodal Biometric Authentication using PSO based Watermarking" Procedia Technology, Volume 4, 2012, pp 612-618.

[6] Urvi H. Panchal and Rohit Srivastava "A Comprehensive Survey on Digital Image Watermarking Techniques" 2015 Fifth International Conference on Communication Systems and Network Technologies, pp 592-595.

[7] Huang-Nan Huang, Der-Fa Chen, Chiu-Chun Lin, Shuo-Tsung Chenand Wei-Che Hsu "Improving SVD-based image watermarking via block-by-block optimization on singular values" 2015 EURASIP Journal on Image and Video Processing pp 343-352.

[8] Anil Kumar Shaw, Swanirbhar Majumder, Souvik Sarkar, Subir Kumar Sarkar "A novel EMD based watermarking of fingerprint biometric using GEP" International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013 pp 172-183.

[9] AM Kothari, AC Suthar, RS Gajre "Performance Analysis of Digital Image Watermarking Technique–Combined DWT–DCT over individual DWT" International Journal of Advanced Engineering & Applications ISSN: 0975-7783 January 2010 Volume 1 pp 128-132.

[10] Pooja Dabas and Kavita Khanna. "A Study on Spatial and Transform Domain Watermarking Techniques" International Journal of Computer Applications (0975-8887) May 2013 volume 71 pp 38-41.

[11] Sneha Jose, Rajesh Cherian Roy and Shreenesh Shashidharan "Robust Image Watermarking Based on DCT-DWT-SVD Method" International Journal of Computer Applications (0975-8887) November 2012 Volume 58 pp 12-16.