

---

# A Multimodal Biometric System Using Hybrid Watermarking Technique

**Prachi Dholu**

PG Student

L.J. Institute of Engineering & Technology

GTU, Ahmedabad, Gujarat, India

**Dr. A. C. Suthar**

Director

L.J. Institute of Engineering & Technology

GTU, Ahmedabad, Gujarat, India

## ABSTRACT

*With the growing accessibility and usability of internet there is a growing concern over content protection of digital images. 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;

## 1.INTRODUCTION

Now-a-days 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. The SVD of an image  $A$  with size  $m \cdot m$  is given by  $A = USV^T$ , where  $U$  and  $V$  are orthogonal matrices, and  $S$  is a diagonal matrix of singular values (SV),  $i = 1, \dots, m$ , 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  $A = USV^T$ .

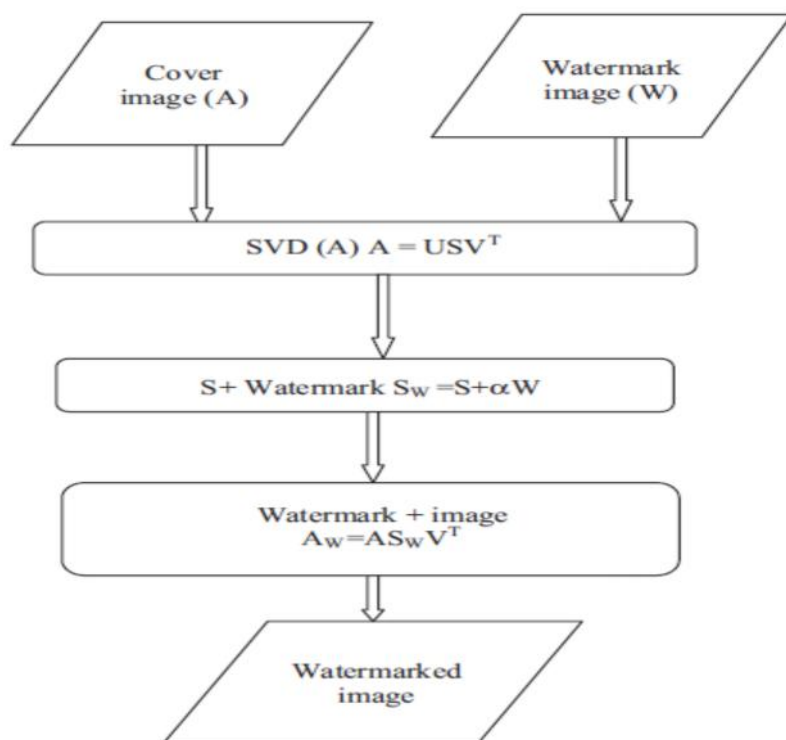


Figure1: SVD Watermarking Technique<sup>[3]</sup>

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 Dahiwalé [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. transparency 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] described 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 subbands –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. 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.

#### 3.1 Watermark Embedding Process

Step1: The host fingerprint image undergoes 2-level decomposition resulting into two-dimensional DWT coefficients. Only  $LL_2$  approximation sub-band is selected for another process.

Step2: Apply SVD matrix transform on  $LL_2$  sub-band of host fingerprint image and by using Face image as the watermark image.

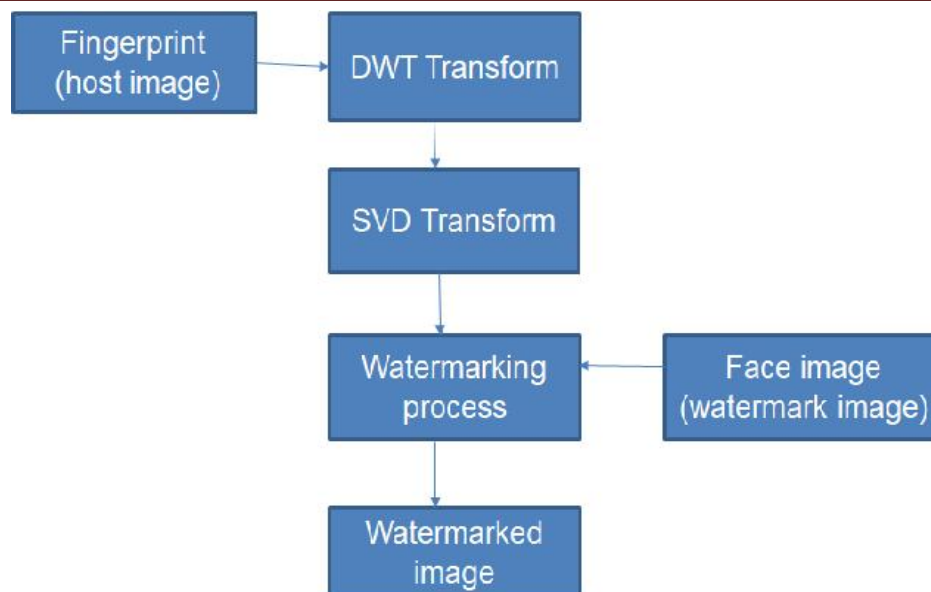
Step3: Thus we obtain the watermarked image in which watermark is embedded.

#### 3.2 Watermark Extraction Process

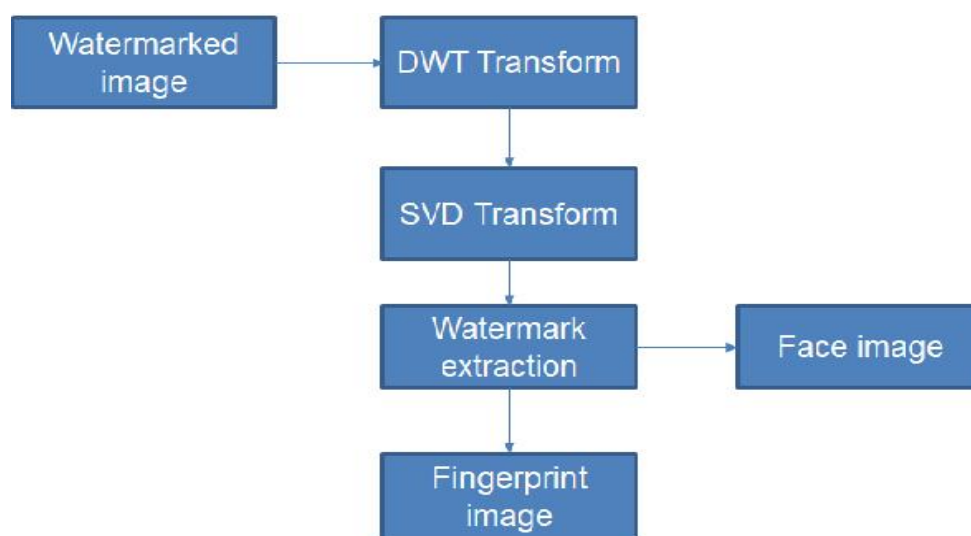
Step1: Perform a 2-level decomposition DWT transform on watermarked image and obtain low frequency wavelet coefficient  $LL_2$ .

Step2: Apply SVD transform to  $LL_2$  sub-band.

Step3: Using values obtained from step2 we reconstruct the watermark image and the host fingerprint image.



**Figure2: Watermark Embedding Process**



**Figure3: Watermark Extraction Process**

#### 4. CONCLUDING REMARKS

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, defence, journalism, medical science and others such as smart cards, passports, visa, e-commerce activities etc.

## 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 Dahiwal. “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 Chen and 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.