Available online at www.sciencedirect.com
ScienceDirect
Image and Vision Computing 27 (2009) 293–304
www.elsevier.com/locate/imavis

Feature based RDWT watermarking for multimodal biometric system

Mayank Vatsa, Richa Singh, Afzel Noore *

Lane Department of Computer Science and Electrical Engineering, West Virginia University, USA

Received 19 January 2006; received in revised form 12 February 2007; accepted 14 May 2007

Abstract

This paper presents a 3-level RDWT biometric watermarking algorithm to embed the voice biometric MFC coefficients in a color face image of the same individual for increased robustness, security and accuracy. Phase congruency model is used to compute the embedding locations which preserves the facial features from being watermarked and ensures that the face recognition accuracy is not compromised. The proposed watermarking algorithm uses adaptive user-specific watermarking parameters for improved performance. Using face, voice and multimodal recognition algorithms, and statistical evaluation, we show that the proposed RDWT watermarking algorithm is robust to different frequency and geometric attacks, and provides the multimodal biometric verification accuracy of 94%.

Keywords: Biometrics; Watermarking; Redundant Discrete Wavelet Transform; Face recognition; Voice recognition; Multimodal biometrics

1. Introduction

Biometric authentication systems have inherent advantage over traditional personal identification techniques [21]. However, there are many critical issues in designing a practical biometric system. These issues are broadly characterized by accuracy, computation speed, cost, security, scalability and real time performance. The security of biometric data is of paramount importance and must be protected from external attacks and tampering [20]. Ratha et al. [25] characterized common attacks in biometric systems as coercive attack, impersonation attack, replay attack, and attacks on feature extractor, template database, matcher, and matching results. Attacks can alter the contents of biometric images or templates and can degrade the performance of a biometric system. It is therefore required to protect the biometric templates of individuals at all times.

Researchers have proposed algorithms to handle challenges confronted by security of biometric systems. Encryption is one way of addressing this issue and has been discussed in [10,30,33]. Another way of securing biometric images and templates is by watermarking. Recently, researchers have proposed algorithms based on image watermarking techniques to protect biometric data [13,19,20,25,34]. In biometric watermarking, a certain amount of information referred to as watermark, is embedded into the original cover image using a secret key, such that the contents of the cover image are not altered. Some of these methods perform watermarking in the spatial domain [13,19,20] while other methods embed the biometric watermark in the frequency domain [25,34]. In existing biometric watermarking algorithms the cover image is either gray scale face image or fingerprint image, and the watermark data is fingerprint minutiae information [20] or face information [19] or iris codes [34].

In this paper we propose a novel biometric watermarking algorithm to securely and robustly embed the biometric voice template into the color face image of the same individual. Color face image is used as the host image and Mel Frequency Cepstral Coefficients (MFCC) extracted from the voice data are used as watermark. Face and voice are chosen for watermarking because of the widespread application of face and speaker verification. There are several applications

* Corresponding author. Tel.: +1 304 293 4821x2547; fax: +1 304 293 8602.
E-mail addresses: mayankv@csee.wvu.edu (M. Vatsa), richas@csee.wvu.edu (R. Singh), noore@csee.wvu.edu (A. Noore).

0262-8856/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.imavis.2007.05.003

where either face or voice or both are used to authenticate an individual [14]. The proposed watermarking algorithm first computes the embedding capacity and location in the face image using edge and corner phase congruency method [22]. Embedding and extraction of voice data is based on Redundant Discrete Wavelet Transformation [9]. The performance of the proposed watermarking algorithm is validated using face, voice and multimodal verification algorithms. We observe that the proposed watermark embedding and extraction algorithm does not affect the quality of the original face image or the recognition performance. In addition, the proposed algorithm is robust and resilient to common attacks. We perform statistical evaluations to further validate that the proposed watermarking algorithm does not affect the verification performance of biometric watermark and cover image.

Section 2 in the paper presents the proposed biometric watermarking algorithm. Section 3 describes the database and recognition algorithms used for verifying the integrity of the biometric data. Section 4 describes the computation of user-specific parameters for the proposed watermarking algorithm and Section 5 discusses the experimental results in detail.

2. Proposed biometric watermarking algorithm

Usually, image watermarking is performed using Discrete Wavelet Transform (DWT) because DWT preserves frequency information in stable form and allows good localization both in time and spatial frequency domain [9,26,31]. However, one of the major drawbacks of DWT is that the transformation does not provide shift invariance because of the downsampling of its bands. This causes a major change in the wavelet coefficients of the image even for minor shifts in the input image. In watermarking, we need to know the exact locations of where the watermark information is embedded. The shift variance of DWT causes inaccurate extraction of the watermark data and the cover image. To address the issues of DWT based watermarking, researchers have proposed the use of Redundant Discrete Wavelet Transform (RDWT) [7,11,12,15,16].

Fig. 1 shows the RDWT decomposition of a face image in four subbands such that the size of each subband is equal to the original image. The redundant space in RDWT provides additional locations for embedding and the watermarking algorithms can be designed such that

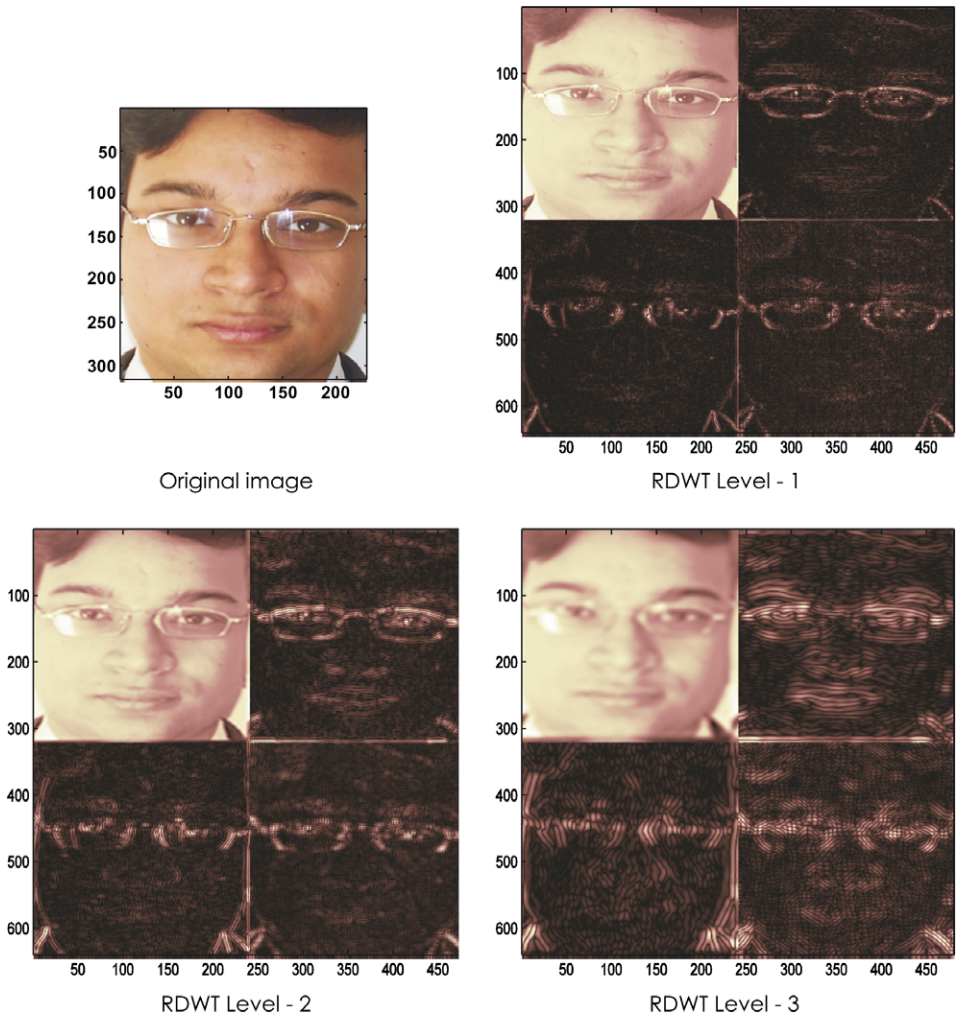

Fig. 1. RDWT decomposition of a face image. Note that size of all the subbands at every level is same as the original image.