Neurocomputing 191 (2016) 69–81

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

Joint Encryption and Compression scheme for a multimodal telebiometric system

Ameya K. Naik*, Raghunath S. Holambe

S.G.G.S. Institute of Engineering and Technology, Vishnupuri, Nanded, Maharashtra 431606, India

ARTICLE INFO

Article history:
Received 3 May 2015
Received in revised form
3 November 2015
Accepted 10 January 2016
Communicated by Dr. Deng Cheng
Available online 4 February 2016

Keywords:
JPEG2000
Multimodal biometric system
SPIHT
Telebiometric system
Watermarking

ABSTRACT

In this paper we present a novel Joint Encryption and Compression (JEC) technique for transmission of biometric data over a wireless channel. The method offers advantages such as reduced data processing, security and enhanced recognition accuracy. The security of the biometric data is ensured by means of watermarking followed by random bit shuffling. The watermarking process involves embedding one's fingerprint information in his/her compressed face image. In order to compress face images face images wavelet based encoders such as SPIHT (Set Partitioning Hierarchical Trees) and JPEG2000 are used. The advantage of the proposed method is that the overall data rate can be minimized while simultaneously maintaining good quality reconstruction. The JEC (Joint Encryption and Compression) scheme is tested for its suitability in a wireless communication system. It can be seen that with the help of appropriate channel coding, high values of PSNR (Peak Signal to Noise Ratio) can be obtained. Consequently the recovered biometric data offers recognition rates that are found to be acceptable for a telebiometric system. Additionally an algorithm is suggested for fusion of individual biometric scores in order to improve the overall recognition performance. Simulation results depict that a significant advantage in verification rates can be achieved by this method.

1. Introduction

Biometric based authentication systems [1–3] are becoming increasingly popular as they offer enhanced security and user convenience as compared to traditional token-based (I. D. Card) and knowledge based (password) systems. This popularity is mainly due to the ability of the biometric technology to differentiate between a genuine person and a fraudulent imposter. With the increasing usage of biometric systems, the problem of storing and handling the sensor data has become critical. Also in most of the cases the sensor data has to be transferred via a communication channel with low bandwidth and high latency. Therefore minimization of the amount of data is highly desirable which is achieved by compressing the data before transmission.

During the last decade several algorithms and standards [4–7] for compressing biometric image data have been evolved. The ISO/IEC 19794 standard specifies that fingerprint and face image data be stored in a lossy manner using JPEG (Joint Photographic Experts Group), WSQ (Wavelet Scalar Quantization) and JPEG2000 format. JPEG2000 standard adopts wavelet based image coder since it outperforms traditional coders based on discrete cosine transform. Recently wavelets have also been accepted as a standardized tool for image analysis and feature extraction. Several biometric identification systems use wavelet domain features [7–9] for recognition. These systems require lesser preprocessing and are found to give acceptable performances as compared to traditional methods. However with the wide spread utilization of biometric systems, establishing the authenticity of biometric data itself has emerged as an important issue. Recently data hiding and watermarking techniques [10,11] have also been proposed as means of increasing the security of fingerprint images. One of such methods [12] is to embed facial information into host fingerprint image or vice versa. These schemes have the advantage that, in addition to fingerprint matching, the recovered face image can be used to establish authenticity of the user. For a digital watermarking method to be effective, it is essential that an embedded watermark should be robust against compression. The problem associated with such schemes is that the watermarking process should not increase the bit rate of the compressed data to a large extent. Moreover, it is desirable that the watermarking algorithm be easily integrated with the existing compression framework (SPIHT, JPEG2000, etc.) so that good quality reconstruction is assured. Consequently recent literature focuses on joint watermarking and compression (JWC) techniques [13–15] for data security, storage and transmission.

* Corresponding author. Tel.: +91 22 28625938.
E-mail addresses: ameyaknaik@yahoo.com (A.K. Naik), rsholambe@sggs.ac.in (R.S. Holambe).

http://dx.doi.org/10.1016/j.neucom.2016.01.006
0925-2312/

In this article we propose a Joint Encryption and Compression (JEC) technique for telebiometric systems. Encryption is achieved by means of compressed domain watermarking and random bit shuffling. The compressed domain refers to images compressed using SPIHT (Set Partitioning Hierarchical Trees) or the JPEG2000 compression standard. These state-of-the art encoders are adopted for the following reasons. Firstly, in addition to their proven coding performance, they are amongst the fastest coding algorithms making them more suitable to be combined with a watermarking system. Secondly both these methods exhibit the property of progressive image transmission [16] leading to easier manipulation of their respective bit streams. In addition the overall bit rate can be controlled (subject to conditions on the requirements of distortion and robustness) which is extremely important in applications involving image transmission. The performance of the proposed JEC scheme is tested over a wireless communication system [17]. It can be seen that with the help of suitable channel coding good quality reconstruction (high peak signal to noise ratio) can be achieved. Consequently the recovered biometric data offers comparable recognition rates in a biometric identification system. Using the proposed watermarking method we intend to transmit data related to two biometric modalities viz. face and fingerprint. At the decoder the fusion of two individual modalities [18, 19] can help to improve the overall recognition performance leading to an effective multimodal biometric system.

The rest of the paper is organized as follows. Section 2 gives a brief description about the existing data hiding methods and their salient features. Section 3 discusses a Joint Encryption and Compression (JEC) technique for a multimodal telebiometric system. The performance of the system under various channel conditions is analyzed in Section 4. This Section also presents the comparison of the proposed method with the state-of-the-art methods followed by the conclusions.

2. Related work

In recent years, considerable work has been done on hiding features or images of one biometric modality into another of the same subject. Existing literature highlights the use of watermarking techniques [10,11,20] for concealing biometric data. In such methods the cover image is usually a gray scale face image or fingerprint image, and the watermark data is fingerprint minutiae information, face information or iris codes. In general watermarking techniques can be classified as transformation domain techniques and spatial domain techniques. Gunsel et al. [20] proposed spatial domain methods in order to embed watermark data into fingerprint images, without corrupting the existing features. These methods do not require original fingerprint image while decoding. In addition the proposed methods provide high decoding accuracy for fingerprint images.

Spatial domain techniques are comparatively simple, but are not resistant to attacks such as compression attack. So when image compression is performed the watermarked features are likely to be disturbed thus limiting the usage of the hidden data. As a result transform-domain watermarking techniques are preferred over their spatial domain counterparts [21,22]. Additionally in most applications, watermarked images are either stored and/or transmitted over bandlimited channels making it necessary to work in the compressed domain. Hence instead of treating watermarking and compression processes separately it is beneficial to focus on joint watermarking and compression schemes (JWC). In JWC, watermarking can be done either in conjunction with a compression algorithm or a compression standard. Ratha et al. [23] introduced a data hiding algorithm for wavelet compressed fingerprint images. The data hiding algorithm is robust and can be easily implemented in hardware. Similar attempts were made by researchers using other compression algorithms. Using Set Partitioning In Hierarchical Trees (SPIHT), Yang et al. [24,25] suggested a semi-blind watermarking scheme which involves replacing bits corresponding to refined coefficients, with the watermark bits. However, the disadvantage of the scheme is that the detection procedure requires the locations of embedded bits for watermark retrieval. Similarly in [25], based on a correlation approach, a watermarking technique was proposed for zerotree coded images. In yet another method Khelefi [13] used SPIHT to design a robust JWC system. The proposed method was found to be robust to various attacks encountered in JWC domain.

Watermarking associated with compression standards (JPEG, MPEG and JPEG2000) generally deal with manipulating the quantized transform coefficients for data hiding. Such an attempt was made by Su et al. [26] by incorporating a spread-spectrum watermarking scheme into the JPEG2000 compression format. A binary watermark sequence was progressively embedded into the bit planes of quantized coefficients. For identification the correlation between signature and the corresponding watermarked coefficients was computed. Another approach to compressed domain watermarking was presented by Mobasseri and Berger [27]. The technique was presented mainly for JPEG and MPEG standards. The fragile watermark was embedded by replacing some variable length codewords with unused codewords in the code space. These techniques are known to work well in case only data authentication is required. However enhanced security can be achieved by using watermarking in combination with encryption particularly when the signal is of composite nature. Deng et al. [28] proposed an efficient buyer-seller watermarking protocol based on composite signal representation given in [29]. However, the applicability of the embedding scheme was not guaranteed particularly when the watermark embedded was accessible only as encrypted content. Moreover, the ciphertext expansion associated with such schemes was quite significant which was undesirable in certain applications. Prins et al. [30] proposed a robust quantization index modulation (QIM) based watermarking technique, which embeds the watermark in the encrypted domain. In this technique the addition or subtraction of a watermark bit to a sample is based on the value of quantized plaintext sample. The drawback of this technique is that the embedder has direct access to the plain text values. A similar technique based on content-dependent watermarking was proposed by Li et al. [31]. This technique embeds the watermark in an encrypted format, but the host signal is still in the plain text format. Also if the content is present in encrypted format the algorithm may introduce severe distortion in the host signal. In [32] Sun et al. proposed a semi fragile authentication system for JPEG2000 images. However, this scheme is not fully compressed and encrypted domain watermarking compatible as it derives the content based features for watermarking from the plain text. In [33] a more robust watermarking technique for JPEG2000 images is proposed in which predictable watermarking of compressed-encrypted byte stream can be performed by exploiting the homomorphic property. Although this method offers some advantage in computational complexity, the proposed technique faces the following drawbacks. A perfect identification of the watermark position is required as a small change in the compressed data may lead to a considerable deterioration in the quality of decoded image. Secondly it is difficult to maintain both compression efficiency and payload capacity at the same time. Hence such a method may not be viable in applications involving image transmission.

In this paper a watermarking technique for compressed biometric images is proposed. The advantage of our method is that the overall bit rate can be easily controlled as per requirement. The proposed scheme is robust to transmission errors [34–37] and