ELSEVIER
SIGNAL PROCESSING
IMAGE
COMMUNICATION
Special issue on Interactive representation of still and dynamic scenes
Guest Editors: G.M. Cortelazzo, D.S.Taubman
Theory, Techniques & Applications
A publication of the European Association for Signal Processing (EURASIP)
Available online at ScienceDirect www.sciencedirect.com
EURASIP

www.elsevier.com/locate/image

A combined watermarking approach for securing biometric data

Lamia Rzouga Haddada, Bernadette Dorizzi, Najoua Essoukri Ben Amara

PII: S0923-5965(17)30043-7
DOI: http://dx.doi.org/10.1016/j.image.2017.03.008
Reference: IMAGE15192

To appear in: *Signal Processing : Image Communication*

Received date: 19 March 2016
Revised date: 15 March 2017
Accepted date: 15 March 2017

Cite this article as: Lamia Rzouga Haddada, Bernadette Dorizzi and Najou Essoukri Ben Amara, A combined watermarking approach for securing biometri data, *Signal Processing : Image Communicatio* http://dx.doi.org/10.1016/j.image.2017.03.008

A combined watermarking approach for securing biometric data

Lamia Rzouga Haddada[a], Bernadette Dorizzi[b], Najoua Essoukri Ben Amara[a]

[a]*SAGE, National Engineering School of Sousse, BP 264 Sousse Erriadh 4023, Tunisia*
[b]*SAMOVAR, Télécom SudParis, CNRS, Université Paris-Saclay, 9 rue Charles Fourier - 91011 Evry Cedex, France*
[*]Corresponding author. Tel.: +0-000-000-0000; fax: +0-000-000-0000. najoua.benamara@eniso.rnu.tn

ABSTRACT
In this paper, we propose a new watermarking reinforcement approach that ensures a suitable compromise between the security level of a person's biometric data and the computational complexity of the proposed scheme while maintaining a reduced storage space and a good visual quality of the watermarked host image. We validate the suggested approach on two biometric modalities, fingerprint and face, which are among the most frequently deployed and mature ones in biometric watermarking systems. The improved level of safety is ensured by a combined watermarking scheme. In fact, the same watermarking algorithm is applied twice in succession. First, the face of an individual is watermarked by the local characteristics, minutia, of his/her fingerprint. Second, the previously watermarked face image is inserted into the original image of the fingerprint as supplementary identity information. Beside securing the biometric data, the exploration of the watermarked image has shown interesting performances in individuals' verification. The results of various tests performed on the Biosecure multimodal database have demonstrated that the proposed method is robust to several signal processing attacks.

Keywords: combined watermarking, biometric data protection, robustness, computational complexity, invisibility, verification

1. Introduction

The biometric data are often transmitted and / or stored for identity verification / recognition purposes [1]. This is the case, for example, of the online payment by biometric control [2].Therefore, it is becoming increasingly important to protect biometric data from accidental or intentional attacks that occur often during data transmission and storage operations [1]. Digital watermarking appears as an emerging tool for securing the original multimedia data [2]. Watermarking is a branch of data hiding that inserts a watermark inside a carrier signal (e;g. audio file, image file, video file or text file) for several aims such as content authentication, intellectual property and copyright protection. A watermark is a signature that can reveal the multimedia object ownership [1]. The watermark can be generated using a confidence key; it must be invisibly inserted into the cover image such that it resists to a variety of malicious operations or acceptable manipulations. Since traditional watermarks like binary logo, text or image do not have a user-based originality and uniqueness, they may cause some corruption, tamper and emulation. Thus, biometric-based watermarks become a solution to such problems, as they provide a high level of identification and authentication [3].

In biometric watermarking, several methods have been suggested in the literature. Few of them adopt the idea of inserting biometric data inside standard test image. Therefore, the extracted watermark can be utilized basically for intellectual property protection (protecting the creator rights, the legitimate owner right, copyright protection and moral rights protection) [4]. However, most methods, with which this paper is concerned, adopt the idea of inserting one biometric image in another one so as to secure the originality of biometric templates transmitted and stored in databases [2, 5].

Yet, the biometric watermarking is often subject to frequent and numerous attacks (compression, noise filters, geometrical and temporal distortions...) which greatly threaten the security of the watermarked data and present a challenge in the watermarking community [2].The generally recommended solution is to combine the biometric watermarking with other security techniques or to insert two or more watermarks in the host image [6, 7]. This is referred to as watermarking reinforcement [2].

The reinforcement by combining security techniques may be carried out by watermarking / cryptography [8-10], by watermarking/ steganography [11] or by watermarking / steganography / cryptography [12, 13]. Despite the fact that the watermarking security tool has no conflict with cryptography and steganography, some common limitations of these reinforcement approaches are incremented computational complexity, increased memory requirements, and watermarked image's visual quality degradation [14-17].

In this paper, to overcome the drawbacks of the existing methods, we put forward a new watermarking reinforcement approach consisting in a watermarking / watermarking combination that could improve the performance of watermarking robustness. We demonstrate that the proposed method can also be explored on improving verification performances while offering a good compromise between security, visual quality, storage space, and complexity in biometric data transmission.

The proposed authentication scheme can be used for a security purpose such biometrics stored in centralized locations as templates in databases or applied to a smart card, a computer login control, a credit card, and secure electronic banking [3]. In addition the extracted watermark during the decoding phase can be used to identify the owner.

We validate the suggested watermarking approach on the fingerprint and the face which are among the most widely used and relatively mature biometrics [18, 19]. We have exploited the watermarking technique not only to hide and secure biometric modalities, but also as a fusion technique to insert a biometric modality into another one. In fact, the proposed watermarking scheme aims to securely and robustly insert the face and minutiae fused together by watermarking into the fingerprint image of the same individual in two steps. In the first step, the face image is utilized as the host image. The minutiae data, which are spatial coordinates and orientations previously extracted from the fingerprint, are used as watermark. The face and minutiae are fused at the signal level using a key which reduces their storage size. Embedding and extracting minutiae data are based on wavelet packet decomposition algorithm (WPD). For the second step, the previously watermarked face by minutiae is embedded in the original image of the fingerprint, which is the principal host image in our scheme.