J. Vis. Commun. Image R. 38 (2016) 1–10

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

Digital images authentication scheme based on bimodal biometric watermarking in an independent domain ☆

Wioletta Wójtowicz *, Marek R. Ogiela

AGH University of Science and Technology, Cryptography and Cognitive Informatics Research Group, Al. Mickiewicza 30, Krakow 30-059, Poland

ARTICLE INFO

Article history:
Received 4 October 2015
Accepted 10 February 2016
Available online 17 February 2016

Keywords:
Image watermarking
Image authentication
Biometric watermarking
Independent Component Analysis (ICA)
Biometric verification
Multibiometrics
Fingerprint recognition
Iris recognition

ABSTRACT

With the growing accessibility and usability of internet there is a growing concern over content protection of digital images. Recently, 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. This paper presents a new scheme for protecting and authenticating invisibly watermarked digital images. It applies Independent Component Analysis to the cover image and enables the insertion of two independent watermarks based on fingerprint and iris biometrics. In this approach biometric techniques are used for watermarks generation and for owners authentication. The main advantage of proposed algorithm is construction of ICA based watermarking domain to enable insertion of two independent watermarks, that improve authentication accuracy and makes scheme more robust.

1. Introduction

Nowadays unrestricted access to computers and computer networks makes it possible to share multimedia data such as digital images among many people, not only authorized users. To ensure that images are transmitted from the correct sources to the intended recipients (authentication) many systems, including cryptography, encryption, steganography and watermarking techniques, have been elaborated, of which some examples can be found in [1–4]. Recently, these security technologies are increasingly combined with biometric techniques mostly due to its ability to differentiate between authorized and unauthorized users (e.g. [5,6]). As a result, biometric-based security schemes, using unique, measurable physiological and behavioral characteristics of a users, represent a robust alternative to traditional copyright protection and authentication schemes. Many examples of such systems combining biometric features with encryption [7], cryptography [8], steganography and watermarking [9,10] have been provided so far. As a continuation of these studies, this paper is concerned with overcoming the major limitation of traditional watermarking schemes, that is lack of watermark uniqueness, introducing biometric-based watermarks.

In general, watermarking technology, that is subject to the same security requirements as cryptography ([2]), solves important security problems including copyright protection and authentication (e.g. [1,11]). In such schemes watermark data are hidden in the image, so that they could identify the owner during potential ownership controversies. However, as traditional watermarks such as logo, text or images, do not have a user based uniqueness, they may lead to some imitation, tamper and repudiation. Such watermarks could be hacked by the hackers (e.g. at brute-force attack) and use by them to claim ownership or the host image could be fraudulently watermarked by impersonators. Therefore, biometric-based watermarks, that are generated using biometric traits of the image owners, become solution to these issues, as they provide the requisite level of authentication. Employment of user-specific watermarks is critical for determining if certain individual is authorized to access the content or whether current user is a legitimate owner of the work. In case of any ownership dispute on the image, the watermark is extracted from the image and compared against different samples of the person claiming ownership. If they match, the claiming person is the actual owner of the image.

Several methods of using watermarking techniques in conjunction with biometrics have been proposed in the literature. Most of them adopt the idea of hiding one biometrics in another biometric image to protect the originality of biometric templates stored in

☆ This paper has been recommended for acceptance by M.T. Sun.

* Corresponding author.

E-mail addresses: wioletta.wojtowicz26@gmail.com (W. Wójtowicz), mogiela@agh.edu.pl (M.R. Ogiela).

http://dx.doi.org/10.1016/j.jvcir.2016.02.006

databases, e.g. [12,13]. Although there are also methods, that this paper is concerned with, where biometric data are inserted into neutral images, sometimes even unrelated to this data, so that after extraction could be used for copyright protection purposes. For example [14] presents method of embedding fingerprint data in a watermarking domain, that is combination of DWT and SVD transformations. Authors proposed to use minutiae coordinates matrix after SVD transformation as a watermark and after extraction compare it with data provided by user claimed ownership. Another algorithm in which binary iris code is inserted in the neutral image is presented in [15]. In this scheme decision about user acceptance depends on similarity measure between extracted and provided by users biometric samples, that is computed as ratio of correctly detected watermark bits. In this field there are also methods, that use more than one biometric watermark, mostly to take advantages of multimodality, e.g. [16–18]. In [16] authors present method of embedding face, speech and signature data at different stages of watermarking procedure, that combines different transformations, e.g. DWT, DCT and Linear Predictive Coding (LPC). After extraction biometric traits are separately compared with their original versions using correlation and similarity factors, but there is no authentication procedure that fuses these biometrics. Next two methods presented in [17,18] deal with embedding fingerprint and iris features as the binary watermarks in DCT based watermarking domain. In [17] features of both traits are used to construct one watermark (fusion at feature level), that after extraction is again divided into two biometrics. Then both traits are compared with their original versions separately, using normalized correlation for iris and minutiae matching procedure for fingerprints. Finally, in [18], where two binary watermarks are inserted modifying the amplitude of some selected coefficients of the cover image in DCT domain, user authentication procedure is performed after fusion of both biometric traits at the decision level. Proposed algorithm is tested for real biometric databases and considering attacks influence to demonstrate advantages of multimodal authentication procedure.

This paper proposes a new bimodal biometric watermarking algorithm based on Independent Component Analysis (ICA) of the cover image, that enables the authentication of digital images owners. In our algorithm two biometric watermarks based on fingerprint image and binary iris template are embedded invisibly in a neutral cover image. After watermarks extraction, instead original watermarks, just another samples of biometric traits are required to perform owners authentication. Our scheme involves ICA decomposition of the cover image into four basic components and choosing two of them, with the highest energy ones, for embedding. The first component (approximation of the cover image) is mixed with scrambled fingerprint image, whereas in the second component (details of the cover image) binary iris template and its mask are embedded by pixels quantization. The main reason for applying ICA in this algorithm is its ability to decompose any image into statistically independent source images. In that the cover data is partitioned into disjoint components and each watermark is embedded into them independently. Incorporating idea of using two independent biometrics make system robust to variations of biometric data, processing connected with watermarking and influence of possible attacks.

The novelty of the proposed method is introducing Independent Component Analysis (ICA) to biometric watermarking field, as to the authors knowledge, it is the first biometric watermarking algorithm, that is based on ICA transform. In our method standard ICA approach, that involves embedding only one image watermark, is employed and extended, so that insertion of two biometric watermarks would be possible. Moreover, embedding procedure is adjusted to the watermarks as selection of ICA components for embedding depends on representation of biometric watermarks. Finally, we propose owners authentication procedure based on biometric data fusion at matching score level, that improves user authentication accuracy even when watermarked images undergo some attacks. The main goal of our simulation study is to elaborate how user verification accuracy changes after watermarking procedure and how significant improvement of these results could be achieved when information provided by both biometrics is fused.

The paper is structured as follows. Section 2 introduces watermarking in ICA domain bases and some issues connected with biometric verification methods that will be elaborated in our scheme. Proposed methodology is described in Section 3. The experimental study, algorithms settings and results discussion are presented in Section 4. Section 5 concludes on the study carried out.

2. Preliminary

In this section, we give an introduction to the properties of standard watermarking algorithm in ICA domain, i.e. MRICA method, that will be extended to construct watermarking domain in our scheme. Then some information about biometric verification methods, especially based on fingerprint and iris images, that will be used for watermarks construction, are provided. Finally, some issues connected with biometric verification errors and multimodal biometric systems are discussed.

2.1. ICA for watermarking

Independent Component Analysis (ICA) is a statistical and computational technique in which the goal is to find a linear representation of nongaussian data so that the components are statistically independent [19,20]. ICA is typically known as a method for Blind Source Separation (BSS), because it tries to find a transform of signals mixture such that the recovered signals are as independent as possible. With its blind separation capability, several authors have tried to apply ICA also to watermarking, often emphasizing the similarity between crucial stages of these procedures [21,22]. In this context the embedding stage of watermarking can be viewed as a mixing process of ICA algorithm, that mixes original image and some watermark to produce the watermarked image. Likewise, the extraction stage of watermarking can be viewed as a demixing process of ICA, where the original image and the watermark are the statistically independent sources that should be separated from the watermarked image.

An example of application ICA in watermarking is Multi Resolution by Independent Component Analysis (MRICA) method, that decomposes any image into statistically independent components and uses one of them for watermark insertion [23]. Precisely, the watermarking process starts with dividing the cover image of size $N \times M$ into blocks of size $k \times k$ to obtain k^2 observation images of size $N/k \times M/k$ (the corresponding components of blocks are used for construction of observation images). The value of k is set in advance, depending on how many observation images/what size of these observations are desired. Then some ICA algorithm demixes these observations to obtain k^2 independent images that build ICA bases (one approximation image and $k^2 - 1$ detail images). This process requires reshaping of all observation images to the vectors x_l, for $l = 1, \dots, k^2$, sized $1 \times NM/k^2$, that become rows of matrix X sized $k^2 \times NM/k^2$. The ICA algorithm finds $k^2 \times k^2$ demixing matrix B and $k^2 \times NM/k^2$ matrix Y, such that $Y = BX$. Finally, rows of Y are statistically independent and after resizing to $N/k \times M/k$ are taken as ICA bases (independent components). As it is proven that the component with the highest energy denoted as IC_H (approximation of the original image) is the most robust, the watermark W of the size $N/k \times M/k$ is embedded in it according to the rule