Journal of Network and Computer Applications 33 (2010) 247–257

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

A novel image hiding approach based on correlation analysis for secure multimodal biometrics

Miao Qi [a,b], Yinghua Lu [b,*], Ning Du [a], Yinan Zhang [a], Chengxi Wang [a], Jun Kong [a,c,**]

[a] Computer School, Northeast Normal University, Changchun, China
[b] Faculty of Chemistry, Northeast Normal University, China
[c] Key Laboratory for Applied Statistics of MOE, Northeast Normal University, China

ARTICLE INFO

Article history:
Received 20 May 2009
Received in revised form
17 November 2009
Accepted 7 December 2009

Keywords:
Correlation analysis
Partial least squares
Particle swarm optimization
Middle-significant-bit
Multimodal biometrics

ABSTRACT

This paper proposes a novel multimodal biometric images hiding approach based on correlation analysis, which is used to protect the security and integrity of transmitted multimodal biometric images for network-based identification. Compared with existing methods, the correlation between the biometric images and the cover image is first analyzed by partial least squares (PLS) and particle swarm optimization (PSO), aiming to make use of the abundant information of cover image to represent the biometric images. Representing the biometric images using the corresponding content of cover image results in the generation of the residual images with much less energy. Then, considering the human visual system (HVS) model, the residual images as the secret images are embedded into the cover image using middle-significant-bit (MSB) method. Extensive experimental results demonstrate that the proposed approach not only provides good imperceptibility but also resists some common attacks and assures the effectiveness of network-based multimodal biometrics identification.

1. Introduction

Biometrics is an emerging technology that utilizes distinct physiological or behavioral characteristics to determine or verify the identity of an individual. Due to the outstanding features of uniqueness, reliability and stability, biometrics has been widely applied to secure identification/verification systems and has replaced traditional recognition methods. Although biometrics-based identification methods have many advantages over traditional methods, biometric data themselves cannot provide secrecy and security. Ratha et al. (2001) outlined the potential eight basic sources of attacks to the biometric verification system. For instance, the biometric data being transmitted over the network is vulnerable to potential attacks, which can alter the content of biometric data and degrade the performance of biometric systems. Thus, protecting the security and integrity of the biometric data is a critical issue for ensuring valid biometric identification.

Recently, making use of information hiding techniques, such as watermarking and steganography, to protect the security and integrity of the transmitted biometric data has been becoming an active topic. Ratha et al. (2000) described a blind data hiding method to protect fingerprint images with wavelet-packet scalar quantization standard. Jain et al. (2002) introduced an amplitude modulation-based watermarking method, in which a bit stream of eigenface coefficients was embedded into the selected fingerprint image. Hiding biometric information in a digital image using watermarking technique was described in the literature (Mohamed, 2007). The proposed technique gave a quite simple solution for inserting a secure authentication watermarking in dispersed-dot halftone images, and the hidden biometric data was extracted accurately from the carrier image. Vatsa et al. (2004) presented a case where a face image was used as the cover image and an iris code as the watermark for multi-biometric verification using four kinds of watermarking algorithms. Meanwhile, several types of attacks were studied to evaluate the robustness of various algorithms in their work. Recently, they presented a 3-level RDWT biometric watermarking algorithm (Vatsa et al., 2009) to embed the voice biometric MFC coefficients in a color face image. The watermarking algorithm used adaptive user-specific watermarking parameters to improve the performance of hiding method. Also, the experimental results indicated that the proposed algorithm was robust against some frequency and geometric attacks. Noore et al. (2007) presented a watermarking technique using face and demographic text data as multiple watermarks for verifying the chain of custody and protecting the integrity of a fingerprint image. The watermarks were embedded into the coefficients of DWT. Combining DWT

* Corresponding author. Tel.: +86 13756158633; fax: +86 431 85696533.
** Corresponding author at: Computer School, Northeast Normal University, Changchun, China. Tel.: +86 13756158633; fax: +86 431 85696533.
E-mail addresses: qim801@nenu.edu.cn (M. Qi), luyh@nenu.edu.cn (Y. Lu), kongjun@nenu.edu.cn (J. Kong).

1084-8045/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2009.12.004

and LSB, literature (Vatsa et al., 2006) proposed a multimodal biometric image watermarking scheme that embedded the feature vectors of a face image into a fingerprint image in order to verify the integrity of biometric data. The results demonstrated that the proposed method was more robust against a set of attacks. Khan et al. (2007) introduced a chaotic secure content-based hidden transmission scheme using DWT. They encrypted biometric data using chaotic encryption to guarantee the system was more secure and protected from the copy attack.

Analyzing existing biometric data hiding methods, almost all of them adopt the idea of digital watermarking and hide one or more biometric image/s or its/their features into another biometric image directly based on transform domain for verification. These methods are robust against some types of attacks but the hiding capacity is not high. For example, literature (Vatsa et al., 2004) embedded 10×100 bits to the grayscale face image of size 1024×768 and the average capacity is about 0.0013 bit/pixel. It embedded 128×128 face template into the grayscale fingerprint of size 512×512 in Vatsa et al. (2006), where the average capacity is about 0.0625 bit/pixel. However, due to their real or supposed secret characteristics of biometric images, when transmitting biometric images as carriers there is the risk that attackers will try to intercept or destroy them resulting in degrading the security of transmission. For security purpose, the steganography technique, which hides the very existence of secret communications (Chang et al., 2009) and allows hiding large amounts of information within image, is employed to embed multimodal biometric images into the public transmitted image in this paper.

Regarding information hiding methods, researchers recently are paying more attention to the similarity between secret image and cover image for enhancing the imperceptibility and hiding capacity using block–block scheme (Kermani, 2005; Wang and Tsai, 2007; Shen and Hsu, 2007; Hedieh Sajedi and Mansour Jamzad, 2008). In these methods, both the secret image and the cover image were divided into fixed non-overlapping image blocks in advance, and then computed their similarity. In addition, to insert the secret information into the cover image with transparency and robustness, the characteristics of the human visual system (HVS) are often considered in the process of hiding (Kutter and Winkler, 2002; Eyadat and Vasikarla, 2005; Qi et al., 2008; Lee and Tsaia, 2009). The perceptual masking of the HVS is used to determine perceptually significant positions for embedding robust and transparent information. Thus, the embedding strength is adaptive to the features of the cover image and could guarantee maximum-possible imperceptivity.

In this paper, a novel biometric images hiding approach with high capacity is proposed, which aims to protect the multimodal biometric images (palmprint and iris) for secret and secure transmission. The cover images, as transmission carriers, have no specific and visual relations to the biometric images, which can assure the security compared with existing biometric information hiding methods. On the sender side, the sample images are first divided into non-overlapping regions for each modality. Then, the related regions are located in the cover image to reconstruct the non-overlapping regions best through correlation analysis using PLS and PSO. After correlation analysis, the residual images, which cannot be represented by the regions, are generated with much less energy. Second, considering the human visual system (HVS) model, the residual images as the secret images are embedded into the middle-significant-bit plane (MSB) of cover image for resisting some common attacks, which also guarantees the quality of stego-image simultaneously. Finally, the biometric images are extracted for identification on the receiver side.

The extensive experiments prove the proposed multimodal biometric images hiding method exhibits the following advantages: (1) high hiding capacity, the average capacity is about 0.1094 bit/pixel; (2) perfect stego-image quality, the PSNR is higher than 49; (3) good robustness, the stego-image is resilient to some common attacks such as frequency and geometric attacks.

The remainder of this paper is organized as follows. Section 2 describes the relative methods for correlation analysis briefly. Section 3 proposes the process of proposed biometric images hiding method. The multimodal biometric identification is depicted in Section 4. Section 5 presents the extensive experimental results, followed by the conclusions and future work in Section 6.

2. Relative methods

2.1. Partial least squares

Partial least squares (PLS) regression (Wold, 1985) is a multivariate data analysis method developed from the practical application, which is mainly used for regression model between multi-dependent variables and multi-independent variables. Compared with ordinary multiple regressions, PLS possesses many advantages, such as avoiding the harmful effects of multicollinearity, and being capable of building the models when the number of observation is less than the number of variables, etc. The goal of PLS regression is to predict Y from X and to describe their common structure. Let X be the mean-centered n by m data matrix of n observations on m predictor variables, Y be the mean-centered n by r data matrix of n observations on r response variables. In PLS, X and Y are decomposed using a given number of latent variables as follows:

$$X = TP^T + E,$$
$$Y = UQ^T + F, \quad (1)$$

where T and P are the score and loading for X, U and Q are the score and loading for Y, E and F are the residual for X and Y. The first score vector $t_1 = Xw_1$ with the constraint $w_1^T w_1 = 1$, is the linear combination of predictor data X that has maximum covariance with the y-scores $u_1 = Yc_1$ with the constraint $c_1^T c_1 = 1$. w_1 and c_1 are the eigenvectors corresponding to the largest eigenvalues of matrices $X^T YY^T X$ and $Y^T XX^T Y$, respectively.

The regression equation of X and Y respect to t_1 and u_1 can be described as:

$$X = t_1 p_1^T + E,\ Y = u_1 q_1^T + F, \quad (2)$$

where $p_1 = X^T t_1 / \|t_1\|^2$, $q_1 = Y^T u_1 / \|u_1\|^2$.

2.2. Particle swarm optimization

Particle swarm optimization (PSO) is introduced by Kennedy and Eberhart (1995). It is an evolutionary metaheuristic inspired by the flocking behavior of birds, which has successfully been used to solve optimization problems in some fields (Sun, 2009; Zhou et al., 2009; Oliveira and Schirru, 2009).

In the PSO algorithm, each potential solution, called a particle, owns a random generated velocity that directs the particle through the problem space by the fitness value. For the optimization process, each particle is initialized with a random position (X_{id}), velocity (V_{id}), and a fitness value evaluated with a predefined fitness function. Then, the fitness value of each particle is updated based on the local best value (P_{id}) and global best value (P_{gd}). The local best value is the best solution that the particle has achieved in the current stage. The global best value is the overall best solution tracked by the particle swarm optimizer. After