Information Sciences 269 (2014) 1–20

Contents lists available at ScienceDirect

Information Sciences

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

Two-factor face authentication using matrix permutation transformation and a user password ☆

Jeonil Kang [a], DaeHun Nyang [b,*], KyungHee Lee [c]

[a] School of Information and Communication Engineering, INHA University, Incheon, Republic of Korea
[b] School of Computer and Information Engineering, INHA University, Incheon, Republic of Korea
[c] Department of Electrical Engineering, University of Suwon, Suwon, Republic of Korea

ARTICLE INFO

Article history:
Received 24 December 2010
Received in revised form 27 June 2013
Accepted 1 February 2014
Available online 12 February 2014

Keywords:
Face authentication
Biometrics security
User privacy

ABSTRACT

Although authentication using biometric techniques is convenient, security issues such as the loss of personal bio-information are serious problems. However, the development of a secure biometrics scheme poses considerable challenges because users' bio-information is not precisely the same for each authentication attempt. This uncertainty during the authentication process obstructs direct application of cryptographic one-way functions in the authentication system. In this paper, we suggest a two-factor face authentication scheme using matrix transformations and a user password. Our scheme is designed with a secure cancellation feature, in that templates composed of permutation and feature vectors can be freely changed. Through experimental scenarios and results, we introduce the notable features of our scheme. Furthermore, we consider possible attacks on the proposed scheme and suggest security enhancement methods.

1. Introduction

A one-way transformation strengthens the security of encoded information if, upon comparison, the results of the transformed domain correspond with those in the original domain. On this basis, several authentication schemes have been introduced to adopt this unidirectional feature in their security strategies. Generally, unidirectionality makes template cancellation possible in biometrics. An old template should be replaced by a new template only after cancellation of the old template if security issues arise. Without unidirectionality, an attacker could recover bio-information from corresponding templates even after cancellation.

Owing to the difficulties encountered with unidirectionality in biometrics, relatively few schemes have been proposed. In particular, in face authentication, developing a scheme that has a high security level with high accuracy is difficult because the features used for classifying each face are not easily defined. In brief, sufficiently good classifiers are lacking in the field of face authentication, as opposed to other biometrics areas. Nevertheless, extensive research on face authentication, including security challenges, has been performed, because face authentication has considerable advantages in terms of both economics and non-intrusiveness.

☆ Portions of the research in this paper use the FERET database of facial images collected under the FERET program, sponsored by the DOD Counterdrug Technology Development Program Office.

* Corresponding author. Address: #307 Hi-tech Center, INHA University, 100 Inha-ro, Nam-gu, Incheon 402-751, Republic of Korea. Tel.: +82 32 876 8424; fax: +82 32 865 0480.

E-mail addresses: dreamx@isrl.kr (J. Kang), nyang@inha.ac.kr (D. Nyang), khlee@suwon.ac.kr (K. Lee).

http://dx.doi.org/10.1016/j.ins.2014.02.011
0020-0255/

In this paper, we suggest a two-factor face authentication scheme that has an efficient and secure cancellation feature in that the templates composed of permutation and feature vectors can be freely and efficiently changed, thereby resolving the security problems found in the scheme by Kang and colleagues [20]. In Section 2, we briefly look at the security aspects of biometrics, dealing specifically with face authentication. We then explain the basic concept of the scheme in Kang and colleagues and its security problems in Section 3. In Section 4, we introduce our new face authentication system with various considerations pertaining to the scheme. In Section 5, various experimental scenarios and results are presented. Section 6 addresses the security problems of our scheme, which also apply to Kang and colleagues. Section 7 discusses other issues, and Section 8 provides conclusions.

2. Security problems in biometrics

2.1. Biometrics for user authentication

Three methods are used for authenticating an entity in a general system: something you know, something you have, and something you are.

- ***Something you know*** is information possessed, such as passwords or personal identification numbers (PINs).
- ***Something you have*** includes physical items you possess, such as smart cards and universal serial bus (USB) devices.
- ***Something you are*** is bio-information, such as the face, fingerprints, the iris, and the voice. By definition, biometrics refers to methods of verifying the identity of individuals based on physical or behavioral traits, including bio-information, as well as the study of this field.

Bio-information is a strong method when it comes to authentication. For example, passwords (something you know) or hardware tokens (something you have) is easily guessed or stolen, but bio-information (something you are) is not. The probability of finding two persons with identical bio-information is very low. Therefore, it is widely held that bio-information can secure a system against forged authentication, and many organizations that require high security levels have adopted bio-information in their systems. Biometrics has been used in financial services, such as Internet banking and automatic teller machines. Many companies that require a high level of access control have employed biometrics for basic authentication means.

Unlike information utilized in the first two methods, bio-information is very difficult to change. When it comes to security issues, bio-information must not be revealed. If a template (that is, the bio-information stored in the system) is revealed, then it must be removed from the system and replaced with a new template in order to prevent threats to other systems or databases. In addition, bio-information can be physically spoofed [35,5,48].

Biometric data that can be removed from stored templates and placed into new templates are referred to as cancelable biometrics [7,45]. However, this cancel-and-change procedure is difficult to achieve with some biometrics because people cannot offer the same bio-information to the system for every authentication attempt. This uncertainty makes the application of cryptographic one-way functions difficult due to an avalanche effect [56,16].

2.2. Face authentication

In particular, face authentication (the biometrics discussed in this paper) has a slightly different characteristic from other biometrics. Face authentication normally does not require special equipment, such as a fingerprint scanner, a microphone, or an infrared camera. The face provides a natural and initial means of distinguishing people, and thus people do not feel a sense of incongruity about face authentication. Despite those strong points, face authentication has several weak points. Face authentication suffers from relatively low accuracy compared to other systems. Moreover, people do not generally hide their faces, and thus an attacker can easily obtain the face images (s)he wants. Due to these weaknesses, face authentication is often utilized as a supplementary means of authentication.

2.2.1. Linear face recognition and face authentication

When comparing two face images, it cannot be expected that all position will indicate the same features. In linear projection face recognition, in order to allow a certain position to indicate the same feature, a face image is projected to a feature space. This procedure is referred to as "feature extraction." Our scheme utilizes the advantages gained from feature extraction.

Let $\mathbf{X} = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N\}$ be a set of N training face images. Each face image $\mathbf{x}_i \in \mathbb{R}^n$ can be represented by the feature vector $\mathbf{y}_i \in \mathbb{R}^m$.

$$\mathbf{y}_i = \mathbf{U}\mathbf{x}_i \tag{1}$$

where $\mathbf{U} \in \mathbb{R}^{m \times n}$ is the projection matrix for transforming an n-dimensional image space to an m-dimensional feature space.

Based on the methods for generating a projection matrix $\mathbf{U}$, several methodologies are available for face recognition schemes. For example, principal component analysis (PCA) schemes [3,54] extract a common feature from the complete raw data, and as such can be used to eliminate unessential information from face data. Linear discriminant analysis (LDA, also known as Fisher's linear discriminant) schemes [4,8,29,34,60] maximize the distance between classes and minimize