Cancelable Biometric Identification by Combining Biological Data with Artifacts

Nobuyuki Nishiuchi
Graduate School of System Design
Tokyo Metropolitan University
Tokyo, Japan
e-mail: nnishiuc@sd.tmu.ac.jp

Hiroka Soya
Graduate School of System Design
Tokyo Metropolitan University
Tokyo, Japan
e-mail: soya-hiroka@sd.tmu.ac.jp

Abstract—Recently, due to the ability to accurately and rapidly identify an individual using physical attributes, the development of identification systems using biometrics has attracted a great deal of interest. Despite progress with various types of systems, users are often hesitant to submit their unique biological data during the initial enrollment process. In addition, current biometric identification systems have a major vulnerability: spoofing. In this study, we introduce a novel method of cancelable biometric identification that combines biological data with the use of artifacts, and is resistant to spoofing.

Keywords—biometrics; cancelable; artifact; identification; image processing

I. INTRODUCTION

In present day information-oriented society, the ability to accurately and rapidly identify an individual in various situations, such as identity verification at an ATM, login authentication, and permitting access to secured rooms, has taken on considerable importance. Personal identification systems that rely on knowledge, for example, a password and ID number, or possession, for example, an ID card or keys, are subject to loss, counterfeiting, and theft. In addition, such systems suffer from the inability to identify the genuine user if the information is borrowed on permission of the user. Due to these limitations, the development of an identification system based on biometrics has attracted a great deal of interest as it obviates the requirement for physical possession or memorization of a security code, and has the potential to differentiate individuals with high accuracy. To date, fingerprints, veins, irides, retina patterns, and facial features and other features have been used for biometric identification. The ideal biological data for biometrics has the following five characteristics [1]:

(i) Distinctive: the biological data differs from one person to another.
(ii) Repeatable: the biological data remains constant over a long period.
(iii) Accessible: it is easy to view the biological data.
(iv) Acceptable: it is not objectionable to show the biological data.
(v) Universal: all people possess the biological data.

From different viewpoints, the five characteristics are associated with the potential problems and limitations of biometric identification.

A. Problems of Biometric Identification

Current biometric identification systems have a number of problems that are related with the five characteristics of biological data described in the above section. The three main problems are as follows:

Problem 1: all users are specified from the biological data.

As biological data is information linked directly with individuals, if biological data is leaked, the user can be specified using only the leaked biological data. This problem is related with characteristic (i).

Problem 2: the biological data cannot be replaced.

For instance, if a user’s fingers are lost, or if fingerprint information is stolen, the user cannot use a fingerprint identification system. This problem is related with characteristics (ii) and (v).

Problem 3: the biological data can be collected without consent of the user.

In general, because biological features are exposed on the surface of the body, such as the face, fingerprints, and irides, it is difficult to keep these features located concealed from others. This problem is related with characteristics (iii) and (iv).

Due to these problems, current biometric identification systems have a major vulnerability: spoofing. Stén et al. [2] Hirabayashi et al. [3], and Matsumoto [4] described this vulnerability of biometric identification and demonstrated that it is possible with existing technology to obtain fingerprint information from adhered surface residue and replicate the fingerprint on an artificial finger. The theft and counterfeit of exposed biological information can be accomplished by first capturing an individual’s targeted information as a two-dimensional image, and then using the data to reproduce a counterfeit model.

Due to these problems, and despite progress with various types of biometric systems, users are often hesitant to submit their unique biological data during the initial enrollment process. It is easy to envision that users of restricted facilities, such as a building, commercial establishment, accommodations, and amusement parks, may
not willingly submit the necessary biological information for a biometric identification system.

To overcome these limitations, novel approaches for the development of practical biometric identification systems that do not retain or require potentially sensitive user information are needed.

B. Proposed Method of Cancelable Biometric Identification

In this study, we introduce a novel method of cancelable biometric identification that combines biological data with the use of artifacts and is resistant to spoofing. In this identification system, the user first attaches an artifact (a sticker with two dots) to the fingernail of the thumb or forefinger during the enrollment step, and subsequently presents the finger (biological data) with the attached artifact to the system. The position and direction of the artifact are uniquely detected based on the individual’s biological data (outline of finger) using image processing. In the identification step, the user presents the finger with the artifact, and identification is accomplished by comparison of the probe and reference data. As the randomness of the position and direction of the artifact on the fingernail is quite high, the user can be uniquely identified. Notably, this system represents cancelable biometric identification, because once the artifact is removed from the fingernail, re-enrollment is required. From the viewpoint of ease of use, our proposed method is more acceptable than other identification methods using artifacts, such as RFID Implants [5].

II. EXPERIMENTAL SETUP

The artifact and hardware prototypes used in the experimental biometric identification system are shown in Figures 1 and 2. A representative input image obtained using this system is shown in Figure 3.

III. ALGORITHM FOR CANCELABLE BIOMETRIC IDENTIFICATION

A. Image Processing for Artifacts

In this step, the center of each dot on the artifact in the input image is determined. First, the input image is binarized by the color of each dot (blue and red), and the area of each dot is extracted (Figure 4(a)). For the center of the blue area, horizontal maximum $X_{bmax}$ and minimum $X_{bmin}$ and vertical maximum $Y_{bmax}$ and minimum $Y_{bmin}$ are searched by horizontal and vertical scanning, respectively. The intersection point of line segment $X_{bmax}X_{bmin}$ and $Y_{bmax}Y_{bmin}$ is determined to represent the center of blue point area ($B_c$). Using the identical process, the center of the red area ($R_c$) is also detected (Figure 4(b)).
B. Image Processing for Fingers

In the next step of image processing, the finger outline is determined from the input image. The input image is first processed by binarization to separate the background and finger area into a binary image (Figure 5(a)). The finger outline is then obtained by edge extraction using a Laplacian filter (Figure 5(b)).

![Figure 5. Image processing for the finger.](image)

C. Feature Extraction

As a preprocessing step for feature extraction to equalize the volume of finger outline data, the finger outline is excised at a set distance (450 pixels) from the edge of the fingertip (indicated by a vertical line in Figure 6(a)), and the edges opposite the fingertip (towards the first finger joint) are connected with a line (Figure 6(a)). The fingertip location is decided based on the horizontal maximum point of the finger outline by horizontal scanning.

For the processing of feature extraction, the finger outline pixels are pursued in an anti-clockwise direction from the starting point until returning to that point, and the distance between pixels on the finger outline and the middle of the two dots (between $B_c$ and $R_c$) on the artifact is measured continuously. The starting point for pursuing the finger outline is detected based on the intersection between the finger outline and the extended line connecting points $R_c$ and $B_c$ on the artifact (Figure 6(b)).

A representative graph based on the feature extraction processing procedure is presented in Figure 7, where the horizontal and vertical axes represent the position of the pursued pixels and the measured distance, respectively. The red area in Figure 7 corresponds to the line connecting the two edges (red circles in Figure 6(a)) of the outline of the finger. The data within this area is not used during the comparison step.

![Figure 7. Distance between the pixels on the outline of finger and the middle of the two dots on the artifact.](image)

D. Comparison

In the final comparison step, the correlation coefficient is used for the comparison between the reference and probe data. Correlation coefficient $R$ is calculated using Equation (1):

$$R = \frac{\sum_{i=1}^{n} (x_i - \bar{x}_{aa})(y_i - \bar{y}_{aa})}{\sqrt{\sum_{i=1}^{n} (x_i - \bar{x}_{aa})^2} \sqrt{\sum_{i=1}^{n} (y_i - \bar{y}_{aa})^2}}$$

In Equation (1), $x_i$ ($i=1, 2, 3, ..., n$) represents reference data, $y_i$ ($i=1, 2, 3, ..., n$) represents probe data, and $\bar{x}_{aa}$ and $\bar{y}_{aa}$ represent the arithmetic average of $x_i$ and $y_i$.

IV. EXPERIMENTAL EVALUATION

A. Genuine Trial

To validate the repeatability of the proposed biometric identification method, five images of a finger with an attached artifact were captured from one subject (A) with the finger resting on the stage of the imaging system. The reference data (Data A1) was then compared with the probe data (from Data A2 to Data A4) of the genuine subject.

The result of the comparison is shown in Figure 8, where the horizontal and vertical axes represent the position of the pursued pixels and the measured distance, respectively, and the five lines represent each feature extracted from the five images of the genuine finger with the attached artifact. On comparison of the plotted reference and probe data, it is clear that they are quite similar. This determination was confirmed by examining the correlation coefficients resulting from the comparison (Table 1). As the correlation coefficients are all 0.996 or greater, the repeatability for the identification was considered to be high. In addition, the repeatability could be increased by using a guide for fixing the finger in place during the capture of the input image.
After validating the repeatability of the proposed method, its resistance to spoofing was next evaluated by capturing five images of fingers with an attached artifact from five subjects (A-E). The reference data (Data A) was then compared with the probe data (Data B to E) of the four imposter subjects. The result of the comparison between the data of the imposters and genuine user is shown in Figure 9, where the horizontal and vertical axes represent the position of the pursued pixels and the measured distance, respectively, and the five lines represent the features of each subject (A-E). It can be seen that lines of subjects D and E are quite similar to subject A. Table 2 lists the correlation coefficients resulting from the comparison between genuine user A with each of the imposters. However, for the genuine trial, the correlation coefficient values were 0.996 or higher, whereas the imposter trial resulted in values ranging from 0.680 to 0.983. In addition, the distributions from the genuine and imposter trials did not interfere. When the threshold value for identification was set at 0.995, both the false rejection rate (FRR) and false acceptance rate (FAR) were 0%. Even though the imposter subjects attempted to spoof the artifact position of the genuine user, it was impossible to spoof. It was difficult for the imposter subjects to set the artifact at the identical position and angle as that of the genuine user.

B. Imposter Trial

V. CONCLUSIONS

We have described a novel method of cancelable biometric identification that combines biological data with the use of an artifact. The proposed biometric identification system would be suitable for use as a one-day pass for office buildings, factory buildings, and amusement and medical facilities, among numerous other potential applications.

ACKNOWLEDGMENT

The authors would like to thank Mr. Toshihito Sioya To and Mr. Ryota Tsurumiat at Toppan Technical Design Center Co., Ltd. for their constructive support. This study was partially supported by the Research Fund of A-STEP (FS) in the Heisei 22 fiscal year, and the identification system presented in this chapter is patent pending (Japan Patent No. 2011-003885).

REFERENCES

[1] J. Wayman, National Biometric Test Center Collected Works 1997-2000, 2000, pp. 1–3.
[2] A. Stén, A. Kaseva, T. Virtanen, “Fooling Fingerprint Scanners – Biometric Vulnerabilities of the Precise Biometrics 100 SC Scanner”, Proceedings of 4th Australian Information Warfare and IT Security Conference 2003, 2003, pp. 333-340.
[3] M. Hirabayashi, T. Tanabe, and T. Matsumoto, “Can We Make Artificial Fingers That Fool Fingerprint Systems? (Part VI)”, IEIC Technical Report, Vol.103, No.715, Japan, 2004, pp.151-154.
[4] T. Matsumoto, “Biometric Authentication Systems: Vulnerability of Biometric Authentication: On the Issue of Physiological Spoofing “”, Information Processing Society of Japan Magazine, Vol.47, No.6, Japan, 2006, pp.589-594.
[5] P. Rotter, B. Daskala, R. Compañó, “RFID implants: opportunities and challenges for identifying people”, IEEE Technology and Society Magazine, 2008, Vol. 27, Issue 2, pp. 24–32.