physical biometrics,
dynamic data, anti-spoofing

Nobuyuki NISHIUCHI[1]

COMBINING DYNAMIC DATA WITH PHYSICAL BIOMETRIC VERIFICATION TO COUNTERACT SPOOFING

Current physical biometric verification systems are hampered by a major vulnerability: spoofing. Keeping biological information, such as the face, fingerprints, and irises, concealed from others in daily life is difficult, and therefore theft and counterfeit of exposed biological information can be relatively easily accomplished by first capturing an individual's targeted information as an image and then using the data to reproduce a model. Here, I propose a new method of physical biometric verification that uses dynamic data which are difficult to spoof. This basic concept can be applied to several types of biometric verification, such as those based on finger geometry, finger veins, irises, and the contour of the eyelid. I also propose an algorithm for this new verification method and provide experimental examples of its application.

1. INTRODUCTION

Personal verification systems which rely on knowledge, such as a password and ID number, or possession, such as an ID card or set of keys, are subject to loss, counterfeiting, and theft. In light of these limitations, the development of a verification system using biometrics has attracted a great deal of interest, as it obviates the need for physical possession or memorization of a security code and can differentiate individuals with high accuracy. However, despite this promising potential, current biometric verification systems have a major vulnerability: spoofing.

Yamada et al., Hirabayashi, and Matsumoto et al. pointed out this vulnerability in biometric verification and demonstrated that existing technology can be used to steal fingerprint information from adhered surface residues and replicate the fingerprint on an artificial finger [1-3]. Keeping biological information located on the exterior of the body, such as the face, fingerprints, and irises, concealed from others is difficult in daily life, and therefore this exposed biological information can be relatively easily stolen and counterfeited by first capturing an individual's targeted information as two-dimensional image and then using the data to reproduce a model.

To counter this Achilles' heel, several anti-spoofing approaches have been developed, among which the use of traditional behavioural biometrics which are difficult to spoof, such as car-driving style, dynamic facial features, keystroke dynamics, gait, and purchase history, has attracted attention from several research groups as potential methods of verification [4-9]. Yampolskiy et al. classified behavioural biometrics into five categories: authorship, human-computer interaction, indirect human-computer interaction, motor-skills, and pure behavioural biometrics [10]. In particular, the usefulness of behavioural biometrics based on the use of motor-skills has been demonstrated in many studies. In these previous studies, however, overall behavioural biometrics (motor skills) suffered from low accuracy of verification due to a lack of repeatability.

2. BASIC IDEA OF COMBINING DYNAMIC DATA WITH PHYSICAL BIOMETRICS

When applied to verification, both physical and behavioural biometrics have merits and demerits (Table 1). Although physical biometrics allow for high accuracy, they are relatively easy to spoof; in contrast, behavioural biometrics are difficult to spoof but have low repeatability and low accuracy. To overcome these drawbacks, we attempted to combine the advantages of both types of biometrics to

[1] Associate Professor in the Department of Management Systems Engineering, Graduate School of System Design at Tokyo Metropolitan University, Japan.

achieve greater overall benefit than using either alone. For example, only dynamic data—no behavioural characteristics—are extracted from motion of a body part for use in verification. Based on these dynamic data, biological data of physical characteristics are then compared. Concretely speaking, the biological data are compared only when dynamic data of probe data are consistent with reference data in the comparison process. Thus, strength against spoofing is achieved by using dynamic data, represented by the motion of a body part, and high verification accuracy is obtained by using biological data, represented by physical characteristics.

This basic concept can be applied to several types of biometric verification, such as those based on finger geometry, finger veins, irises, and the contour of the eyelid. Several such applications are described in further detail in the next section.

Table 1. Attributes of physical and behavioural biometrics.

	Physical biometrics	**Behavioural biometrics**
Advantages	High accuracy	Difficult to spoof
Disadvantages	Easy to spoof	Low accuracy (Low repeatability)

3. APPLICATIONS TO SEVERAL TYPES OF BIOMETRIC VERIFICATION

3.1. FINGER GEOMETRY AND FINGER MOTION

Here, I will first discuss finger geometry verification combining finger motion. In this scenario, the biological data of the "physical characteristic" aspect are the finger's geometry (the contour of the finger), and the dynamic data are the angle of the finger's joints.

The experimental system used to capture side images of a bending forefinger in this scenario is illustrated in Figure 1. After placing the forefinger up to the metacarpophalangeal joint into the field of view of the capture system, temporally continuous images of a user's bending finger were obtained using a single charge-coupled device (CCD) camera at 30 frames per second. A representative series of temporally continuous images captured using this system are shown in Figure 2.

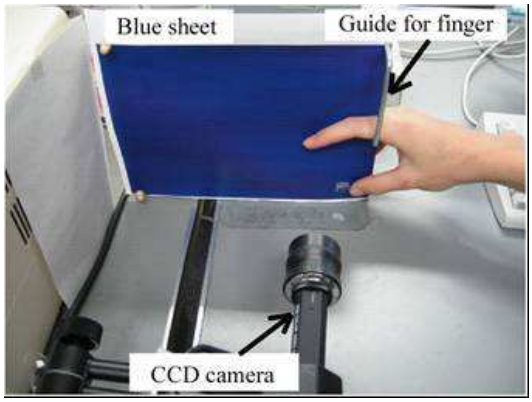

Fig.1. Experimental setup.

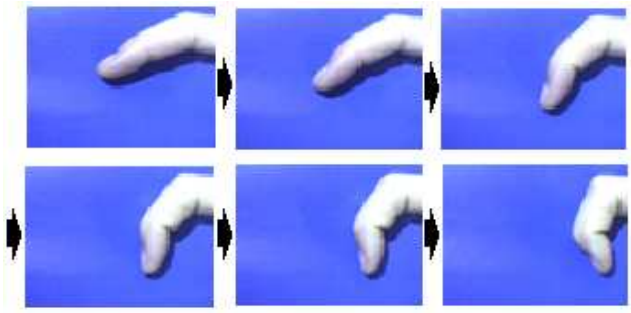

Fig. 2. Series of images showing forefinger bending.

To facilitate analysis of the captured images, binarization was used to extract the blue colour and separate the background and finger into a binary image. The edge pixels of the forefinger were then obtained by edge extraction using a Laplacian filter (Fig. 3). This proposed method is based on traditional hand geometry verification which uses the length and width of fingers and the thickness of the hand as biological features. Given that the extracted edge pixels of the forefinger in captured images include both biological and dynamic features, we determined the curvature of the extracted edge pixels, which

indicates the level of bending at each point on a curve or a curved surface as the feature for verification (Fig. 4).

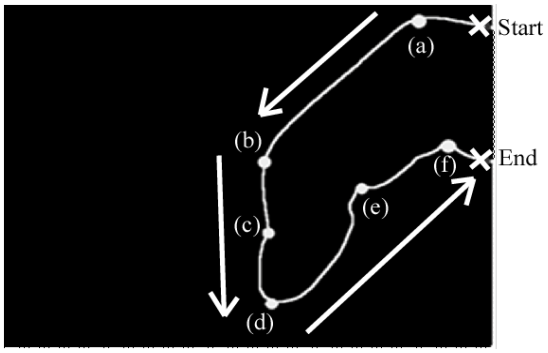

Fig. 3. Pursuing the edge pixels of the forefinger.

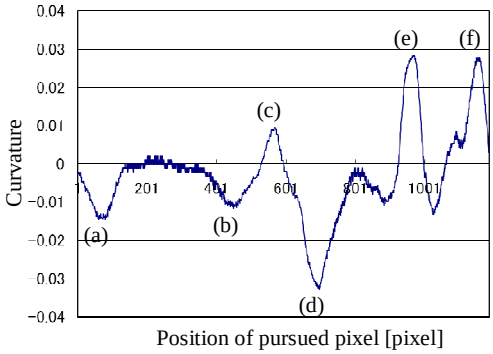

Fig. 4. Curvature profile of a bent forefinger.

Figure 5 is an overview of the comparison between reference and probe data. In the comparison step, the joint angle of the forefinger is measured as the dynamic data, and the curvature profiles (biological data) are compared only when the joint angle (dynamic data) of the probe data are consistent with reference data. Using this comparison step, the low accuracy characteristic of behavioural biometrics was significantly improved. Further, users need not replicate the exact same motion to serve as reference data, because biological data are only compared based on the dynamic data, providing an easy-to-use interface.

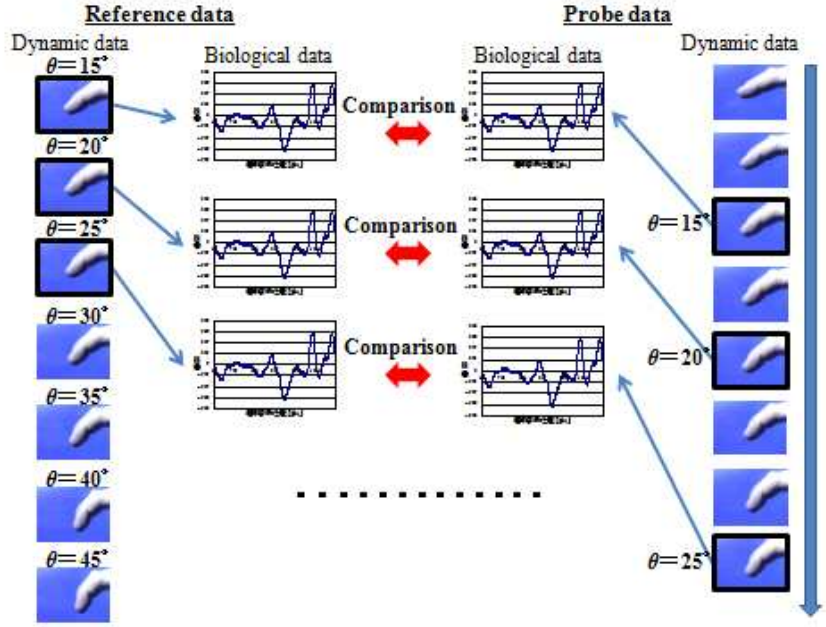

Fig. 5. Overview of the verification process comparing reference (left) and probe (right) data.

3.2. FINGER VEINS AND MOTION

In this section, I describe the combination of finger vein pattern verification with finger motion. In this scenario, the biological data of the “physical characteristic” aspect are the finger veins, and the dynamic data are the angle of the finger’s joints.

The experimental system used to capture side images of a bending forefinger in this scenario is illustrated in Figure 6. Near-infrared lighting was used, and polarization filters were installed onto the

lens of a CCD camera and in front of the lighting apparatus. As a result, only the near-infrared light that reflected freely inside the finger was captured by the camera, while light passing through directly was blocked by the polarization filter. Therefore, even if the forefinger moved while taking images, the vein pattern could be obtained with clarity (Fig. 7).

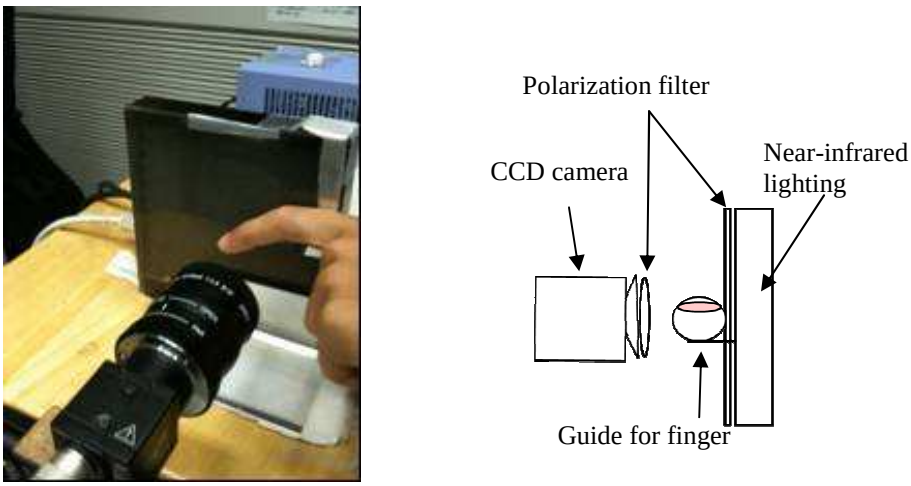

Fig. 6. Experimental setup.

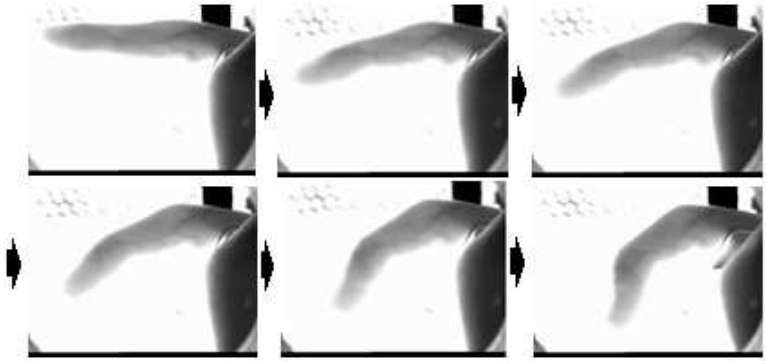

Fig. 7. Series of vein pattern images bending motion of the forefinger.

In the comparison step, the joint angle of the forefinger was measured as the dynamic data, and the vein pattern (biological data) was matched only when the joint angle (dynamic data) of the probe data was consistent with the reference data.

In addition, using this system, a gyrating motion of the finger can be assessed as dynamic data instead of a bending motion. In this case, the biological data of the physical characteristic would remain the finger vein pattern, and the dynamic data would be the rotating angle of finger.

3.3. IRIS AND EYE MOVEMENT

In this section, I describe the combination of iris verification with eye movement. In this scenario, the biological data of the “physical characteristic” aspect are irises, and the dynamic data are the gaze angle.

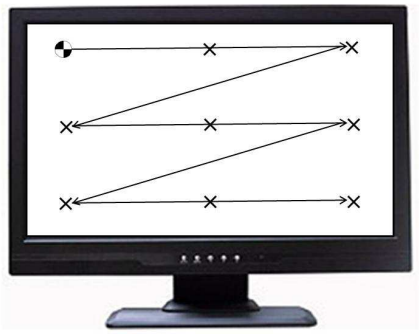

Fig. 8. Mark moving through nine points.

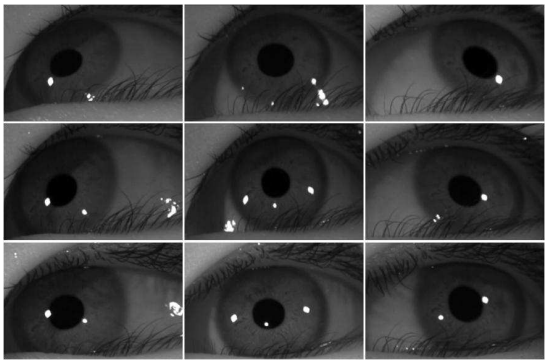

Fig. 9. Captured iris images oriented in nine directions.

The key point of this proposed method is the concavity and convexity of the iris surface, which means that the shape of the iris surface forms three dimensions. As such, the shadow pattern present in the iris differs according to the angle of lighting. With current iris verification systems, when the gaze angle at the device exceeds the tolerance (with the exception of the center image in Fig. 9), an error occurs and verification must be reattempted. However, the method proposed here uses various iris patterns (all images in Fig. 9) which, in previous verification methods, had given errors.

In this test, the user stared at a moving mark, following it through the nine points illustrated in Figure 8. Temporally continuous images of the user's iris pattern and the line of eye movement were obtained using an Eyemark Recorder (EMR-8B; Nac Image Technology Inc., Tokyo, Japan). Captured iris images oriented in nine directions are shown in Figure 9.

In the comparison step, the gaze angle at nine specific points was measured as the dynamic data, and the iris pattern (biological data) was matched only when the gaze angle (dynamic data) of the probe data was consistent with reference data.

3.4. CONTOUR OF EYELID AND BLINKING DEGREE

In this final section, I introduce the concept of blink verification. In this scenario, the biological data of the "physical characteristic" aspect are the contour of the eyelid, and the dynamic data refer to blinking, specifically the open-eye degree (length between top and bottom eyelids).

The experimental system used to capture images of blinking in this scenario is shown in Figure 10. After the user's face was placed in the retainer, temporally continuous images of their blinks were obtained using a high-speed camera at 1000 frames per second (FASTCAM-PCI; Photron Inc., Tokyo, Japan). A sample of the images captured using this system is shown in Figure 11.

Obtained images were first processed using binarization to separate the eye area and skin area into a binary image. The edge pixels of the upper eyelid were then obtained using edge extraction and fitted to a polynomial equation. The coefficient of the polynomial equation was then used for the biological data. Figure 12 is a graph based on the image processing described above, with number of frames described on

the X-axis and the coefficient of the polynomial equation (second-order coefficient in quadratic equation) on the Y-axis.

Given that the repeatability of blinking was not confirmed, the original biological data of the eyelid could not be used in the comparison step. Therefore, these data (Fig. 12) were normalized using the open-eye degree (dynamic data) described above.

Fig. 10. Experimental setup.

Fig. 11. Series of images blinking.

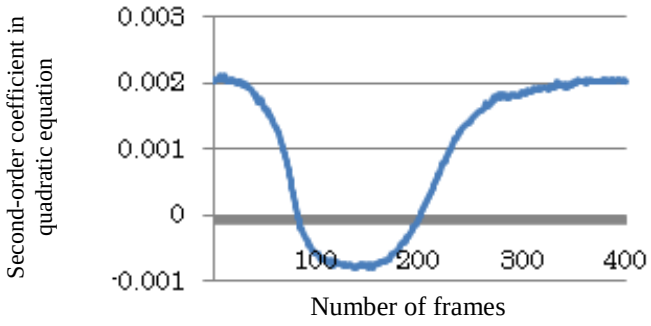

Fig. 12. Change in second-order coefficient of quadratic equation for blinking.

The contour of the eyelid lacks sufficient uniqueness for identification. However, given that the blinking reflex in humans is frequently unconscious, I proposed a verification system integrating data from several blinks, not simply one blink alone. Normalized biological data from five trials are integrated based on the open-eye degree, and these data are subsequently used in the comparison step. Without integration, an obscure difference was discernible between genuine and impostor normalized data, and less similarity across trials was noted for genuine data. By integrating data, a remarkable difference was discernible between genuine and impostor normalized data, and much greater similarity across trials was noted for genuine data.

4. CONCLUSIONS

In the present study, I proposed a new method of physical biometric verification combining dynamic data obtained from four sources: finger geometry, finger veins, irises, and eyelid contours (Table 2).

Table 2. Applications to several types of biometric verification.

	Biological data	**Dynamic data**
Finger geometry	Contour of the finger	Finger motion
Finger veins	Vein pattern	Finger motion
Irises	Iris pattern	Eye movement
Eyelids	Contour of the eyelid	Blinking

Several limitations to the present study warrant mention. First, it was not always possible to completely match dynamic data between the reference and probe data due to missing images, and an indeterminate comparison had to be conducted using the closest dynamic data available. To increase accuracy in verification in future evaluations, the number of frames captured per second (image sampling rate) during motion exercises should be increased, to provide more reference data. Second, the usability and accessibility of the system interface were may not be sufficient. Verification requiring a motion to be performed may be less usable and accessible than static verifications. The system interface should be easy-to-use and suitable for not only the average user, but older individuals and children as well.

Several strengths of this study also stand out. First, use of body motion in verification combines both biological data and dynamic data, thereby providing strength against spoofing. Further, this basic concept can also be applied in other types of physical biometric verification systems. Second, although based on dynamic data, using one of the most repeated body motions and comparing biological data based on dynamic data allows for compensation for differences between the motion of the probe and reference data and provides an easy-to-use interface for users.

BIBLIOGRAPHY

[1] YAMADA K., MATSUMOTO H., MATSUMOTO T., Can we make artificial fingers that fool fingerprint systems?, Technical Report of Institute of Electronics, Information and Communication Engineers, 2000, pp. 159–166.
[2] HIRABAYASHI M., TANABE T., MATSUMOTO T., Can we make artificial fingers that fool fingerprint systems? (Part VI), Technical Report of Institute of Electronics, Information and Communication Engineers, 2004, pp. 151–154.
[3] MATSUMOTO T., Biometric authentication systems: vulnerability of biometric authentication – on the issue of physiological spoofing, IPSJ Magazine, Vol. 47, No. 6, Information Processing Society of Japan, 2006, pp. 589–594.
[4] RYBNIK M., PANASIUK P., SAEED K., User authentication with keystroke dynamics using fixed text, Proceedings of the 2009 International Conference on Biometrics and Kansei Engineering, 2009, pp. 70–75.
[5] YAMANA N., INBE A., MIURA F., MAEJIMA A., MORISHIMA S., Face authentication system using 3D frequency component of moving image, IEICE Technical Report, 2006, pp. 13–18.
[6] RYGUŁA A., Driving style identification method based on speed graph analysis, Proceedings of the 2009 International Conference on Biometrics and Kansei Engineering, 2009, pp. 76–79.
[7] SANO T., SATO E., YAMAGUCHI T., Personal authentication based on buying history applying classification method, International Journal of Biometrics, Vol. 1, No. 2, 2008, pp. 209–230.
[8] NANDINI C., KUMAR C. N. R., Comprehensive framework to gait recognition, International Journal of Biometrics, Vol. 1, No. 1, 2008, pp. 129–137.
[9] OSADA R., AOKI T., YASUDA H., A real time verification system based on individual characteristic extraction of hand motion, Technical Report of Information and Communication Engineers, Vol. J84–D–II, No. 2, 2001, pp. 258–265.
[10] YAMPOLSKIY R. V., GOVINDARAJU V., Behavioural biometrics: a survey and classification, International Journal of Biometrics, Vol. 1, No. 1, 2008, pp. 81–113.