Multi - Factor Authentication Using Spectral Biometrics

Davar PISHVA *

This paper describes the feasibility of enhancing existing biometrics technology with a spectroscopic method in order to prevent spoofing. It goes beyond the simple approach of an aliveness detection technique and proposes the implementation of verification of a person's unique 'spectral signatures' or 'factors' in addition to currently employed methodologies in a multi - factor manner to reduce the likelihood of an imposter getting authenticated. This paper also shows how to augment two widely used biometrics systems (fingerprint and iris recognition devices) with spectral biometrics capabilities in a practical manner and without creating much overhead or inconveniencing their users.

Keywords : Security, Authentication, Multi-factor authentication, Biometrics, Spectral biometrics

1. INTRODUCTION

Numerous technologies are available for automatic verification of a person's identity. The authentication process usually involves verification of what a person knows (e.g., passwords, pass phrases, PINs), has (e.g., tokens, smart cards), is (e.g., fingerprint, hand geometry, facial features, retinal print, iris pattern), or generates (e.g., signature, voice). Use of something known by a person and use of something held by a person are two simple identification/verification solutions widely used today. Biometrics (also known as biometry) is defined as "the identification of an individual based on biological traits, such as fingerprints, iris patterns, and facial features" [1], and relies on what a person is or can generate.

Using something you know requires only a good memory, but can on the other hand be easily overheard, seen, or even guessed. An item you hold can be stolen and used or copied later. Using biometrics might at first seem to overcome these problems since fingerprints, iris patterns, etc. are part of one's body and thus not easily misplaced, stolen, forged, or shared. However, the thousands of fingerprints that we leave everywhere in our daily life can be recovered forensically and molded into artificial fingers to

fool biometrics devices. Furthermore, with a commercially available high resolution digital camera, the iris pattern of a person's eye can be readily extracted from the person's facial picture and molded into contact lenses to be used to fool machines.

2. VULNERABILITIES OF EXISTING BIOMETRICS SYSTEMS

As biometrics technology becomes a preferred standard for identification and authentication in ATMs, credit card transactions, electronic transactions, e-passports, airports, international borders, nuclear facilities and other highly restricted areas, it has become more attractive to attackers and has provoked interest in exploration of spoofing mechanisms against biometric systems [2]. Matsumoto et al. showed in a test that eleven optical and silicon fingerprint sensors accepted artificial fingers in at least sixty percent of attempts [3]. Their experiment with two commercial iris recognition devices also showed that one could be fooled 50% of the time while the other 100% of the time [4].

Although susceptibility of most biometric system to spoofing have been experimented on fingerprint and iris recognition devices as these technologies are used in a variety of commercial products, other biometrics devices can also be spoofed and to give examples, a dummy hand can be used on a hand geom-

* Carnegie Mellon CyLab Japan

etry system, a high resolution picture can be used on face recognition system, etc.

3. MULTI-FACTOR AUTHENTICATION

A multi-factor authentication method, on the other hand, relies on either multiple biometrics or, biometrics in conjunction with smart cards and PINs in order to reduce the likelihood of an imposter being authenticated.

3.1 Use of Spectroscopic Techniques

Spectroscopy refers to a method of examining matter and its properties by analyzing light, sound, or particles that are emitted, absorbed or scattered by the matter under investigation [5]. A multiple biometrics system employing spectroscopy can make spoofing very difficult and time consuming, if not impossible. This is because a spectroscopic approach using various wavelengths allows us to examine various parameters of skin, underlying tissue, blood, fat, melanin pigment in eyes, etc. that vary from person to person, and makes spoofing a very difficult task of imitating multiple physiological characteristics.

3.2 Skin Morphology

Skin is a complex biological structure made of different layers with distinct morphologies and optical properties. Conventionally, it is described by dividing it into two major layers. The inner layer, or the dermis, is between 1 to 4 mm thick and consists mainly of connective tissue composed of collagen fibers. Other dermal structures include nerves, blood vessels, lymph vessels, muscles, and gland units. The outer layer, the epidermis, is typically 40- μ m thick, but it can be much thicker on load-bearing areas such as palms and soles.

3.3 Skin Reflectance

When we look at light reflected from the skin, we usually see two distinct reflection components : a specular or interface reflection component L_s and a diffuse or body reflection component L_b [6]. The specular or interface reflection occurs at the surface and in only one direction, such that the incident light beam and the surface normal are coplanar, and angles between incident and reflected light are equal with

respect to the surface normal.

As shown in Fig. 1, not the entire incident light is reflected at the surface and some penetrate into the skin. The refracted light beam travels through the skin, hitting various physiological particles from time to time. Within the body, the light rays repeatedly get reflected and refracted at boundaries that have different refractive indices. Some of the scattered light ultimately return to the surface and exit from the skin in various directions, forming the diffuse reflection component L_b . This component carries information about the person's skin color and his/her unique biological 'spectral signature'.

Fig. 1 Principle of body reflectance.

Using the 2-layer model, Ohtsuki and Healey [7] determined the surface reflectance, which takes place at the epidermis surface, to be about 5 % of the incident light, independent of the lighting wavelength and the human race [8]. The rest of the incident light (95 %) enters the skin and becomes absorbed and scattered within the two skin layers. The absorption is mainly due to such ingredients in the blood as hemoglobin, bilirubin, and beta-carotene. Fig. 2 shows a spectral reflectance curve of a typical Caucasian skin [8] [9].

Fig. 2 Spectral reflectance of a typical Caucasian skin. [9]

Fig. 3 shows an exploded form of this spectrum into its distinct components, namely : epidermis and hemoglobin (there are also spectra of water and collagen substances, but these do not play a significant role in the indicated wavelength range). As can be observed, the melanin in the epidermis absorbs the most part of blue light at $\sim 470\text{nm}$; and hemoglobin absorbs green light at $\sim 525\text{nm}$ and red light at $\sim 640\text{nm}$. Also, though not shown, near infrared light at 850nm is used to identify papillary dermis [9].

Fig. 3 Distinct components of skin reflectance. [9]

3.4 Principle of Operation

Usually after making electromagnetic radiation, in the form of light, propagate into an individual's skin, the spectrum of light scattered from his/her tissue as body reflectance is measured. The measured spectrum contains information about a person's skin, underlying tissue, distribution of blood and blood vessels within the skin, etc., which are unique to the person, and can thus be used for identification of the person.

In the enrollment phase of biometrics [10], a user's biometrics traits are acquired in the form of a spectrum and the spectral variation of multiple wavelengths of a predetermined wavelength interval is converted into a template and stored in a database. In the verification process, a spectrum is acquired anew, and after extraction of the relevant multiple information from the newly acquired spectrum, a comparison is made with the data in the database. The individual is designated as having an identity associated with the previously stored spectral variation if the measured spectral variation is consistent with the previously stored spectral variation.

Although the use of spectral biometrics as the sole

identification method may be difficult due to intra-individual variations of 'spectral signature', a combination with a primary biometrics signature (e.g., fingerprint, iris pattern, etc.) can ensure that the identity obtained through the primary biometrics signature comes from a living, authentic person.

4. SPECTROSCOPIC INVESTIGATION

In order to establish the feasibility of using a person's reflectance spectra as a complementary method to ensure the individual's aliveness and authenticity in a biometrics identification process, a number of spectra from every finger of numerous persons were measured at different times. This section briefly explains the measurement process and obtained results.

4.1 Experiment Setup

The following optical setup, which simulates the measurement environment of commercially used optical fingerprint sensors, was used for making measurements.

Fig. 4 Optical setup used for measuring fingerprint spectra.

As can be observed, finger reflectance spectra were measured with a 45-degree projection and 0-degree detection setup. An I2 lamp was used as a light source and a commercial photodiode array (PDA) spectrometer was employed as the detecting device. The spectrometer sampling time was set to 1 second, i.e., each spectrum was measured in 1 second. A sheet of white diffuser paper was used as a reference sample. All measurements were carried out through a glass plate

to simulate the effect of fingerprint scanners and maintain a uniform sampling environment. A total of 150 reflectance spectra (350nm~1050nm) from 10 fingers of 5 Japanese persons having a similar complexion was measured at three different times in order to investigate intra-individual and inter-individual spectral variations. The experimental conditions during the three measurements were set so that there were no possible spectral alterations due to consumption of alcohol, exposure to warm/cold temperature, or other situation that could alter an individual's complexion, blood circulation, etc., as it was done for the sake of a preliminary examination.

4.2 Intra - individual variations

Fig. 5 shows the three spectra that were captured from the right index finger of an individual at three different times. As can be observed, the spectra look identical, understandably because, it comes from an object of the same finger pattern, skin color and physiological structure.

Fig. 5 Spectral variation in the same person's finger.

Fig. 6 shows spectra of the same person's left and right index fingers. Although coming from the same individual (i.e., same skin color and physiological structure), there are some differences in the spectra that can largely be attributed to finger pattern differences between the individual's left and right index fingers.

Fig. 6 Spectral variation in the same person's different fingers.

4.3 Inter-individual variations

Fig. 7 shows spectra of the right index fingers of five different persons. As can be observed, there are significant variations in the spectra as there are numerous physiological differences among individuals. Thus, it looks feasible to use such variations at different wavelengths to monitor and check aliveness and authenticity of the person during a biometrics' verification process.

Fig. 7 Finger spectral variation among different individuals.

5. CONFIGURATION OF THE PROPOSED SYSTEM

This paper proposes spectral biometrics methods as enhancement techniques for preventing spoofing in existing biometrics technologies. The idea is to double check the authenticity of an identified subject in order to ensure that a live person with a matching biological 'spectral signature' is being authenticated. As such, implementation and configuration of multi-factor spectral biometrics would depend on the configuration of the base biometrics authentication technology used in the system.

Moreover, when complementing existing biometrics technology with a spectral biometrics method, factors such as the device size, performance, cost, power requirements, operating environment, and human interaction requirements must also be considered. Taking these into account, this section shows how the two widely used biometrics systems (fingerprint and iris recognition devices) can be augmented with spectral biometrics without creating much overhead or inconvenience to users.

5.1 Multi-factor Spectral Based Fingerprint Scanners

Fig. 8 is an optical diagram of a frustrated total internal reflection (FTIR) based fingerprint sensor [11]. In this configuration, light at the ridges are ab-

sorbed and randomly scattered, but at the valleys, specular reflectance occurs and the specularly reflected light is fed into the camera. A CCD/CMOS forms an image of the fingerprint by sensing the specular light reflectance from the valleys and the lack of reflectance at the ridges (i.e., the fingerprint image gets created from specular reflectance of the light from the light source that occurs at the prism surface which remains at a distance from the valleys).

Fig. 8 An FTIR-based fingerprint sensor. [11]

Fig. 9 is an optical diagram for a spectral biometrics enhanced fingerprint sensor that uses FTIR with a sheet prism. In this configuration, diffused reflectance components of the light, which ultimately exits from the finger (at ridges and valleys), through the prism, are passed through a diffraction grating and a spectrum of the finger is formed on an extended portion of the original sensor (CCD/CMOS).

Fig. 9 Optical configuration of a spectral biometrics enhanced fingerprint sensor.

In the above configuration, size reduction gained from replacing a single large prism with a sheet prism is used to accommodate additional optics required to capture finger spectrum. Furthermore, capture of the spectrum on an extended portion of the sensor not only maintains device's compactness, but also allows multiple identical spectra to be formed on that portion of the sensor, a binning operation on which can result in an intensified single spectrum that has a much higher signal to noise (S/N) ratio.

5.2 Multi-factor Spectral Based Iris Recognition Devices

An iris recognition system relies on the iris pattern which is formed as an image on the CCD/CMOS device. However, unlike the image of an FTIR based fingerprint system, which is formed from specular reflectance, an iris image is formed as a result of body reflectance components from the eye.

Fig. 10 is a schematic diagram of an image acquisition system proposed by Wildes et al. [12]. In this configuration, light emerging from the circular polarizer has a particular sense of rotation. When it strikes specularly reflecting parts of the eye (e.g. the cornea) the light that is reflected back is still polarized, but has reversed sense and does not pass through camera's filter to form an image. In contrast, the diffusely reflecting parts of the eye (e.g. iris) scatter the impinging light. This light passes through the camera's filter and forms the image [13].

Fig. 10 Schematic diagram of the Wildes et al. image acquisition rig [12].

The simplest way to augment spectral biometrics into the system is to place a half-mirror between the camera lens and the detecting device, disperse the reflected portion of the light through a diffused grating and capture a spectrum on the extended portion of the detecting device, as shown in Fig. 11, in a similar manner that was explained for the fingerprint scanners.

Fig. 11 Optical configuration of a spectral biometrics enhanced iris recognition sensor.

In this configuration, the half-mirror can be made to transmit 80% to 90% of the light, so as not to adversely affect the quality of the iris pattern image taken by the system. On the other hand, by capturing the reflected portion of the light (10% to 20%) as spectra on hundreds of CCD rows simultaneously and integrating these spectra into a single spectrum, a spectrum that has sufficient S/N ratio for spectral analysis purpose can be obtained.

6. DISCUSSION

Intra-individual spectral variations seem to be negligible when observed on the same finger. However, there are intra-individual spectral variations among different fingers of the same person understandably because of the differences in the finger patterns. On the other hand, there are significant spectral variations among different people, as their finger patterns, skin color and other physiological structure are different. This shows that use of spectroscopic approach as a complementary measure to prevent spoofing is quite possible.

Furthermore, a large number of spoofing techniques against biometrics authentication systems

make use of an artificial or non-human material, such as a plastic fingertip, contact lens, copy medium, etc., to provide a false biometric signature. However, such objects cannot provide the same spectral information as that of a portion of a living human being. If an imposter, whose spectral variation closely resembles that of an authentic person, attaches a fingertip cover, molded to provide the image of the authentic fingerprint image, to his/her own fingertip, the detected spectral information may contain spectral information of the imposter's fingertip, which is spectral information of a living human being. Nonetheless, as long as the fingertip cover that is attached is an artificial object, or in the least, a non-living object, the detected spectral information will contain spectral information that differs from that of a living human being and thus as a whole, the detected spectral information will not be the same as that of a living human being. As an extreme example, even if the proposed system is presented with the severed finger of the authentic person, the spectrum pattern will still be different as the severed finger would no longer contain the person's living physiological components such as oxy-hemoglobin.

6.1 Special Features of the Proposed System

Traditional spectrometers either use a scanning grating and measure a spectrum one point at a time on a point sensor, or employ a photodiode array (PDA) and capture the whole spectrum at once on the detector. The point sensor system has the disadvantage of being slow and employing a moving component (i.e., scanning grating) while PDA system suffers from being less responsive to weak signals. Spectral biometrics system on the other hand, needs to withstand rugged environments, be fast and have enough sensitivity in order to measure reliable spectra from weak or highly scattered diffused reflectance signals.

This paper proposes a portion of existing sensor (CCD/CMOS) to be used for capturing the physiological spectra. It configures the portion to behave like an array of PDAs, each of which captures an identical spectrum simultaneously. Although the spectrum signal sensed by each of the array may contain weak signals, after a binning process (adding them together) it would result in an intensified spectrum having a

much higher S/N ratio. Hence, the proposed system has high sensitivity, can withstand rugged environments and does not significantly alter the base biometrics authentication technology's specifications (such as device size, performance, cost, power requirements, operating environment, and human interaction). The proposed system can also operate within the speed tolerance of its base biometrics technology as spectra measurement and readout can be performed simultaneously with the base biometrics technology.

6.2 Enrollment and Verification Phase of the Proposed System

The enrollment phase of multi-factor authentication that employs spectral biometrics would consist of acquiring a primary biometrics signature (e.g., fingerprint, iris pattern, etc.) as well as users' biometrics traits in the form of spectra, converting the information into a template at a predetermined wavelength interval (e.g., melanin absorbance from 350 to 470nm, hemoglobin absorbance in the vicinity of 525nm, 640 nm and 850nm, arterial blood peak at 650 and 750nm, and venous blood peak at 750 and 925), and storing the template in a database.

In the verification (authentication) process, after determining the identity of the person through the base biometrics technology, the relevant multiple information are extracted from a newly acquired spectrum and compared with the template stored in database. The individual is considered authenticated if the result of his/her identity, determined from the primary biometrics signature, is consistent with that of 'spectral signature'. This ensures that the identity obtained through the primary biometrics signature comes from a living and an authentic person.

7. CONCLUSION

This paper showed that it is quite feasible to use spectral biometrics as a complementary method for preventing spoofing of existing biometrics technologies. The proposed method ensures that the identity obtained through the primary biometrics signature comes from a living, authentic person. It also showed how spectral biometrics can be implemented in two widely-used biometrics systems in a practical manner without introducing much overhead to the base

biometrics technology or inconvenience to users.

In achieving such objectives, this paper showed how to capture reliable spectra from highly scattered diffused reflectance (in case of fingerprint system) or weakened signal due to augmentation of half-mirror to the system (in the case of iris recognition system), by configuring an extended portion of the original sensor (CCD/CMOS) of the system into an array of PDAs, capturing identical spectrum on each array and binning them together in order to realize a single spectrum with a much higher S/N ratio.

ACKNOWLEDGMENTS

The author would like to thank his former colleagues at Otsuka Electronics Co. Ltd., especially Dr. Kazunori Tsutsui, who greatly facilitated and helped in the spectroscopic data acquisition. He is also grateful to the reviewers. They helped to improve the paper significantly.

References

- [1] P. McFedries. The Word Spy {biometrics. Available at <http://www.wordspy.com/words/biometrics.asp> }
- [2] From findBIOMETRICS, {Available at <http://www.findbiometrics.com/press-release/2560> }
- [3] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada and Satoshi Hoshino, "Impacts of Artificial 'Gummy' Fingers on Fingerprint System", Optical Society and Counterfeit Deterrence Techniques IV, Proceedings of SPIE, 4677, pp. 275-289, January 2002.
- [4] Tsutomu Matsumoto, Masashi Hirabayashi and Kenji Sato, "A Vulnerability of Irsi Matching (Part 3)", Proceedings of the 2004 Symposium on Cryptography and Information Security, the Institute of Electronics, Information and Communication Engineers, pp. 701-706, January 2004.
- [5] From Wikipedia, the free encyclopedia {spectroscopy. Available at <http://en.wikipedia.org/wiki/Spectroscopy> }
- [6] S. A. Shafer, "Using color to separate reflection components," Color Research and Application, vol. 10, no. 4, pp. 210-218, 1985.
- [7] Tomoyuki Ohtsuki and Glenn Healey. "Using color and geometric models for extracting facial features", Journal of Imaging Science and Technology, 42 (6), pp. 554-561, December 1998.
- [8] R. R. Anderson, J. Hu, and J. A. Parrish. Optical radiation transfer in the human skin and applications in vivo remittance spectroscopy. In R. Marks and P. A. Payne, editors, Bioengineering and the Skin, chapter 28, pp. 253-265. MTP Press Limited, 1981.
- [9] From Melanoma. {Skin reflectance spectra. Available at

- [http://melanoma.blogsome.com/2006/03/24/skin-reflectance-spectra/.](http://melanoma.blogsome.com/2006/03/24/skin-reflectance-spectra/)
- [10] T. van der Putte and J. Keuning. Biometrical fingerprint recognition: don't get your fingers burned. In Proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, pages 289–303. Kluwer Academic Publishers, September 2000.
- [11] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. Handbook of Fingerprint Recognition. Springer Verlag, New York, NY, USA, chapter 2, pp. 53–81, June 2003.
- [12] R. P. Wildes, J. C. Asmuth, G. L. Green, S. C. Hsu, R. J. Kolczynski, J. R. Matey and S. E. McBride, “A machine vision system for iris recognition”, Machine Vision and Application, 9, 1–8, 1996.
- [13] F. A. Jenkins and H. E. White, “Fundamentals of Optics”, Macmillan, New York, 1976.
(2006年12月11日 受付)
(2007年 1 月18日 採録)
- [Contact Address]
Carnegie Mellon CyLab Japan, Kobe Harborland Center Building 17F
1-3-3 Higashikawasaki-cho, Chuo-ku, Kobe, Japan
Carnegie Mellon CyLab Japan
Davar PISHVA
TEL : 078-360-6328
FAX : 078-360-1618
E-mail : dpishva@andrew.cmu.edu

Information about Author

Davar PISHVA [non-member]

He received a B.Sc. degree in electrical engineering from the University of the Philippines, M.Sc. degree in computer science from Ateneo de Manila University, Philippines and Ph.D. degree in System Engineering from Mie University, Japan in 1983, 1986 and 2002, respectively. He initially came to Japan as a visiting lecturer to Osaka University and later joined a Japanese electronics company. He also served as a part time lecturer at Mie University. He is currently working as a Senior Teaching Staff at Carnegie Mellon CyLab Japan.* His research interests include information security, image processing, spectroscopy and software.

He is a member of the Institute of Electrical and Electronics Engineers (IEEE Computer Society) and the Institute of Electronics, Information and Communication Engineers of Japan (IEICE).

* From April 1, 2007 he will serve Ritsumeikan Asia Pacific University at the rank of an Associate Professor at the Department of Information Communications & Technology (ICT).