7

Use of Spectral Biometrics for Aliveness Detection

Davar Pishva
Ritsumeikan Asia Pacific University, ICT Institute
Beppu City,
Japan

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" (McFedries, 2007), and relies on what a person is or can generate.

Using something one knows requires only a good memory, but can on the other hand be easily overheard, seen, or even guessed. An item that one holds 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. Indeed, biometrics technology is becoming 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. Presently Europe leads the way but, the highest growth potential is forecasted to be in Asia as many Asian countries have already started adopting the technology. Its market size is estimated to be US$7.1 billion by 2012 (Bailey, 2008). Ironically however, this widespread acceptance of biometrics technology has been attracting the attention of attackers and has provoked interest in exploration of spoofing mechanisms against biometric systems. For example, the thousands of fingerprints that one leaves everywhere in one's daily life can be recovered and molded into artificial fingers for fooling biometrics devices based on fingerprint detection. In an experiment conducted by Matsumoto et al., eleven optical and silicon fingerprint sensors accepted artificial fingers in at least sixty percent of attempts (Matsumoto et al., 2002). 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 employing iris pattern recognition. An experiment conducted on two commercial iris recognition devices also showed that one of these devices could be fooled 50% of the time and the other 100% of the time (Matsumoto et al., 2002, 2004).

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

In view of this, international biometrics standard organizations are quite concerned about the vulnerabilities of biometrics system and reliabilities of corresponding countermeasures (Tilton, 2006). As a matter of fact, biometrics security, including spoofing, dominated agenda of UK Biometric Working Group (BWG) in their annual report during 2003/2004. The group, which helps the British government implement biometric systems, was instrumental in setting up the European Biometrics Forum (EBF) and creating BIOVISION (a one-year European initiative funded by the EC with the principal aim of developing a "Roadmap" for European biometrics for the next 10 years). BWG, which also serves as JCT1/SC37 (a formal standard body) and liaisons to SC27 (the subcommittee on information security), considers aliveness testing as an appropriate countermeasure against spoofing of biometric authentication (UK Biometric, 2003, 2004).

In an aliveness detection scheme, biometric authentication is augmented by a means for detecting that an object being presented to an authentication system is not an artificial dummy but is a part of a living person. For example, a fingerprint identification means may be augmented by a means that detects the blood pulse from a fingertip so that the fingertip presented for authentication can be judged to be that of a living person. However, even this method can be fooled, for example, by covering a living person's fingertip, which will provide a pulse, with a thin, plastic-molded artificial fingertip that can provide an authentic fingerprint pattern.

Although there are more reliable aliveness detection methods such as perspiration detection (Derakshani et al., 2003), skin color (Brownlee, 2001), medical-based measurement (Lapsley et al., 1998, Osten et al., 1998), rate of warming patents (O'Gorman & Schuckers, 2001), or challenges/responses methods (Fukuzumi, 2001), these are cumbersome in terms of device size, performance, cost, power requirements, operating environment, and human interaction requirements. Conversely, compact spectroscopy-based technologies which have been proposed for biometric identity determination (Rowe et al., 2007) can only work under a controlled measurement environment, as there are 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. The author has shown that although spectroscopy can be used to capture even differences in fingerprint pattern (Pishva, 2007, 2008, 2010) relying solely on spectroscopy for biometric identification can only worsen the biometrics false reject ratio as intra-individual spectral variation under a non-controlled measurement environment can be more than the spectral differences that exist due to fingerprint pattern differences.

2. Objective and spectroscopic method

As can be understood from the abovementioned examples, many spoofing techniques against biometrics authentication systems make use of an artificial or nonhuman material, such as a plastic fingertip, contact lens, copy medium, etc., to provide a false biometric signature. In view of this, the author considered that biometrics authentication systems can be significantly reinforced against spoofing by incorporating a means that enables judgment not simply of aliveness but judgment that an object being presented for authentication is a portion of a living human being that is free of any intervening artificial or prosthetic material.

An object of this work is therefore to provide a method and a system that enhances existing biometrics technology with a spectroscopic method in order to prevent spoofing. It goes beyond the simple approach of aliveness detection and proposes the implementation of verification of 'spectral signatures' or 'spectral factors' that are unique to human beings or a predetermined class or group of human beings in addition to currently employed methodologies in a multi-factor manner to reduce the likelihood of an imposter getting authenticated. Another aim of the work is to provide methods and systems that 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 the users.

2.1 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 (Wikipedia, 2011). 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.

2.2 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-μm thick, but it can be much thicker on load-bearing areas such as palms and soles.

2.3 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 (Shafer, 1985). 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".

Using the 2-layer model, Ohtsuki and Healey (Ohtsuki & Healey, 1998) 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 (Anderson & Parrish, 1981). 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

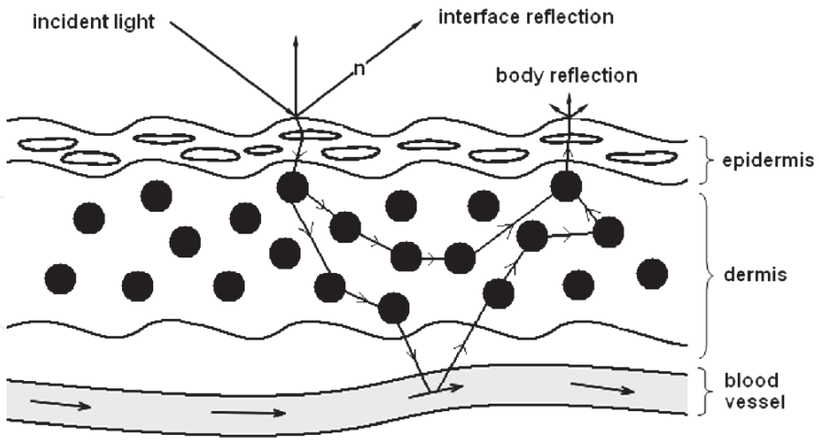
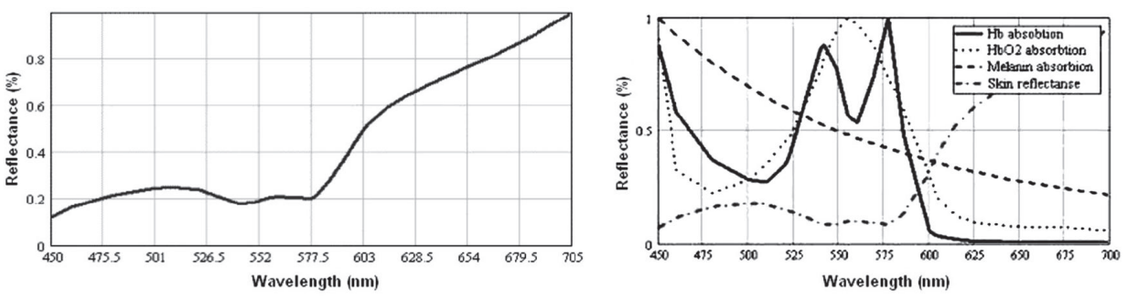


Fig. 1. Principle of body reflectance.

blood as hemoglobin, bilirubin, and beta-carotene. Fig. 2(a) shows a spectral reflectance curve of a typical Caucasian skin (Anderson & Parrish, 1981, Melanoma, 2006). Fig. 2(b) 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 ~ 470 nm; and hemoglobin absorbs green light at ~ 525 nm and red light at ~ 640 nm. Also, though not shown, near infrared light at 850nm is used to identify papillary dermis (Melanoma, 2006).



(a) Typical Caucasian skin spectrum (b) Its distinct components

Fig. 2. A typical Caucasian skin spectrum and its distinct components (Melanoma, 2006).

3. Proposed methodology and technical solution

In order to achieve the above mentioned objectives, this work proposes to augment a base authentication technique, such as optical fingerprint matching, in which a non-spectrometric biometric signature, such as a fingerprint image, is acquired from a biometric signature source, such as a fingertip, with a means of extracting spectral information from the same biometric signature source in a practical manner that does not affect the size, performance, cost, power requirements, operating environment, and human interaction requirements of the base authentication technique.

3.1 Multi-factor authentication approach

A multi-factor authentication method 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. One aspect according to this work provides: a multifactor authentication method including the steps of: acquiring a primary signature of a primary signature source of a subject to be authenticated; acquiring a secondary signature source of the subject; using the primary signature to determine the unique identity of the primary signature source; and using the using the secondary signature to verify that the subject to be authenticated belongs to a predetermined class of objects.

Here, the primary source is a non-spectrometric biometric signature of a biometric signature source of the subject to be authenticated; and the secondary source is a spectral information of the biometric (primary) signature source; wherein the non-spectrometric biometric signature is used for determining the unique identity of the biometric signature source; and the spectral information for verifying that the subject to be authenticated is an authentic living human being.

Here, the multifactor authentication method may further include the steps of: registering a non-spectrometric biometric signature of a biometric signature source of a subject to be authenticated; and registering spectral information of the biometric signature source; and in the step of using the non-spectrometric biometric signature to determine the unique identity of the biometric signature source, the acquired non-spectrometric biometric signature may be compared with the registered non-spectrometric biometric signature to determine the unique identity of the biometric signature source, and in the step of using the spectral information to verify that the subject to be authenticated belongs to the predetermined class of objects, the acquired spectral information may be compared with the registered spectral information to verify that the subject to be authenticated belongs to a predetermined class of objects.

Here, a 'non-spectrometric biometric signature' refers to an image, pattern, set of geometrical parameters, or other form of biological trait data obtained by an existing biometrics technology. Thus for example, the subject to be authenticated may be a person, and with this example, the predetermined class of objects may be 'living human beings with predetermined spectral characteristics,' the biometric signature source may be a fingertip, the non-spectrometric biometric signature may be a fingerprint image of the fingertip, and the spectral information of the biometric signature source may be a diffuse reflectance spectrum of the fingertip. That is, with this example, first, a fingerprint image of a person's fingertip is registered and a diffuse reflectance spectrum of the person's same fingertip is registered. Thereafter, a fingerprint image of a fingertip of a person, who is to be authenticated, is acquired, and a diffuse reflectance spectrum of this person's same fingertip is acquired. The acquired fingerprint image is then compared with the registered fingerprint image to determine the unique identity of the person, in other words, to determine that the fingerprint is that of the person to be authenticated, that is, the person whose fingerprint had been registered in advance and not that of anybody else, and the acquired diffuse reflectance spectrum of the fingertip is compared with the registered reflectance spectrum to verify that the person is actually a living human body with the predetermined spectral characteristics.

3.2 Reliability of the approach

Here, because the non-spectrometric biometric signature, such as a fingerprint image, of the biometric signature source, such as the fingertip, is augmented by the spectral information of the biometric signature source, such as the diffuse reflectance spectrum of the fingertip,

so that while the non-spectrometric biometric signature (e.g. fingerprint image) ensures the unique identity of the object or the person to be authenticated, the spectral information (e.g. diffuse reflectance spectrum) ensures that the non-spectrometric biometric signature (e.g. fingerprint image) is a genuine signature of the predetermined class of objects (e.g. living human beings), spoofing, for example, that uses the non-spectrometric biometric signature (e.g. fingerprint image) formed on an object (e.g. copy medium, plastic finger, etc.) not belonging to the predetermined class of objects (e.g. living human beings) can be prevented. That is, the spectral information of an object reflects the optical complexity of that object, and the more complex an object is, the more complex the spectral information. In particular, skin or other portion of a living human is a complex biological structure made of different layers with distinct morphologies and optical properties. Thus for example, a diffuse reflectance spectrum obtained from a fingertip includes spectral components of such substances as melanin, hemoglobin, and other constituents of skin, muscle, blood, etc., with which the proportions present, etc. differ among individual persons. The spectral information obtained from a fingertip or other portion of a living human is thus extremely complex and cannot be replicated readily by the use of artificial dummies and prosthetic devices, and especially because in the present approach, the non-spectrometric biometric signature of the same portion is acquired for identification, spoofing is made a practically insurmountable task.

In the above example of spoofing using a fingertip image printed on a copy medium, because any copy medium is an artificial object, such as paper, plastic, etc., or in the least, a non-living object, such as non-living skin, it cannot provide the same spectral information as that of a portion of a living human being. If an imposter attaches a fingertip cover, which is molded to provide the image of an 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. However, 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.

In the present approach, the spectral information is used to verify that the subject to be authenticated belongs to a predetermined class of objects. The predetermined class of objects is preferably broad enough to provide allowance for intra-object variations and yet narrow enough to preclude spoofing. In the above example, 'living human beings with predetermined spectral characteristics' is the predetermined class of objects, and this allows for intra-personal variations due to such external conditions as injury and exposure to high or low temperatures, chemicals, ultraviolet rays, or such internal conditions as changes in blood flow due to consumption of medicine, alcohol, etc., and at the same time precludes the use of artificial and non-living-human objects for spoofing.

3.3 Implementation steps and means

Here, the steps of acquiring the non-spectrometric biometric signature of the biometric signature source of the subject to be authenticated and acquiring the spectral information of the biometric signature source may be carried out simultaneously. This significantly shortens the time required for authentication.

In the step of comparing the acquired spectral information with the registered spectral information to verify that the subject to be authenticated belongs to the predetermined class

of objects, cluster analysis may be performed on the acquired spectral information and the registered spectral information to determine a similarity value of the acquired spectral information and the registered spectral information, and the subject to be authenticated may be verified as belonging to the predetermined class of objects when the determined similarity value is within a predetermined range.

Another aspect according to this approach provides: a multifactor authentication system including: a means for acquiring a non-spectrometric biometric signature of a biometric signature source of a subject to be authenticated; a means for acquiring spectral information of the biometric signature source; and a means that uses the non-spectrometric biometric signature to determine the unique identity of the biometric signature source and uses the spectral information to verify that the subject to be authenticated belongs to a predetermined class of objects.

Here, the multifactor authentication system may further include: a means for storing an acquired non-spectrometric biometric signature as a registered non-spectrometric biometric signature and storing an acquired spectral information as registered spectral information; and the means that uses the non-spectrometric biometric signature to determine the unique identity of the biometric signature source and uses the spectral information to verify that the subject to be authenticated belongs to a predetermined class of objects may compare a newly acquired non-spectrometric biometric signature with the stored, registered non-spectrometric biometric signature to determine the unique identity of the biometric signature source and compare newly acquired spectral information with the stored, registered spectral information to verify that the subject to be authenticated belongs to a predetermined class of objects.

In the above-described example where the subject to be authenticated is a person, the predetermined class of objects is 'living human beings with predetermined spectral characteristics,' the biometric signature source is a fingertip, the non-spectrometric biometric signature is a fingerprint image of the fingertip, and the spectral information of the biometric signature source is a diffuse reflectance spectrum of the fingertip, the means for acquiring the non-spectrometric biometric signature may be a CCD or CMOS detecting system, with which an image of the fingerprint is formed on a detecting surface of a CCD or CMOS sensor, the means for acquiring the spectral information may be a photodiode array (PDA) detecting system, with which diffusely reflected light from the fingertip is spectrally dispersed onto a PDA, and a computer or other information processing means may be used as the means that uses the fingerprint image (non-spectrometric biometric signature) to determine the unique identity of the fingertip (biometric signature source) and uses the spectral information to verify that the person (subject to be authenticated) is a 'living human being with predetermined spectral characteristics' (belongs to the predetermined class of objects).

Here, a half-mirror or a beam splitter may be used to simultaneously acquire the non-spectrometric biometric signature (e.g. fingerprint image) and the spectral information (e.g. diffuse reflectance spectrum), and an extended portion of the CCD/ CMOS detector may be configured as PDAs for simultaneously capturing numerous identical spectra to be integrated into a single spectrum having a sufficient S/N ratio for spectral analysis. The system can thereby be made compact and high in the speed of authentication.

4. Spectroscopic investigation

To thoroughly investigate the applicability, effectiveness and usability of the spectroscopic method as an enhancement technique for preventing spoofing in existing biometrics

technology, a number of spectra from real fingers, real fingers covered with a fingertip molds that provide fingerprint pattern of authentic persons and artificial fingers made of different materials that contain authentic fingerprint patterns, were measured and analyzed. In the analysis phase, reflectance values of numerous physiological components ('spectral factors') were extracted from the measured spectra and Euclidean distances (Wikipedia, 2011) among the corresponding extracted factors of the spectra were computed to verify authenticity of an identified individual.
A through explanation of the investigation is given in (Pishva, 2008) and the author will simply highlight the main findings here. Furthermore, even though the spectroscopic investigation was only carried out on fingerprint system, the approach is general and can very well be applied to other biometrics systems such as iris pattern, hand geometry, etc.)

4.1 Measurement

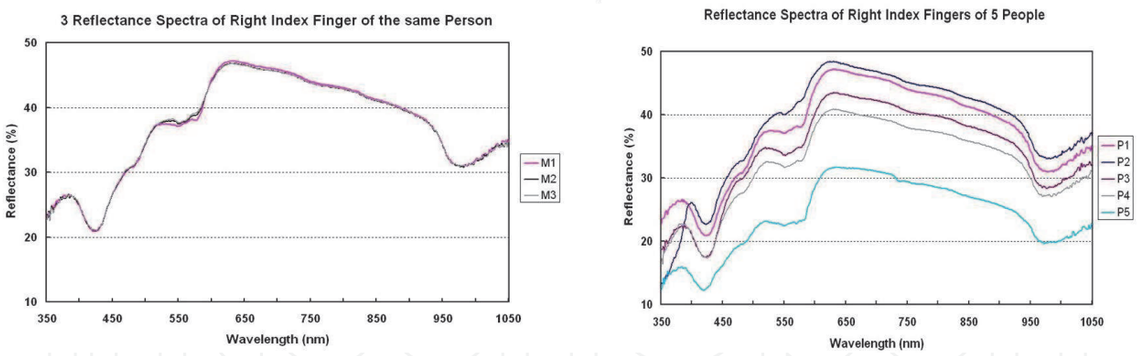
Initially a total of 150 reflectance spectra (350nm ~ 1050nm) from 10 fingers of 5 Japanese men having a similar complexion was measured at three different times in order to investigate intra-individual and inter-individual spectral variations. The experimental conditions during the three measurements 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.
In the second stage, under a similar condition, the five peoples' fingers were covered with fingertip covers made of transparent plastic and rubber materials in order to provide fingerprint pattern of an authentic person. A set of similar measurements were also taken from artificial fingers that were made of craft paper, wooden and plastic materials.
In the final stage, 750 spectra data were also measured from different fingers of a man (the above mentioned P1), a woman (W1) and a child (C1) under different conditions to study the effects of finger size, finger texture, finger orientation and as well as stableness of the 'spectral factors'. Some spectra were measured when fingers placed flat, while others when rotated to counterclockwise or clockwise directions by about 45°. Some spectra were measured right after having lunch while others late in the evening. Some spectra were also measured after consumption of alcoholic drink (i.e. sometimes after drinking two bottles of beer).

4.1.1 Spectral patterns of real fingers

Fig. 3(a) 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. 3(b) shows spectra of the right index fingers of five different persons. As can be observed, around a general pattern, there are significant variations in the spectra as there are numerous physiological differences among individuals. Thus, it looks feasible to use such pattern and variations at different wavelengths to monitor and check aliveness and authenticity of the person during a biometrics' verification process.

4.1.2 Spectral patterns of bogus fingers

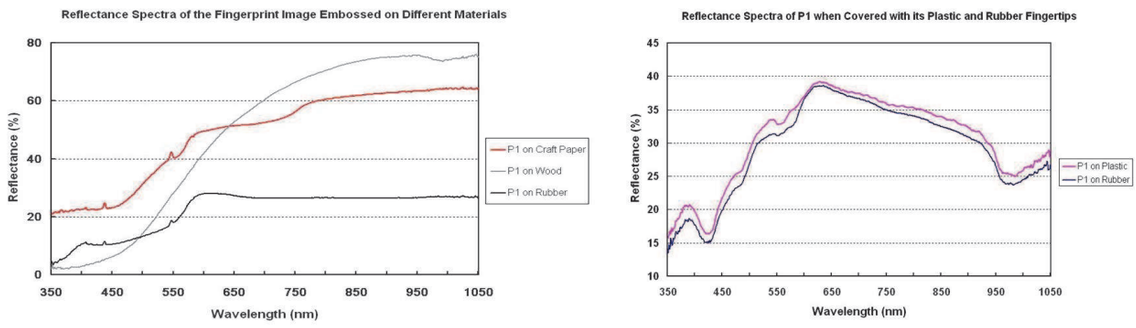
Fig. 4 (a) shows spectral patterns of artificial fingers made of craft paper, wooden and rubber materials (non-living objects) which are supposedly contain fingerprint of the person whose finger spectral pattern is shown in Fig. 3(a). As can be clearly observed, spectral patterns of craft paper, wooden and rubber fingers are quite different from each other and



(a) The same person's finger spectra (b) Variation among different persons

Fig. 3. An individual's finger spectra and spectral variation among different individuals.

they are also very much different from that of the authentic person's finger spectra. It is obvious that shape of the spectra from artificial finger highly depends on the base materials used in making them rather than the fingerprint pattern that is molded on them. Fig. 4(b) shows spectral patterns of the right index finger of the person whose finger spectral pattern is shown in Fig. 3(a), when covered with his fingertip prints made of transparent plastic and rubber materials. As can be observed, each spectrum, though different, have a general shape as the transparent fingertips are worn by the same person. It should also be noted that the spectra are different from those of the artificial finger spectra shown in Fig. 4(a) and the authentic one indicated in Fig. 3(a). This justifies an earlier claim that attachment of artificial fingertip cover on a real finger alters the reflectance spectra and is a proof of the robustness of the multi-factor spectral biometrics approach.



(a) Spectral patterns of artificial fingers (b) Spectral patterns with fingertips

Fig. 4. Spectral Patterns of Artificial Fingers and fingers covered with fingertips.

4.2 Data analysis

Cluster analysis with MINITAB statistical software (Minitab, 2009) was used for data analysis after extracting 'spectral factors' from the measured spectra. In this work spectral factors' refers to reflectance values at certain wavelengths or regions on a spectrum which correspond to specific physiological components. For example, in the finger reflectance spectrum of Fig. 5, shaded areas correspond to certain physiological components (i.e., 350 to 470 nm indicate melanin reflectance, vicinity of 525 nm, 640 nm and 850 nm indicate hemoglobin, vicinity of 650 and 750 nm are for arterial blood peak, and 750 and 925 nm are

for venous blood peak (Melanoma, 2006, Pishva, 2007). Each 'spectral factor' can be extracted by computing area of the corresponding shaded region.

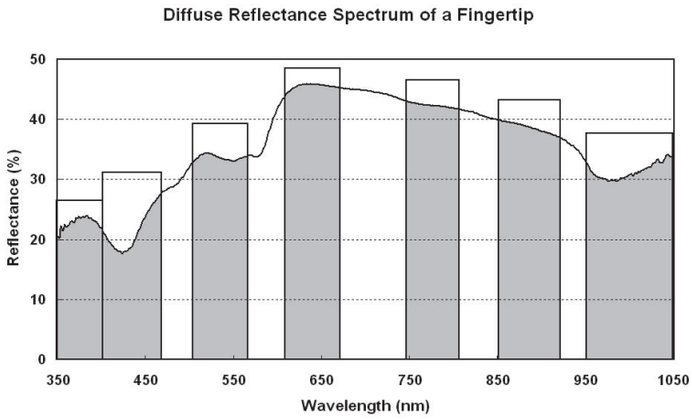


Fig. 5. 'Spectral Factors' Regions.

4.2.1 Results at verification phase – presentation of real fingers

Table 1 shows the 'Similarity' values that are obtained when P1-1 is used as the registered template set and the extracted 'spectral factor' sets of the five persons are presented, one set at a time, to the analysis routine as the newly acquired 'spectral factors' for verification.

Template Value	Newly Acquired 'Spectral Factors'	'Similarity' Level
P1-1	P1-1	100.00
P1-1	P1-2	99.47
P1-1	P1-3	99.49
P1-1	P2-1	96.03
P1-1	P2-2	96.39
P1-1	P2-3	96.29
P1-1	P3-1	92.20
P1-1	P3-2	92.01
P1-1	P3-3	92.02
P1-1	P4-1	86.86
P1-1	P4-2	86.87
P1-1	P4-3	86.01
P1-1	P5-1	65.49
P1-1	P5-2	65.49
P1-1	P5-3	64.71

Table 1. 'Similarity' values of real finger spectra.

As can be seen, whereas 'Similarity' values higher than 99% are obtained when the 'spectral factors' of the same finger of the same person are presented in the verification phase, the

'Similarity' value drops significantly (96% to 64%) when a different person's 'spectral factors' are presented.

4.2.2 Results at verification phase – presentation of bogus fingers

In the previous section, it was shown that a 'Similarity' value higher than 99% is obtained when the same person's 'spectral factors' are presented to the analysis routine. As such, some researchers have even proposed that skin spectroscopy alone can be used for biometrics identity determination of an individual (Rowe et al., 2007). This work, however, proposes spectral biometrics as an enhancement technique and not as an identification method.

Table 2 shows the 'Similarity' values determined in the verification phase when P1-1 is used as the registered template, and the 'spectral factors,' extracted from the index finger of P1 at different times under various conditions, the fingers of five persons covered with transparent plastic and rubber fingertip molds having the fingerprint pattern of the authentic person (P1) and artificial fingers made of craft paper, wooden and plastic materials that contain the authentic fingerprint pattern of P1, are presented one set at a time as the newly acquired 'spectral factors.'

Template Value	Newly Acquired 'Spectral Factors'	'Similarity' Level
P1-1	P1-2 (authentic, controlled)	99.47
P1-1	P1-m (authentic, after meal)	96.23
P1-1	P1-n (authentic after alcohol)	95.46
P1-1	P1onP1-PlasticCvr-1	82.00
P1-1	P1onP1-RubberCvr-1	78.28
P1-1	P1onP2-PlasticCvr-1	91.20
P1-1	P1onP2-RubberCvr-1	93.13
P1-1	P1onP3-PlasticCvr-1	85.05
P1-1	P1onP3-RubberCvr-1	84.09
P1-1	P1onP4-PlasticCvr-1	88.22
P1-1	P1onP4-RubberCvr-1	90.09
P1-1	P1onP5-PlasticCvr-1	81.21
P1-1	P1onP5-RubberCvr-1	79.44
P1-1	P1onCraftPaperFngr-1	62.85
P1-1	P1onWoodenFngr-1	48.94
P1-1	P1onPlasticFngr-1	59.27

Table 2. 'Similarity' values during verification process.

As can be observed from Table 2, 'Similarity' values obtained from artificial fingers and fingers containing fingertip covers are quite different from that of the real authentic finger. However, even for the real authentic finger, 'Similarity' values obtained under a controlled measurement environment is much better than those obtained under relaxed conditions

(e.g., after having meal or being under the influence of alcohol). In fact some 'Similarity' values obtained under a more relaxed condition are comparable to those values that were obtained from another person (e.g., person P2 in Table 1). This clearly indicates that although the use of spectral biometrics as the sole means for identity determination may be difficult, spectral biometrics can be used as an enhancement technique, as proposed in this work, since it discriminates authentic fingers from artificial fingers and fingers containing fingertip covers.

4.3 Optimal boundary conditions

In order to obtain a consistently reliable result, determination of optimal boundary conditions including establishment of optimal settings and effect of spectrum resolution was carried out. It was found out that the stability of the 'spectral factors' for consistently generating a 'Similarity' value higher than 95%, largely depended on the size of the measurement spot rather than on the physiological or environmental factors, or spectrum resolution. Sampling the center of a 1 cm^2 measurement spot, a condition which can easily be provided by thumb fingers, provided a uniform reflectance condition at the measurement point (Pishva, 2008).

5. System configuration and application scope

As mentioned earlier, this work 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 Preferred configuration for fingerprint authentication system

Preferred embodiments of this approach shall now be described. Fig. 6 is a schematic diagram of a basic arrangement of a spectral biometrics enhanced authentication system according to a first embodiment of this approach, which is a fingerprint authentication device that authenticates a person's identity based on his/her fingerprint and biospectral characteristics of his/her finger.

As shown in Fig. 6, this fingerprint authentication device 1 includes a measurement unit 2, a controller 120, a memory (storage device) 130, and a monitor 140. The measurement unit 2 includes an optical system 10 and a CCD (charge coupled device; image sensor) 100. The optical system 10 includes an I2 lamp (light source) 15, a sheet prism (prism means) 20, a first lens 40, a second lens 60, a mirror 70, and a diffraction grating 80. As shown in Fig. 7, the CCD 100 is an image sensor with pixels arranged in 1280 rows and 1024 columns and has an image acquisition portion 102 (first portion of a detecting surface of the CCD sensor),

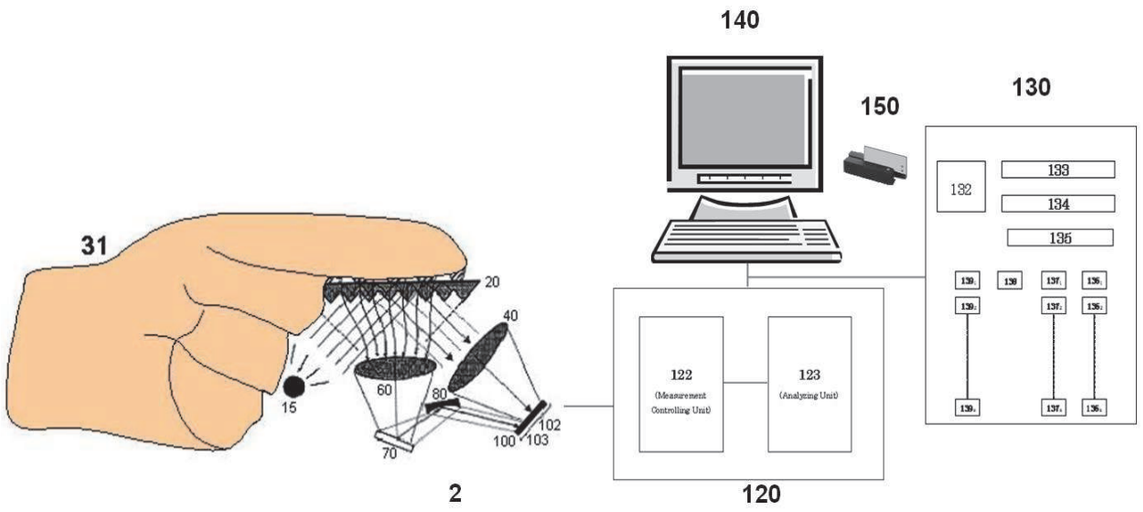


Fig. 6. A Schematic diagram of a basic arrangement according to a first embodiment.

which is a region of 960×960 pixels at an upper portion of the CCD 100 that excludes the pixels of 32 edge rows at the top side and 32 columns at each of the left and right sides of the CCD 100 as boundary pixels, and a spectrum acquisition portion 103 (second portion of a detecting surface of the CCD sensor), which is a region of 160×960 pixels at a lower portion of the CCD 100 that excludes the pixels of 32 edge rows at the bottom side and 32 columns at each of the left and right sides of the CCD 100 as boundary pixels. 96 rows of pixels between the image acquisition portion and the spectrum acquisition portion 103 are also handled as boundary pixels. The controller 120 is electrically connected to the CCD 100, the memory 130, and the monitor 140 and controls operations of these components by issuing appropriate instruction signals. The memory 130 has a measured image (matrix) storage area 132, a reference spectrum (vector) storage area 133, a measured spectrum (vector) storage area 134, a reduced measured spectrum (vector) storage area 135, registered image

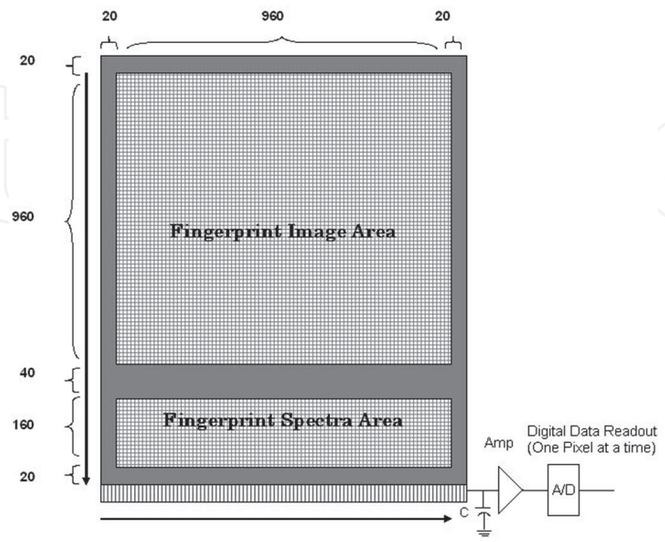


Fig. 7. A schematic diagram of a CCD (image sensor) according to a first embodiment.

pattern (template) storage areas 136_1 to 136_n (where n is an integer greater than 1), registered spectral template data storage areas 137_1 to 137_n, an identity storage area 138, and registered identity storage areas 139_1 to 139_n. The controller 120 is also electrically connected to a card reader 150 that serves as an identity inputting means.

A manner in which a fingerprint image is acquired as a non-spectrometric biometric signature of a fingertip (biometric signature source) of a person (subject to be authenticated) and a diffuse reflectance spectrum of the fingertip is acquired as spectral information of the fingertip (biometric signature source) by this fingerprint authentication device 1 shall now be described.

5.1.1 Incident light and its reflected components

As shown in Fig. 6, with this fingerprint authentication device 1, light from the I2 lamp 15 is made incident via a sheet prism 20 onto a finger 31_1, which belongs to a person 30_1 to be authenticated and is being pressed against an upper surface of the sheet prism 20. A portion of the light made incident on the finger 31_1 is reflected as a specular reflection component Ls from the surface of the finger 31_1, and a first lens 40 forms an image of this specular reflection component Ls on the image acquisition portion 102 of the CCD 100.

Another portion of the light made incident on the finger 31_1 penetrates into the skin, is refracted, reflected, absorbed, or re-emitted as fluorescence or phosphorescence, etc. by internal tissue, blood, and other various physiological components inside and below the skin, and some of this light ultimately returns to the surface and exits from the skin in various directions, thus forming a diffuse reflection component Lb. Because this light component results from light that has traveled inside the skin, it carries information concerning the person's skin color and his/her unique biological 'spectral signature' (Fig 4). After exiting from the skin, the diffuse reflection component Lb passes through the sheet prism 20 and is converged, via the second lens 60 and the mirror 70, onto the diffraction grating 80, which spectrally disperses and makes the diffuse reflection component Lb incident on the spectrum acquisition portion 103 of the CCD 100 in a manner such that a fingertip diffuse reflection spectrum of a range of 350nm to 1050nm is acquired from each row of the spectrum acquisition portion 103.

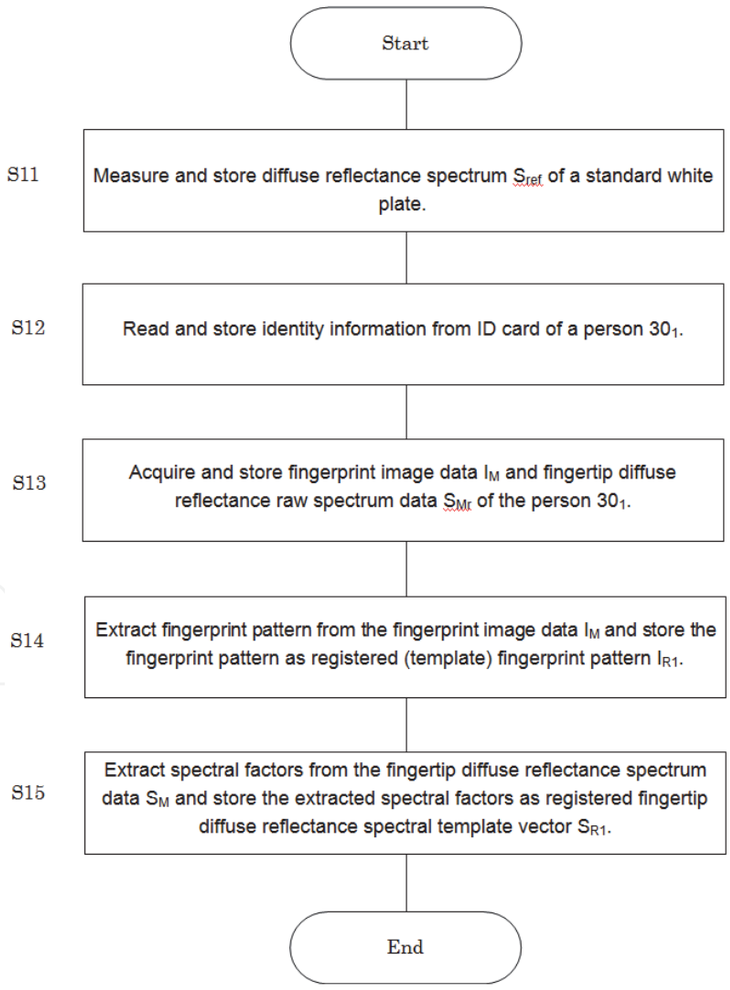
5.1.2 Reflected components and their detection process

Light made incident on the CCD 100 is photoelectrically converted into electrical charges at the respective pixels. In accordance to an instruction signal from a measurement controlling unit 122 of the controller 120, these charges are electronically shifted into a horizontal shift register 104, one row at a time, and thereafter, the contents of the horizontal shift register 104 are shifted, one pixel at a time, into a capacitor 105. The charges in the capacitor 105 are then provided as an analog voltage to an amplifier 106, which performs amplification to an appropriate analog voltage level (e.g., 0 to 10 volts). The amplified voltage output by the amplifier is then converted to a digital value by an analog-to-digital (A/D) converter 107. The digital values output by the A/D converter 107 are then input as data into the memory 130 according to instruction signals from the measurement controlling unit 122 of the controller 120. The digital values obtained by reading the charges from the image acquisition portion 102 of the CCD 100 are thus stored as data in the measured image storage area 132 in accordance to an instruction signal from the controller 120, and the digital values obtained by reading the charges from the spectrum acquisition portion 103 of

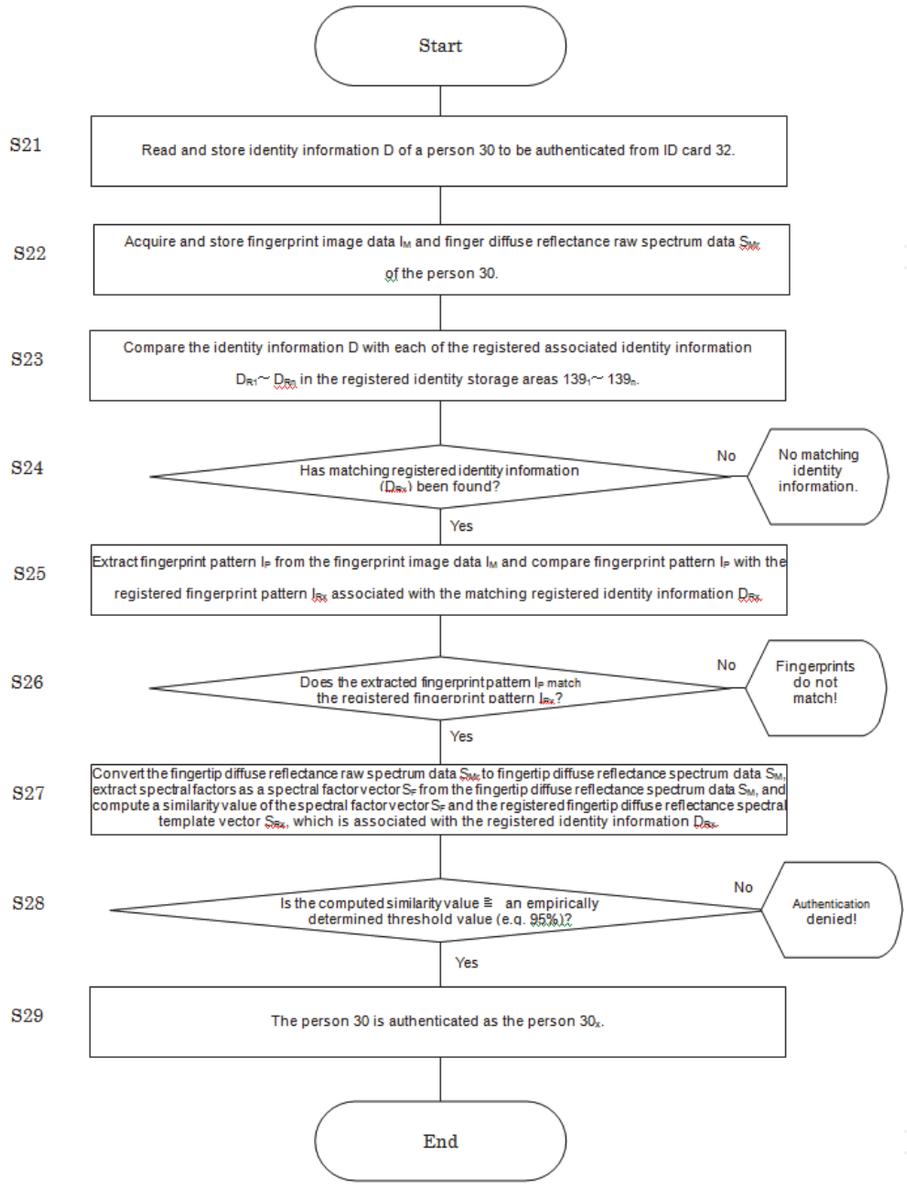
the CCD 100 are binned as data in the measured spectrum storage area 134 in accordance to an instruction signal from the measurement controlling unit 122 of the controller 120.
In this readout process, the data of the boundary pixels (i.e. the pixels of the 32 edge rows at the top and bottom sides, the 32 columns at each of the left and right sides, and the 96 rows between the image acquisition portion 102 and the spectrum acquisition portion 103 of the CCD 100) are ignored as data that may not be reliable in comparison to data of other portions or as data that may be hybrid data of the image and the spectrum.

5.1.3 Authentication process

An authentication process using the fingerprint authentication device 1 shall now be described with reference to the flowcharts of Fig 8. This authentication process is constituted of an enrollment process (Fig. 8a), in which a person's fingerprint image and fingertip diffuse reflectance spectrum are registered along with the person's identity, and a verification process (Fig. 8b), which is performed each time a person needs to be verified.



(Fig 8.a) Flowchart of an enrolment process



(Fig 8.b) Flowchart of a verification process

Fig. 8. A flowchart of an enrolment and a verification process in an authentication process according to an embodiment of this work.

5.1.3.1 Enrollment process

Firstly, in the enrollment process shown in Fig. 8(a), a diffuse reflectance spectrum S_{ref} of a standard white plate (not shown) is set on the upper surface of the sheet prism 20 and its diffuse reflectance spectrum S_{ref} is measured. The spectrum data S_{ref} that are obtained by this measurement and stored in the measured spectrum storage area 134 of the memory 130 are then transferred and re-stored in the reference spectrum storage area 133 of the memory 130 (step S11).

Identity information, such as the name, etc. of the person 30_1, are then read from an ID card 32_1, belonging to the person 30_1, by means of the card reader 150 and stored as registered identity information D_{R1} in the registered identity storage area 139_1 (step S12).
Fingerprint image data I_M and fingertip diffuse reflectance raw spectrum data S_{Mr} of the person 30_1 are then captured and measured as described above and stored in the measured image storage area 132 and the measured spectrum storage area 134, respectively, of the memory 130 (step S13).
The controller 120 then issues an instruction signal to the memory 130 to make the fingerprint image data I_M, stored in the measured image storage area 132, be transmitted to an analyzing unit 123, where a fingerprint pattern is extracted from the fingerprint image data I_M. Methods of extracting a fingerprint pattern from such fingerprint image data are well-known and described, for example, in 'Handbook of Fingerprint Recognition,' (Maltoni et al., 2003), and a detailed description thereof shall not be provided here. The controller 120 then stores the extracted fingerprint pattern, for example, as a registered (template) fingerprint pattern IR_1 in the registered image pattern (template) storage area 136_1 so that this fingerprint pattern is associated with the registered associated identity information D_{R1} in the registered identity storage area 139_1 (step S14).
Next, the controller 120 issues an instruction signal to the memory 130 to make the fingertip diffuse reflectance raw spectrum data S_{Mr}, stored in the measured spectrum storage area 134, and the reference reflectance spectrum data S_{ref}, stored in the reference spectrum storage area 133, be transmitted to the analyzing unit 123. In the analyzing unit 123, the fingertip diffuse reflectance raw spectrum data S_{Mr} are converted to fingertip diffuse reflectance spectrum data S_M by using the values of reference reflectance spectrum data S_{ref} as 100% reflectance. Spectral factors are then extracted from the fingertip diffuse reflectance spectrum data S_M. In the present example, the fingertip diffuse reflectance spectrum data S_M is integrated in the respective ranges of 350 to 400nm, 401 to 470nm, 500 to 560nm, 600 to 660nm, 730 to 790nm, 830 to 900nm, and 925 to 1025nm to obtain seven integration values (Fig. 5). Here, the ranges of 350 to 400nm and 401 to 470nm correspond to peaks due to melanin, the ranges of 500 to 560nm, 600 to 660nm, and 830 to 900nm correspond to peaks due to hemoglobin, the range of 730 to 790nm corresponds to arterial blood, and the range of 925 to 1025nm corresponds to venous blood. The resulting seven values are then stored as a registered fingertip diffuse reflectance spectral template vector S_{R1} in the registered spectral template data storage area 137_1, and this spectral template vector is thereby associated with the registered associated identity information D_{R1} in the registered identity storage area 139_1 (step S15).
This enrollment process is not performed each time a person needs to be authenticated but is performed just once or once every predetermined interval (months, years, etc.). Also, for persons besides the person 30_1, the procedure from step S12 to step S15 of this enrollment process may be performed at any time to register a registered fingerprint image IR and a registered fingertip diffuse reflectance spectrum S_R in association with an associated identity information D_R for each of an arbitrary number n of persons.

5.1.3.2 Verification process

In the verification process (Fig. 8b), first, the identity information of a person 30 to be authenticated are read from an ID card 32, belonging to the person 30, by means of the card reader 150 and stored as identity information D in the identity storage area 138 (step S21).
Fingerprint image data I_M and fingertip diffuse reflectance raw spectrum data S_{Mr} of the person 30 are then captured and measured as described above and stored in the measured

image storage area 132 and the measured spectrum storage area 134, respectively, of the memory 130 (step S22).
The controller 120 then issues an instruction signal to the memory 130 to make the identity information D, stored in the identity storage area 138, be transmitted to the analyzing unit 123. At the analyzing unit 123, the identity information D is compared with each of the registered associated identity information D_{R1} # D_{Rn} in the registered identity storage areas 139_1 # 139_n to find matching registered identity information (step S23, S24). If matching registered identity information is found, step S25 is entered. On the other hand, if matching registered identity information is not found, step S41 is entered, in which a message, such as 'No matching identity information,' is displayed on the monitor 140, and then the process is ended without authentication of the person 30.

5.1.3.3 Process at control and analysis unit

For the present description, it shall be deemed that the identity information D matches the registered associated identity information D_{Rx} of a person 30_x (where x is a value in the range of 1 to n). In this case, upon entering step S25, the controller 120 issues an instruction signal to the memory 130 to make the fingerprint image data I_M, stored in the measured image storage area 132, be transmitted to the analyzing unit 123, where a fingerprint pattern I_P is extracted from the fingerprint image data I_M. At the analyzing unit 123, the extracted fingerprint pattern I_P is compared with the registered fingerprint pattern I_{Rx} in the registered image pattern storage area 136x, which is the fingerprint pattern associated with the registered identity information D_{Rx}, to judge whether the extracted fingerprint pattern I_P matches the registered fingerprint pattern I_{Rx} (step S26). Methods of comparing fingerprint patterns from such fingerprint image data are well-known and described, for example, in the abovementioned 'Handbook of Fingerprint Recognition,' (Maltoni et al., 2003), and a detailed description thereof shall not be provided here.
If by the above analysis of step S26, the extracted fingerprint pattern I_P is found to match the registered fingerprint pattern I_{Rx}, step S27 is entered. On the other hand, if the fingerprint patterns do not match, step S42 is entered, in which a message, such as 'Fingerprints do not match!' is displayed on the monitor 140, and then the process is ended without authentication of the person 30.
For the present description, it shall be deemed that the extracted fingerprint pattern I_P matches the registered fingerprint pattern I_{Rx}. In this case, upon entering step S27, the controller 120 issues an instruction signal to the memory 130 to make the fingertip diffuse reflectance raw spectrum data S_{Mr}, which are of the person 30 and are stored in the measured spectrum storage area 134, and the reference reflectance spectrum data S_{ref}, which are stored in the reference spectrum storage area 133, be transmitted to the analyzing unit 123. In the analyzing unit 123, the fingertip diffuse reflectance raw spectrum data S_{Mr} are converted to fingertip diffuse reflectance spectrum data S_M of the person 30 by using the values of reference reflectance spectrum data S_{ref} as 100% reflectance. Seven spectral factors are then extracted as a spectral factor vector S_F from the fingertip diffuse reflectance spectrum data S_M in the same manner as described above. A similarity value of the spectral factor vector S_F thus acquired and the registered fingertip diffuse reflectance spectral template vector S_{Rx} in the registered spectral template data storage area 137_x, which is associated with the registered identity information D_{Rx}, is then computed by cluster analysis using single linkage Euclidean distance. The computation of the similarity value is performed, for example, using a cluster analysis software, such as Minitab Statistical Software© (made by Minitab Inc., 2009), and using a seven-valued vector R_0, having zero

entries for all seven spectral factors, as a dissimilarity reference vector corresponding to a similarity value of 39.11%. Because the computation of the similarity value by cluster analysis using single linkage Euclidean distance is a well-known art (see for example, Ragnemalm, PhD Thesis 1993), a detailed description thereof shall be omitted here.
The computed similarity value is then compared with, for example, an empirically determined threshold value of 95% (S28). If the computed similarity value is greater than or equal to this threshold value, the process ends upon authentication of person 30 as the person 30_x (step S29). On the other hand, if the computed similarity value is less than the threshold value, step S44 is entered, in which a message, such as 'Authentication denied!' is displayed on the monitor 140 and then the process is ended without authentication of the person 30.

5.1.4 Reliability of the approach

As can be understood from the above description of the embodiment, with the present approach, because a non-spectrometric biometric signature (fingerprint image) of a biometric signature source (fingertip) is augmented by spectral information of the biometric signature source (diffuse reflectance spectrum of the fingertip) in a manner such that the non-spectrometric biometric signature (fingerprint image) is used to ensure the unique identity of the object (person) to be authenticated and the spectral information (diffuse reflectance spectrum) is used to ensure that the non-spectrometric biometric signature (fingerprint image) is a genuine signature of the predetermined class of objects (living human beings with fingerprint diffuse spectral characteristics within a predetermined similarity range of predetermined characteristics), spoofing, for example, that uses a non-spectrometric biometric signature (fingerprint image) formed on an object (e.g. copy medium, plastic finger, etc.) not belonging to the predetermined class of objects (living human beings with fingerprint diffuse spectral characteristics within a predetermined similarity range) can be prevented. That is, the spectral information of an object reflects the optical complexity of that object, and the more complex an object is, the more complex the spectral information. In particular, skin or other portion of a living human is a complex biological structure made of different layers with distinct morphologies and optical properties. Thus for example, a diffuse reflectance spectrum obtained from a fingertip includes spectral components of such substances as melanin, hemoglobin, and other constituents of skin, muscle, blood, etc., with which the proportions present, etc. differ among individual persons (see, for example, Fig. 3b). The spectral information obtained from a fingertip or other portion of a living human is thus extremely complex and cannot be replicated readily by the use of artificial dummies and prosthetic devices, and especially because in this approach, the non-spectrometric biometric signature of the same portion is acquired for identification, spoofing is made a practically insurmountable task.

5.2 Preferred configuration for iris authentication system

To illustrate a further scope of application of this approach, a second embodiment according to this approach shall now be described. Fig. 9 is a schematic diagram of a basic arrangement of a spectral biometrics enhanced authentication system according to the second embodiment of this approach, which is an iris authentication device 200 that authenticates a person's identity based on his/her iris pattern and biospectral characteristics of his/her iris.

5.2.1 Incident light and its reflected components

As shown in Fig. 9, this iris authentication device 200 uses the same CCD 100, having the image acquisition portion 102 and the spectrum acquisition portion 103, as that used in the

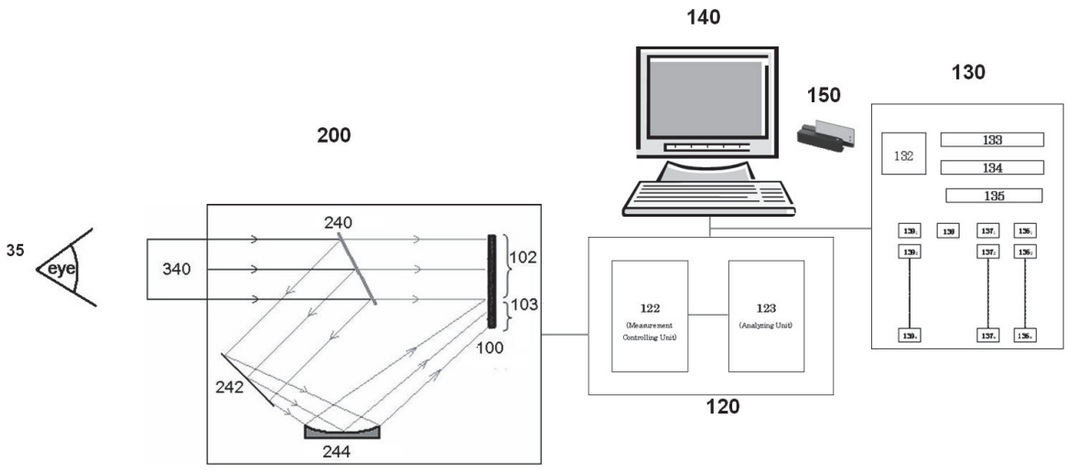


Fig. 9. A schematic diagram of a basic arrangement of a spectral biometrics enhanced authentication system according to a second embodiment of this work.

first embodiment. With this authentication device 200, an image of an iris 35 of a person 30 to be authenticated is formed on the image acquisition portion 102 by a lens 340. A portion (10% to 20%) of the light propagating from the iris 35 to the CCD 100 is reflected by a half-mirror 240 and then reflected by a mirror 242 onto a diffraction grating 244, which spectrally disperses and makes the component, reflected by the half-mirror 240, incident on the spectrum acquisition portion 103 of the CCD 100 in a manner such that a reflection spectrum of the iris within a range of 350nm to 1050nm can be acquired from each row of the spectrum acquisition portion 103.

5.2.2 Data acquisition and authentication process

The iris image, acquired by the image acquisition portion 102 of the CCD 100, and the iris reflection spectrum, acquired by the spectrum acquisition portion 103, are then handled in the same manner as the fingerprint image and fingertip diffuse reflectance spectrum, respectively, of the first embodiment to obtain an iris pattern and an iris spectral information vector, which are then handled in the same manner as the fingerprint image pattern and the fingertip spectral information vector of the first embodiment to perform the authentication process.

5.2.3 Reliability of the approach

As with the fingertip diffuse reflectance spectrum, the iris reflection spectrum contains information on internal tissue, blood, and other various physiological components of the eye (iris) and thus provides information concerning a person's unique biological spectral signature that cannot be spoofed readily.

5.3 More general system configuration approach

The present approach is not limited to the embodiments described above, and various modifications can be made within the scope of the approach. For example, although the CCD 100, having pixels arranged in 1280 rows and 1024 columns, was used as the image sensor in the embodiment described above, a CCD of any other size may be used or a CMOS device may be used instead as the image sensor. Also together with a CCD, CMOS sensor, or other image sensor; a PDA (photodiode array) or a sensor having just the same number of

photodetecting elements as the number of spectral information to be determined (seven in the case of the above-described embodiments) may be configured to perform image acquisition and spectrum acquisition, respectively. Other variations such as employment of different light source (e.g., D2 lamp, laser, etc.) for acquisition, use of a more flexible ID reading mechanism for database access, or use of different biometrics signature (e.g., hand geometry, facial features, retinal print, etc.) may also be employed instead. Furthermore, during the analysis process a different wavelength range, wavelength number, or even a different pattern recognition method; such as neural networks, fuzzy logic, or linear programming may be employed instead.

6. Conclusion

This chapter 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.

7. References

Anderson, R., Hu, J. & Parrish, J. (1981). Optical radiation transfer in the human skin and applications in vivo remittance spectroscopy. In: *Bioengineering and the Skin, MTP Press Limited*, pp. 253-265.

Bailey, E. (2008). Europe Lead the Way with Biometric Passports, But Highest Growth Potential is in Asia, In: *Report Buyer*, Date of access: 2011, Available from: <http://www.sbwire.com/press-releases/new-report-predicts-that-global-biometrics-market-will-reach-71-billion-by-2012-18766.htm>

Brownlee, K., (2001). Method and apparatus for distinguishing a human finger from a reproduction of a fingerprint, In: *US Patent 6,292,576*, Digital Persona Inc.

Derakshani, R., Schuckers, S., Hornak, L. & Gorman, L. (2003). Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners, In: *Pattern Recognition*.

Fukuzumi, S. (2001). Organism identifying method and device, In: *US patent 6,314,195*.

Ingemar R. (1993). The Euclidean distance transform, In: *PhD Thesis, Linköping University, E.E.Dept., Dissertation #304*, Linköping studies in science and technology.

Jenkins, F. & White, H. (1976). Fundamentals of Optics, Macmillan, New York.

Lapsley, P., Lee, J. & Pare, D. (1998). SmartTouch LLC Anti-fraud biometric scanner that accurately detects blood flow, In: *US Patent 5,737,439*.

Maltoni, D., Jain, A. & Prabhakar, S. (2005). Handbook of Fingerprint Recognition, Springer, 1st ed.

Maltoni, D., Maio, D., Jain, A. & Prabhakar, S. (2003). Handbook of Fingerprint Recognition. Springer Verlag, New York, NY, USA.

Matsumoto, T., Hirabayashi, M. & Sato, S. (2004). A Vulnerability of Irsi Matching (Part 3), In: *Proceedings of the 2004 Symposium on Cryptography and Information Security*, the Institute of Electronics, Information and Communication Engineers, pp. 701-706.

Matsumoto, T., Matsumoto, H., Yamada, K. & Hoshino, S. (2002). Impacts of Artificial 'Gummy' Fingers on Fingerprint System, In: *Optical Society and Counterfeit Deterrence Techniques IV,* Proceedings of SPIE, 4677, pp. 275-289.

McFedries, P. (2007). Biometrics, In: *The Word Spy*, Date of access: 2011, Available from: <http://www.wordspy.com/words/biometrics.asp>

Melanoma, (2006). Skin Reflectance Spectra, In: *Melanoma*, Date of access: 2011, Available from: <http://melanoma.blogsome.com/2006/03/24/skin-reflectance-spectra>

MINITAB Inc., (n.d.). In: *Minitab Statistical Software*, Date of access: 2007, Available from: <www.minitab.com/contacts>

O'Gorman, L. & Schuckers, S. (2001). Spoof detection for biometric sensing systems, In: *WO 01/24700*, Veridicom, Inc.

Ohtsuki T. & Healey, G. (1998). Using color and geometric models for extracting facial features, In: *Journal of Imaging Science and Technology*, 42(6), pp. 554-561.

Osten, D., Carim H., Arneson, M. & Blan, B. (1998). Biometric, personal authentication system, In: *US Patent 5,719,950*, Minnesota Mining and Manufacturing Company.

Pishva, D. (2007). Multi-factor Authentication Using Spectral Biometrics, In: *Journal of Japan Society for Fuzzy Theory and Intelligent Informatics - Special Issue on Security and Trust*, Vol.19, No.3, pp. 256-263.

Pishva, D. (2007). Spectroscopic Approach for a Liveness Detection in Biometrics Authentication, In: *41st Annual IEEE International Carnahan Conferences on Security Technology*, pp.133-137.

Pishva, D. (2008). Spectroscopic Method and System for Multi-factor Biometric Authentication, In: *International Patent Application Number PCT/JP2007/060168, International Publication No: WO/2008/139631 A1.*

Pishva, D. (2008). Spectroscopically Enhanced Method and System for Multi-factor Biometric Authentication, In: *IEICE Trans. Inf. & Syst.*, Vol. E91-D, No. 5, pp. 1369-1379.

Pishva D. (2010). Spectroscopic Method and System for Multi-factor Biometric Authentication, In: *International Patent Application Number PCT/JP2007/060168, Australian Patent Number: 2007352940*.

Rowe, R., Corcoran, S., Nixon, K. (n.d.). Biometric Identity Determination using Skin Spectroscopy, In: *Lumidigm, Inc.*, Date of access: 2007, Available from: <www.lumidigm.com>

Shafer, S. (1985). Using color to separate reflection components, In: *Color Research and Application*, Vol. 10, no. 4, pp. 210-218.

Tilton, C. (2006). Biometric Standards – An Overview, In: *Daon*, Date of access: 2007, Available from: <http://www.daon.com/downloads/standards/Biometric%20Standards%20White%20Paper%20Jan%2006.pdf>

UK Biometric Working Group Annual Report for 2003/2004, (2003, 2004). Date of access: 2011, Available from: <http://www.cesg.gov.uk/policy_technologies/biometrics/media/annual_report_03-04.pdf>

van der Putte, T. & Keuning, J. (2000). 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*, Kluwer Academic Publishers, pp. 289-303.

Wikipedia, the free encyclopaedia (n.d.). Euclidean distance, In: *Wikipedia,* Date of access: 2011, Available from: <http://en.wikipedia.org/wiki/Euclidean_distance>

Wikipedia, the free encyclopaedia (n.d.). Spectroscopy, In: *Wikipedia,* Date of access: 2011, Available from: <http://en.wikipedia.org/wiki/Spectroscopy>

Wildes, R., Asmuth, J., Green, G., Hsu, S., Kolczynski, R., Matey, J. & McBride, S. (1996). A machine vision system for iris recognition, In: *Machine Vision and Application*, Vol. 9, pp. 1-8.

Advanced Biometric Technologies

Edited by Dr. Girija Chetty

ISBN 978-953-307-487-0
Hard cover, 382 pages
Publisher InTech
Published online 09, August, 2011
Published in print edition August, 2011

The methods for human identity authentication based on biometrics â€“ the physiological and behavioural characteristics of a person have been evolving continuously and seen significant improvement in performance and robustness over the last few years. However, most of the systems reported perform well in controlled operating scenarios, and their performance deteriorates significantly under real world operating conditions, and far from satisfactory in terms of robustness and accuracy, vulnerability to fraud and forgery, and use of acceptable and appropriate authentication protocols. To address some challenges, and the requirements of new and emerging applications, and for seamless diffusion of biometrics in society, there is a need for development of novel paradigms and protocols, and improved algorithms and authentication techniques. This book volume on â€œAdvanced Biometric Technologiesâ€ is dedicated to the work being pursued by researchers around the world in this area, and includes some of the recent findings and their applications to address the challenges and emerging requirements for biometric based identity authentication systems. The book consists of 18 Chapters and is divided into four sections namely novel approaches, advanced algorithms, emerging applications and the multimodal fusion. The book was reviewed by editors Dr. Girija Chetty and Dr. Jucheng Yang We deeply appreciate the efforts of our guest editors: Dr. Norman Poh, Dr. Loris Nanni, Dr. Jianjiang Feng, Dr. Dongsun Park and Dr. Sook Yoon, as well as a number of anonymous reviewers.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Davar Pishva (2011). Use of Spectral Biometrics for Aliveness Detection, Advanced Biometric Technologies, Dr. Girija Chetty (Ed.), ISBN: 978-953-307-487-0, InTech, Available from: http://www.intechopen.com/books/advanced-biometric-technologies/use-of-spectral-biometrics-for-aliveness-detection

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen

IntechOpen