Analysis of Palm Vein Biometric System

Kenneth Wong, Thomson Lai
Bosco Lee, Frankie Shum

Abstract – **The purpose of a biometric security system is to enclose a secret into a biometric template in a way that can only be decrypted with a biometric image provided by the enrolled person. Despite the advantages of biometric authentication systems, they are vulnerable to attacks that can decrease their security significantly. This paper discusses the implementation, operation and application of a palm vein biometric system. This document highlights the strengths and weaknesses of the palm vein biometric system, and results an evaluation of the system security and the comparison with other biometric systems. Once the potential vulnerability is known, improving of the system security is necessary. At the end of this paper, suggestions for improving the overall security of the palm vein biometric system are presented.**

Index Terms – **Palm-vein Biometric System, far-infrared, near-infrared**

I. Introduction

Computer security has become a crucial part of our daily living. With the broad concern about confidentiality and authenticity, there is a demand in security advancement. Biometrics has become a popular technology that takes advantages of human's physiological features, in order to verify one's identity and allow access of privileged resources. In the past, biometrics has been widely used through different media – facial features, fingerprints, hand geometry, iris scan etc. Palm vein is a more recent advancement in biometric security systems. Like other systems, palm vein pattern security system can allow calibration errors (e.g. ambient body temperature); however, it presents certain unique features that are not seen in the past technology.

II. Description

Palm vein biometric systems operate differently from other biometric systems such as fingerprint and iris scan systems. These traditional systems compare external physical features of the scanned area; however, as the name suggests, the palm vein system takes the digitalized image of the user's veins and compares it with the templates stored in the system. One important point about palm veins is that throughout the lifetime of individuals, their vein pattern will not change significantly unless the individuals are still in their growth period. Another point to consider is the uniqueness of the pattern. As [1] stated, the pattern of blood veins is unique to every individual, even among identical twins.

A. Implementation

There are two types of palm vein scanning technologies. These two types, known as far infrared and near infrared, were analyzed in [2]. Most systems use the near infrared implementation to avoid several problems with far infrared. The first problem with far infrared technology is the image contrast. From experiments in [2], the vein and its surrounding area have similar temperatures which cause the contrast in the image to be similar. As a result, it is difficult to extract the vein pattern for comparison [2]. The contrast problem leads to another disadvantage of far infrared which is limited details. The images can only display the major veins in the palm which, as stated by [2], is too little information for high security applications. On the other hand, near infrared technology enables the captured image to display the smaller veins properly. This method works by having the deoxidized hemoglobin in the vein vessels absorb the infrared rays, thereby reducing the reflection rate and causing the veins to appear as a black pattern [1]. If the deoxidized hemoglobin stops flowing through the vein, then the pattern will not appear, thus allowing the detection of liveliness in the user. The ray used during the process is not dangerous; it is the same as being exposed to sunlight [1].

B. Operation

The palm vein system does not require the user to have direct contact with the system throughout the entire process. The user simply needs to put their hand over the scanner and the system will complete the scanning and matching instantly. Depending on how the system is set up, the image taken can be matched with either the provided by a user's IC card. Figure 1, taken from [3] shows a typical process of palm vein biometric.

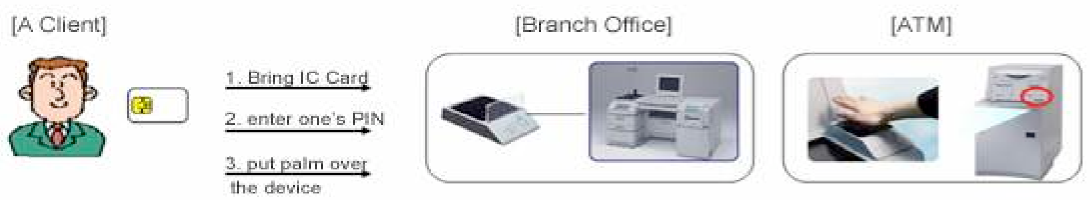

Figure 1 – Palm Vein Scanner Process [3]

C. Applications

Palm vein biometrics can be used for identification and authorization. Several applications for the palm vein biometric are suggested by [1] including the following: login control, security system, and banking services. Fujitsu has already implemented this type of biometric system in Japan's ATM machines which allows the users to identify themselves by comparing their palm vein pattern with the template stored in the user's IC card [3]. Another system offered by Fujitsu is the USB powered model which is responsible for authentication at workstations.

III. Strengths and Weaknesses of Palm Vein Biometric

Every biometric identification method has its strengths and weaknesses. Using the Far-Infrared, Palm Vein Biometric System directly recognizes the geometric shapes of the vein patterns [2]. Although it is impossible to capture the complete vascular network of a palm, the information contained possessed by the superficial vein pattern is sufficient to perform personal verification tasks for a reasonable sized user group [5].

A. Strengths

Palm vein biometric system consists of several benefits over other biometric systems. One such characteristic is that each person's vascular patterns are unique that provide large, robust, stable and hidden biometric features. The pattern of blood vessels is hard-wired into the body at birth and remains relatively unaffected by aging except for predictable growth as with fingerprints [6]. Due to the blood vessels hidden within the body, it is difficult for intruders to forge a person's vascular patterns. In addition, dryness or roughness on the surface of the skin has no effect on the accuracy of vein pattern identification and authentication. A test has been conducted in Japan with more than 70,000 individuals. The result is that palm vein biometric system has a false rejection rate (FRR) of 0.01% and a false acceptance rate (FAR) of less than 0.00008% [#]. Vein patterns are not easily observed, damaged, obscured or changed; the vein patterns require only low resolution infrared imaging allied to simple image processing. Finally, vein structures provide the opportunity for low cost personal pocket biometric keys.

B. Weaknesses

The only weaknesses of the palm vein biometric system are the different factors that affect the quality of the captured image. Such factors include: body temperature, ambient temperature and humidity, unevenly distribution of heat, heat radiation, nearness of the vein to the surface, and camera calibration and focus. Most of these factors are natural cause which is difficult to overcome.

C. Comparison

As mentioned earlier, palm vein biometric yields a better performance than traditional system. This section discusses some of the advantages of the palm vein biometric systems with respect to other biometric systems available in the market. Since palm vein biometrics takes the image of what is inside of the palm, any physical injuries to the hand surface will not affect the outcome of the process. Also, others that wish to copy the pattern will find it more difficult because it is not an external physical feature [1]. Unlike fingerprint and iris scanners, palm vein biometric systems do not require physical contact between the user and the system. This enables better public acceptance because in public areas, some might not like the thought of touching what others have touched for sanitary reasons [5].

IV. Security Evaluation of Palm Vein Biometric System

In a typical biometric system, there are several common methods of attacking the system. Figure 1 shows eight of these points of attack. At point 1, spoofing attacks are possible where an attacker presents the sensor with a fake biometric in an attempt to fool the system. Points 2, 4, 7, and 8 are susceptible to different types of replay and transmission based attacks. Modified code at points 3 and 5 may allow an attacker to bypass the security mechanisms of the system. At point 6, an attacker might add his or her own template to the set of templates or modify existing templates.

A. Spoofing attacks

The palm vein biometric system has a number of traits which make it more resistant to spoofing attacks. One of these traits is that veins are an internal feature of the body. This makes it much more difficult for a subject to leave his or her biometric data in places unknowingly. Fingerprints can be gathered from an object that has been touched, physical features can be caught on video tape, and voice can be recorded. Veins, however, reside within the body and do not transfer on touch.

Furthermore, palm vein recognition methods have an increased ability to detect liveliness in the subjects. It is claimed that only flowing blood will be detected by the infrared imaging component.

B. Replay and Transmission Attacks

Preliminary analysis done in [7] indicates that the signal between the sensors and the computer was able to be intercepted and raw data extracted. Potentially, an attacker could obtain an authentic user's biometric image and at a later time transmit this data to the system posing as that user. Further testing has not been taken on the Palm Vein system to determine whether this attack is feasible on this system.

Hill-Climbing attacks are a type of attack where the attacker continuously generates sets of features which are fed to the matching system. The next set of features that are generated depends on the resulting matching score of the previous attempt. Features which provide increasing scores are used for the next attempt while decreasing scores are discarded. Eventually a score which exceeds the required score to authenticate will be reached and the attacker will have succeeded. In [8], the authors were able to break 160 accounts of a fingerprint system with an average of 195 attempts per account. The Fujitsu PalmSecure system, however, does not return a matching score for each attempt. Instead, PalmSecure returns a result of matched or not matched. This prevents attackers from performing hill-climbing attacks on the PalmSecure system.

V. Known Methods of Improving Security of Biometric Systems

A. Multimodal Biometric Systems

Multimodal biometric systems are biometric systems that utilize multiple independent biometrics in order to identify or verify the user. By requiring the user to provide multiple biometrics, the difficulty of attacking the system increases. This is an example of the Defense in Depth principle of secure design. Hand biometrics is a good area to explore multimodal biometric systems. Many different biometric technologies exist for the hand already, including: fingerprints, palmprints, hand geometry, and hand vein. Combining all these into an all-in-one system may be costly, however the security benefits are obvious and the invasiveness of the system is not greatly affected.

B. Biometrics Combined with Passwords

Another proposed method of increasing security is to change the way biometric authentication is used. Rather than using biometric data as a login and password, have the biometric data provide the login information and the user must input their password afterwards to access the system. This method, however, requires that the user remember their password. This may seem inconvenient to some people who wish that biometrics be used to authenticate without the need to carry additional items or passwords.

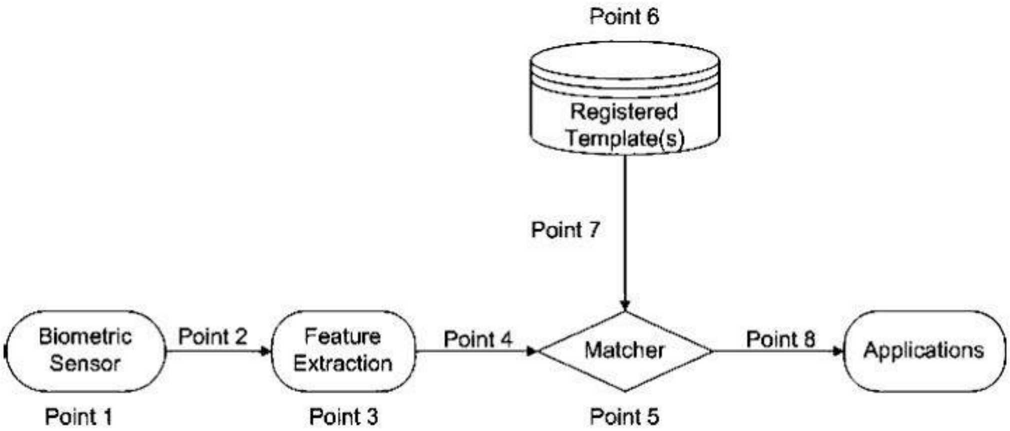

Figure 2 – Points of Attack in a Biometric System

C. Watermarking

Watermarking is a technique that can be used to help prevent replay attacks. With watermarking techniques, biometric data can be time-stamped [9], preventing the data from being reused at a later date. Another idea proposed in [10] is to hide the biometric data in another signal, such as an image. In the case of a multimodal biometric system, the biometric data can be hidden in other biometric data.

VI. Conclusion

Palm vein system has presented a new face to biometric security system. It has a very low FAR and FRR, and is considered more hygienic than other biometric systems. Nevertheless, it is not without weaknesses. To increase the difficulty of system attack, multimodal biometric systems can be employed. By combining different biometric systems, such as palm vein with fingerprints and hand geometry, the risk of system attack will be significantly reduced. Moreover, biometric system can combine with a password in order to strengthen the authentication process, and watermarking can be employed to further protect the resources from attack.

References

[1] "Palm vein biometric systems," Biometric Newsportal, 2006. Available: http://www.biometricnewsportal.com/palm_biometrics.asp. [Accessed on Oct 30, 2007]

[2] L. Wang and G. Leedham, "Near- and far- infrared imaging for vein pattern biometrics," in *AVSS '06. IEEE Int. Conf. Video and Signal Based Surveillance,* pp. 52-52.

[3] "Palm Vein Pattern Biometrics Authentication System," Fujitsu, 2007. Available: http://www.fujitsu.com/global/casestudies/WWW2_casestudy_BTM.html. [Accessed on Oct 19, 2007]

[4] "Fujitsu Palm Vein Technology," Fujitsu, May 2005. Available: http://www.fujitsu.com/global/about/rd/200506palm-vein.html. [Accessed on Oct 30, 2007]

[5] C.L. Lin and K.C. Fan, "The use of thermal images of palm-dorsa vein-patterns for biometric verification," in *Proc. 17th Int. Conf. Pattern Recognition,* 2004, vol. 4, pp. 450-453.

[6] A. K. Jain, R. Bolle and S. Pankanti, *Biometrics Personal Identification in Networked Society*, Kluwer Academic Publishers, Massachusetts, 1999.

[7] R. Sanchez-Reillo, B. Fernandez-Saavedra, J. Liu-Jimenez, C. Sanchez-Avila, “Vascular Biometric Systems and their Security Evaluations,” in *2007 41st Annu. IEEE Int. Carnahan Conf. Security Technology*, pp 44-51.

[8] A.K. Jain and U. Uludag, “Fingerprint Minutiae Attack System,” presented at *The Biometric Consortium Conference,* Arlington, VA, 2004.

[9] M. Faundez-Zanuy, “On the Vulnerability of Biometric Security Systems,” *IEEE Aerosp. Electron. Syst. Mag.*, vol. 19, no. 6, pp 3-8, June 2004.

[10] A.K. Jain and U. Uludag, “Hiding Biometric Data,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, pp. 1494-1498, Nov. 2003.