Image Histogram: Preliminary Findings of Anti-Spoofing Mechanism for Hand Biometrics Acquisition

Zarina Mohd Noh[1, 2], Abdul Rahman Ramli[2], Ridza Azri Ramlee[1] and Syafeeza Ahmad Radzi[1]
[1]*Fakulti Kejuruteraan Elektronik dan Kejuruteraan Komputer, Universiti Teknikal Malaysia Melaka (UTeM),*
Hang Tuah Jaya, 75450 Durian Tunggal, Melaka, Malaysia.
[2]*Department of Computer and Communication Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia,*
43400 UPM Serdang, Selangor, Malaysia.
zarina.noh@utem.edu.my

***Abstract*—Biometrics data are prone to spoofing activities especially on its sensor levels where fake biometrics data can be generated to imitate genuine biometrics data. Fake biometrics are false biometrics data that resemble genuine biometrics characteristics. If fake biometrics is accepted by a biometrics system, the possibility of personal information and data to be stolen is high. The consequences lie in the unwanted access, and the public may become insecure to use biometrics as an authentication tool. Biometrics acquisition process with an added detection mechanism can help distinguish between genuine and fake biometrics data. It is possible by the use of near-infrared (NIR) light during acquisition process because the interaction between NIR light with human skin and fake biometrics are different; due to the living trait property possessed by a human. This paper shares preliminary findings of image histogram for both genuine and fake biometrics images acquired by NIR illumination. Observation on the image histogram reveals that there are differences to the image properties that can be used to distinguish the genuine and fake biometrics data. The approach can be extended to its usage as a detection mechanism for other biometrics data as well. The main principle lies in the difference of image response between genuine and fake biometrics data acquired by the NIR illumination.**

***Index Terms*—Anti-spoofing; Hand Biometrics; Image Acquisition; Near-Infrared Illumination.**

I. INTRODUCTION

Research had been done with regard to identification and recognition system using biometrics data such as the face, fingerprint, iris, gait, vein and signature [1]. In parallel to its development and applicability, biometrics data is also exposed to the possibility of being hacked by the use of fake biometrics supplied during its acquisition time [2]. Fake biometrics is false biometrics data that resembles genuine biometrics data. The fake biometrics data, if accepted as genuine data supplied to a biometrics authentication system may result in unwanted access to private and confidential information. This type of illegal access may bring unknown severe consequences to the individual or institutions related. An added security element needs to be added to curb this kind of biometrics spoofing activity.

Current research in the area had been focusing on multi-biometrics [3]–[5] in identifying a person to increase the biometrics system security. In multi-biometrics, several biometrics modalities are combined to obtain the recognition score in identifying a person. While multi-biometrics has its own merit in providing an added safety feature in protecting an identity, it uses additional sensors in acquiring different types of biometrics modality for recognition purpose. Other methods in increasing biometrics system security are through manipulation at the program level (software) by extracting additional features in the biometrics data for recognition purpose [6]. Still, if a fake biometrics data had been accepted during its acquisition time, the possibility of illegal access is there if it can by-pass the acquisition process. This is because the processing involved in biometrics recognition process depends on related features extracted by the biometric system for identity verification. Once an image had been recorded (regardless of whether it is genuine or fake biometrics), further processing such as detection of biometrics features, image statistics information and extraction of features can be executed on the recorded image. With that, there is a chance for fake biometrics to achieve authentication score needed by the biometrics system.

This paper aims to address an added security element using near-infrared (NIR) illumination during acquisition process in differentiating the genuine and fake biometrics data at the sensor level. The utilisation of NIR illumination is due to the optical response of human skin that allows extra information to be recorded during the imaging process [7]. The extra information can be used as an indicator of a living trait which does not exist in fake biometrics data. The use of NIR illumination as anti-spoofing mechanism in this paper will be going to be demonstrated for hand biometrics data detection.

Organization of this paper starts with the background study on biometrics system and possible spoofing attacks in Section II. Utilization of infrared (IR) illumination in biometrics acquisition system and human skin optical response are also discussed in the same section. Section III presents the preliminary findings on histogram differences between fake and genuine biometrics data. The last section shares future work following the preliminary findings in this paper.

II. BACKGROUND STUDY

The application of biometrics data for personal identification is gaining wide interest from researchers nowadays [8]. This is due to advantages offered by biometrics data compared to conventional methods for authentication or identification purpose. Conventional methods in authentication rely on the availability of some specific tokens such as identification card or keys in accessing a system. In data access purpose, conventional methods use passwords or exclusive information that relies on human memorising capability in recognising an identity. While specific tokens can be stolen or misplaced, the use of information that relies on human memorising capability is not durable for those with memory loss problem. As such, biometrics data is one of the best options for identification purpose as it only relies on the presence of human for identification. With the advancement of technology and communication system nowadays, it is just a matter of time before biometrics data will be coupled with conventional methods (if not used solely) for grant-access system purpose [8].

With the widespread use of biometrics for authentication and grant-access purpose, there is an equal possibility for the data to be vulnerable to attackers too. Although the use of biometrics as identification tool provides an added advantage in terms of data safety, biometrics system is still prone to cyber hackers [8]. Spoofing activities by hackers can be accomplished in two different levels that are in hardware level or software level [3]. These two levels of attacks are as illustrated in Figure 1. In hardware level, attackers can perform illegal access to a system by providing duplicate biometrics data during acquisition process [9]. In software level, access to private information or biometrics database and the program can be done through the intrusion of virus or malicious program in the system [8]. These spoofing activities may result in unwanted access and illegal use of personal data and information. If the hacking activities involving access to confidential data owned by a company or important institutions in a country, the consequences might be severe to the country's economy, growth and public alike.

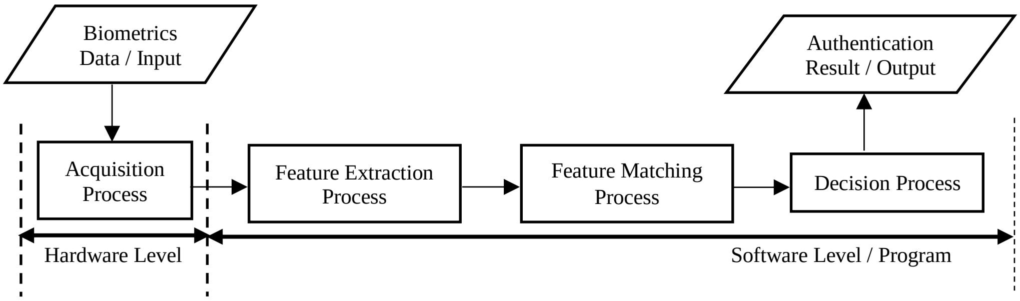


Figure 1: Two levels of possible attacks in biometric authentication.

With respect to the two levels of spoofing activities illustrated in Figure 1, several methods had been done in increasing the security level of biometrics system. One of the methods includes additional analysis and image quality assessments check in biometrics program to detect possible spoofing activity at the hardware level [10]. This method involves vast computation as more than 20 image quality measurements are assessed in detecting possible spoofing activity. Other methods include multi-biometrics acquisition to increase the biometrics system accuracy [3]–[5]. As multi-biometrics comprises of acquisition for many types of biometrics data, integration of this method for practical biometrics design can be questioned for user convenience. In some approaches, additional biometrics features extraction was done for data recognition purpose [6]. As the processing for this approach is computationally heavy, there is a possibility that it will produce low recognition rate due to the strictly defined features for extraction. Other interesting approach focuses on biometrics software or program by setting up some specification in choosing the biometrics decision threshold [11]. In this approach, the biometric decision threshold is specified by taking into account the possible distribution score of fake biometrics data presented during the acquisition process. While the approach seems promising in increasing biometrics recognition accuracy, the decision threshold is directly tied to the type of fake biometrics data used in the training. Furthermore, in all of the mentioned methods and approaches, if fake biometrics had been accepted during its acquisition time, the possibility of illegal access is there if it can get through the recognition process.

Focusing on biometrics as a whole, the main characteristic of the data is the living trait property. The living trait is not present on fake biometrics if it is a product-based imitation of genuine biometrics data. In order to detect the living trait, one of the methods is to prove that there exists blood flow in the subject, indicating heart rates or blood-pumping activity. Although heart rate may not be measured without special equipment and direct contact (i.e. touch) with the human body, vein pattern indicating blood flow in human can be recorded with the help of additional illuminators without the need of direct contact (i.e. touch). Two of illumination sources that can be used for vein imaging are far infrared (FIR) and near-infrared (NIR) light spectrum [12]. The respective wavelengths for the two illumination sources in the electromagnetic light spectrum are as presented in Figure 2. FIR light spectrum manipulates temperature properties of a subject in imaging the vein pattern information [13]. As such, it is prone to be affected by changes in its surrounding temperature. On the other hand, NIR light manipulates the optical reaction of human skin in projecting the vein pattern information in an image [14]. It had been employed in biometrics research for imaging vein pattern in the hand area [12]. However, research on revealing its use as anti-spoofing mechanism is limited and perhaps the closest one is its utilisation as fingerprint anti-spoofing mechanism [15].

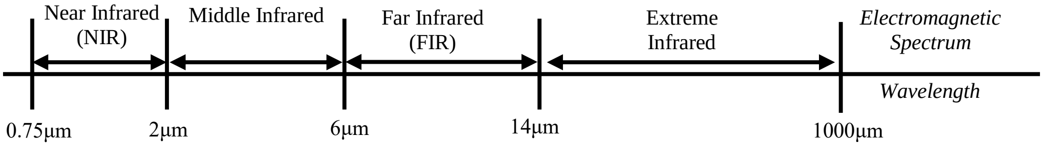


Figure 2: Electromagnetic light spectrum indicating infrared spectrum and its respective wavelength [12].

Although there are varieties of biometrics data, the hand is considered the most accessible part of human body and publicly acceptable area for general use. Besides, hand comprises several data that can be used for biometrics as illustrated in Figure 3. In parallel with the development of biometrics authentication research in the area, research in detecting spoofing activities for hand biometrics are equally expected and necessary. Provided that the image analysis can directly distinguish the difference between genuine and fake biometrics data acquired by the NIR illumination, it is expected that a new dimension to anti-spoofing mechanism can be ventured through the preliminary findings shared in this paper.

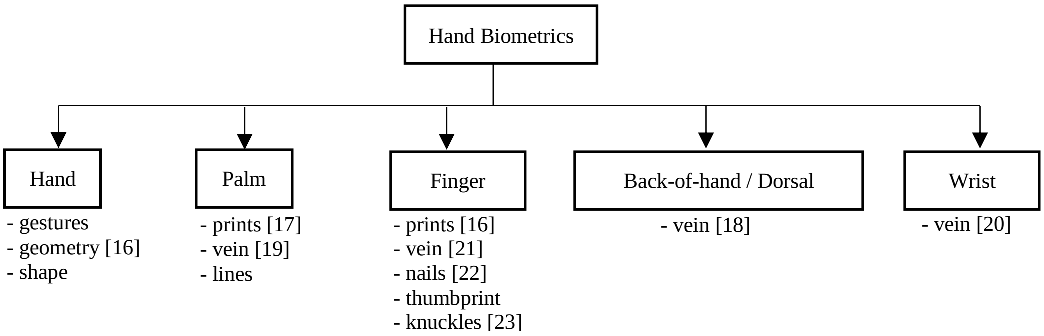


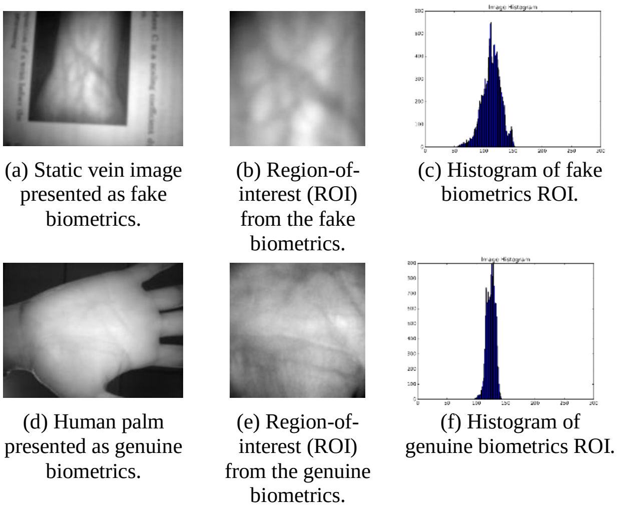
Figure 3: Various biometrics originated from hand.

III. Preliminary Findings: Image Histogram

Differences in properties of images acquired by NIR illumination for both genuine and fake biometrics are as demonstrated in Figures 4-6. Images of both genuine and fake biometrics are acquired independently by three different arrays of LEDs with NIR peak wavelength of 850 nm, 870 nm and the combination of both. The images are captured by NIR-sensitive CMOS camera, connected to a Raspberry Pi single board computer (SBC). Images are processed in Python environment with the help of OpenCV module [24].

In these figures, fake biometrics is generated by a static vein image, while genuine biometrics is represented by human hand. Region-of-interest (ROI) for both biometrics data are also shown in the figures. The ROI is extracted from the acquired image, focusing on areas containing vast vein pattern information. In Figure 4, the biometrics data are acquired by NIR peak wavelength of 850 nm. Through visual interpretation, it can be seen that genuine biometrics data produced sharper and detailed pattern information in the image compared to fake biometrics through their ROIs. Their image histogram is also different, as fake biometrics tend to have a more distributed pixel intensities variation compared to genuine biometrics.

The same observations are also true if the same biometrics are acquired by illumination with different NIR peak wavelengths. In Figure 5, the NIR peak wavelength used as the illuminators is 870 nm, while combinations of 850 nm and 870 nm peak wavelengths are used for acquisition process in Figure 6. With systematic analysis and investigation based on these preliminary findings, properties of these images can be modelled and used as guidelines in detecting fake biometrics data presented during the acquisition process. The main concern is on the optical reaction of human skin concerning NIR illumination and the property possessed by image acquired through the illumination.



(a) Static vein image presented as fake biometrics.

(b) Region-of-interest (ROI) from the fake biometrics.

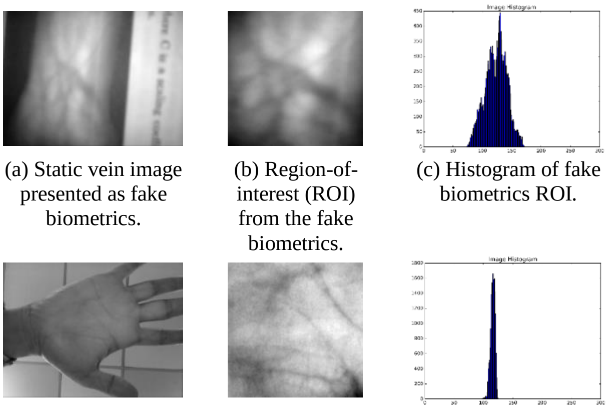
(c) Histogram of fake biometrics ROI.

(d) Human palm presented as genuine biometrics.

(e) Region-of-interest (ROI) from the genuine biometrics.

(f) Histogram of genuine biometrics ROI.

Figure 4: Biometrics data captured by the influence of NIR illumination with a peak wavelength of 850 nm during the acquisition process.



(a) Static vein image presented as fake biometrics.

(b) Region-of-interest (ROI) from the fake biometrics.

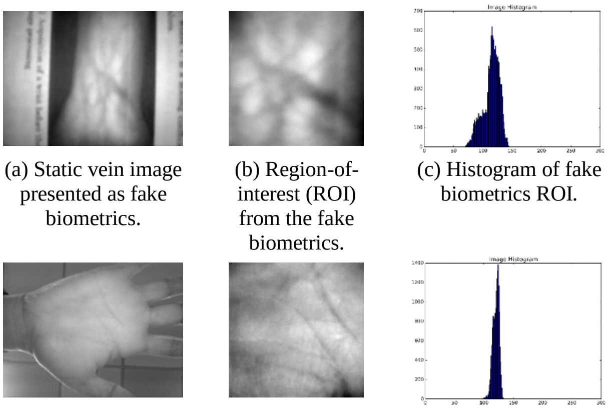
(c) Histogram of fake biometrics ROI.

(d) Human palm presented as genuine biometrics.

(e) Region-of-interest (ROI) from the genuine biometrics.

(f) Histogram of genuine biometrics ROI.

Figure 5: Biometrics data captured by the influence of NIR illumination with a peak wavelength of 870 nm during the acquisition process.



(a) Static vein image presented as fake biometrics.

(b) Region-of-interest (ROI) from the fake biometrics.

(c) Histogram of fake biometrics ROI.

(d) Human palm presented as genuine biometrics.

(e) Region-of-interest (ROI) from the genuine biometrics.

(f) Histogram of genuine biometrics ROI.

Figure 6: Biometrics data captured by the influence of NIR illumination with a combination of the peak wavelength of 850 nm and 870 nm during the acquisition process.

IV. Conclusion

Histograms of hand biometrics data acquired by NIR illumination had been compared in this paper for both genuine and fake biometrics to observe their differences. The differences reflected that images acquired by NIR illumination possessed extra properties that allow them to be differentiated between genuine and fake biometrics data. Regardless of NIR peak wavelengths used during the acquisition process, both genuine and fake biometrics data show a common trend in its respective histogram. In future work, this preliminary findings can be further supported by additional image analysis through a local binary pattern (LBP) and principal component analysis (PCA) techniques. Variation to fake biometrics samples can also be done in future works to investigate the image response of different fake biometrics samples acquired by NIR illumination.

References

[1] J. A. Unar, W. C. Seng, and A. Abbasi, "A Review of Biometric Technology Along with Trends and Prospects," Pattern Recognit., Feb. 2014.

[2] S. Marcel, M. S. Nixon, and S. Z. Li, Eds., Handbook of Biometric Anti-Spoofing. Springer, 2014.

[3] Z. Akhtar, C. Micheloni, and G. L. Foresti, "Biometric Liveness Detection: Challenges and Research Opportunities," IEEE Secur. Priv., vol. 13, no. 5, pp. 63–72, 2015.

[4] S. C. Joshi and A. Kumar, "Design of Multimodal Biometrics System Based on Feature Level Fusion," in 2016 10th International Conference on Intelligent Systems and Control (ISCO), 2016, pp. 1–6.

[5] A. Maheshwari and M. A. Dorairangaswamy, "Multimodal Biometrics Security System for Authentication," in 2016 2nd International Conference on Science Technology Engineering and Management (CONSTEM), 2016, pp. 146–150.

[6] M. Haghighat, M. Abdel-Mottaleb, and W. Alhalabi, "Discriminant Correlation Analysis for Feature Level Fusion With Application to Multimodal Biometrics," in 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2016, pp. 1866–1870.

[7] S. Juric and B. Zalik, "An Innovative Approach to Near-Infrared Spectroscopy Using a Standard Mobile Device and Its Clinical Application in The Real-Time Visualization of Peripheral Veins," BMC Med. Inform. Decis. Mak., vol. 14, no. 100, pp. 1–9, 2014.

[8] A. K. Jain, K. Nandakumar, and A. Ross, "50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities," Pattern Recognit. Lett., vol. 79, pp. 80–105, 2016.

[9] E. Marasco, M. Shehab, and B. Cukic, "A Methodology for Prevention of Biometric Presentation Attacks," IEEE Seventh Latin-American Symp. Dependable Comput., pp. 1–6, 2016.

[10] J. Galbally, S. Marcel, and J. Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition," IEEE Trans. Image Process., vol. 23, no. 2, pp. 710–724, 2014.

[11] I. Chingovska, A. R. Dos Anjos, and S. Marcel, "Biometrics Evaluation Under Spoofing Attacks," IEEE Trans. Inf. Forensics Secur., vol. 9, no. 12, pp. 2264–2276, 2014.

[12] L. Wang, G. Leedham, and S.-Y. Cho, "Infrared Imaging of Hand Vein Patterns for Biometric Purposes," IET Comput. Vis., vol. 1, no. 3, pp. 113–122, Dec. 2007.

[13] M. Moreno-Moreno, J. Fierrez, and J. Ortega-Garcia, "Biometrics Beyond the Visible Spectrum: Imaging Technologies and Applications," Biometric ID Manag. Multimodal Commun., pp. 154–161, 2009.

[14] A. Shahzad, M. N. Saad, N. Walter, A. S. Malik, and F. Meriaudeau, "Hyperspectral Venous Image Quality Assessment for Optimum Illumination Range Selection Based on Skin Tone Characteristics," Biomed. Eng. Online, vol. 13, no. 109, pp. 1–13, 2014.

[15] P. V. Reddy, A. Kumar, S. M. K. Rahman, and T. S. Mundra, "A New Antispoofing Approach for Biometric Devices," IEEE Trans. Biomed. Circuits Syst., vol. 2, no. 4, pp. 328–337, 2008.

[16] T. Duarte, J. P. Pimentao, P. Sousa, and S. Onofre, "Biometric Access Control Systems: A Review Technologies to Improve Their Efficiency," in 2016 IEEE International Power Electronics and Motion Control Conference (PEMC), 2016, pp. 795–800.

[17] B. Bhaskar and S. Veluchamy, "Hand Based Multibiometric Authentication Using Local Feature Extraction," in 2014 International Conference on Recent Trends in Information Technology, 2014, pp. 1–5.

[18] R. Raghavendra, J. Surbiryala, and C. Busch, "Hand Dorsal Vein Recognition: Sensor, Algorithms and Evaluation," in 2015 IEEE International Conference on Imaging Systems and Techniques (IST), 2015, pp. 1–6.

[19] Z. M. Noh, A. R. Ramli, M. I. Saripan, and M. Hanafi, "Overview and Challenges of Palm Vein Biometric System," Int. J. Biom., vol. 8, no. 1, pp. 2–18, 2016.

[20] R. Raghavendra and C. Busch, "A Low Cost Wrist Vein Sensor for Biometric Authentication," in 2016 IEEE International Conference on Imaging Systems and Techniques (IST), 2016, pp. 201–205.

[21] K. Syazana-Itqan, A. R. Syafeeza, N. M. Saad, N. A. Hamid, and W. H. Mohd Saad, "A Review of Finger-Vein Biometrics Identification Approaches," Indian J. Sci. Technol., vol. 9, no. 32, 2016.

[22] A. Kumar, S. Garg, and M. Hanmandlu, "Biometric Authentication Using Finger Nail Plates," Expert Syst. Appl., vol. 41, no. 2, pp. 373–386, 2014.

[23] J. Kim, K. Oh, A. B.-J. Teoh, and K.-A. Toh, "Finger-Knuckle-Print for Identity Verification Based on Difference Images," in Proceedings of the 2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA), 2016, pp. 1073–1077.

[24] OpenCV Development Team, "OpenCV Documentation," 2015. [Online]. Available: http://docs.opencv.org/.