ENHANCED FUZZY VAULT SCHEME ON PALM VEIN BIOMETRIC TEMPLATE PROTECTION USING FAST WALSH HADAMARD TRANSFORMATION

NOOR ALYANIS FARHAIDA BT MOHD ZAINON

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Philosophy

Faculty of Computing
Universiti Teknologi Malaysia

NOVEMBER 2022

DEDICATION

This thesis is specially dedicated to my lovely family for their endless love, support, and encouragement.

ACKNOWLEDGEMENT

In the name of Allah, the most Gracious and the most Merciful.

Alhamdulillah, all praises to Allah for giving me the opportunity to complete this research. I wish to express my sincere appreciation to my main thesis supervisor, Assoc. Prof. Ts. Dr. Shukor Bin Abd Razak, for encouragement, guidance, critics, and friendship. I am also very thankful to my co-supervisor Dr. Arafat Mohammed Rashad Al-Dhaqm for the guidance, advices, and motivation. This thesis would not have been the same if it hadn't been for their continual interest and support.

I would also like to express my deepest appreciation to my lovely family member: my husband, Muhamad Nasiruddin, for offering me unconditional support and motivation through all these years, my parent, Mohd Zainon and Asiah Abdull, my mother and father in law, Umi Kalthum and Mohd Samsi, my sister, Azlina Shazlin and other family members for their constant support and prayers that have given me the strength to keep going. I would also like to especially thank Nurazrin Mohd Esa for her support and help in making my thesis possible.

My sincere appreciation also extends to all my colleagues and others who have provided assistance on various occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space. Thank you, everybody.

ABSTRACT

The widespread use of biometrics as a means of identification continues to rise a security issue for the user. Once a biometric template is compromised, it is considered broken as biometrics cannot be revoked and thus making it obsolete. This is solved by adapting to the biometric template protection scheme. However, not all approaches can meet all the requirements of the biometric template protection scheme. The first requirement is diversity where a biometric template should not link to any other template that is produced from the same original template. Next is revocability where a compromised template should be able to be replaced by a new template generated from the same original biometric template. The third requirement is irreversibility where the transformed template should not revert to the original template and lastly, the fourth requirement is a performance where the performance of the authentication system should not be affected by any methods to secure the biometric template. A fuzzy vault scheme has been widely used in the biometric template protection approach. However, the fuzzy vault scheme only provides irreversibility and performance. Thus, fast Walsh Hadamard Transformation (FWHT) hybridized with fuzzy vault namely FWHT-FV is proposed to equip fuzzy vault scheme with diversity and revocability. The palm vein dataset from Tonji University is used in this study. Then, pre-processing and feature extraction is applied using the Local Binary Pattern (LBP). The result showed that the proposed FWHT-FV achieved 1.25% FAR, 1.75% FRR, and 5.75% EER. The proposed FWHT-FV has improved the accuracy, sensitivity, and specificity by 12.87%, 16%, and 11.75% respectively. Lastly, security analysis showed that the proposed FWHT-FV is able to equip the fuzzy vault scheme with the diversity and revocability properties of the biometric template protection requirements. Hence, the proposed hybrid approach enables the fuzzy vault scheme to meet all the biometric template protection requirements which are diversity, revocability, irreversibility, and performance as well as benefiting the society and industries in the biometric template authentication field.

ABSTRAK

Penggunaan biometrik secara meluas sebagai cara pengenalan terus menimbulkan isu keselamatan bagi pengguna. Sekiranya templat biometrik berjaya diperolehi oleh orang yang tidak bertangugjawab, templat tersebut tidak boleh digunakan lagi. Oleh itu, perkara ini dapat diatasi dengan menepati ciri-ciri yang telah ditetapkan dalam skim perlindungan templat biometrik. Walau bagaimanapun, tidak semua teknik dapat memenuhi kesemua ciri-ciri yang telah ditetapkan oleh skim perlindungan templat biometrik. Ciri yang pertama adalah kepelbagaian dimana templat yang dihasilkan tidak seharusnya berhubung dengan templat lain yang dihasilkan dari templat asal yang sama. Ciri yang seterusnya adalah kebolehbatalan dimana sekiranya berlaku pencerobohan terhadap templat biometrik, ia seharusnya dapat dihapuskan dan diganti dengan templat yang baru dari templat asal yang sama. Seterusnya, templat biometrik perlu memiliki ciri ketakterbalikan dimana templat yang telah ditransformasi tidak boleh kembali ke templat yang asal dan akhir sekali adalah prestasi dimana prestasi sistem pengecaman tidak seharusnya terjejas oleh teknik yang digunakan untuk melindungi templat biometrik tersebut. Skim peti besi kabur telah digunakan secara meluas dalam pendekatan perlindungan templat biometrik. Walau bagaimanapun, skim peti besi kabur hanya menepati ciri ketakterbalikan dan prestasi. Oleh itu, transformasi *Walsh Hadamard* pantas *(FWHT)* telah digabungkan bersama skim peti besi kabur iaitu FWHT-FV untuk melengkapi skim peti besi kabur dengan kepelbagaian dan kebolehbatalan. Set data urat tapak tangan dari Universiti Tonji telah digunakan dalam kajian ini. Kemudian, pra-pemprosesan dan pengekstrakan telah dijalankan menggunakan corak binari tempatan *(LBP).* Keputusan menunjukkan bahawa pendekatan *FWHT-FV* mencapai 1.25% *FAR*, 1.75% *FRR* dan 5.75% *EER*. Pendekatan *FWHT-FV* telah meningkatkan ketepatan, sensitiviti dan kekhususan masing-masing sebanyak 12.87%, 16% dan 11.75%. Akhir sekali, analisis keselamatan menunjukkan bahawa pendekatan FWHT-FV mampu melengkapi skim peti besi kabur dengan ciri-ciri kepelbagaian dan kebolehbatalan. Dengan itu, teknik penggabungan ini telah melengkapi skim peti besi kabur dengan kesemua ciri-ciri yang telah ditetapkan oleh skim perlindungan templat biometrik, iaitu kepelbagaian, kebolehbatalan, ketakterbalikan dan prestasi. Disamping itu, teknik ini juga dapat memberi manfaat kepada masyarakat dan industri dalam bidang perlindungan biometrik.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

FAR	-	False Acceptance Rate
FRR	-	False Rejection Rate
FV	-	Fuzzy Vault
FWHT	-	Fast Walsh Hadamard Transformation
FWHT-FV	-	Fast Walsh Hadamard Transformation with Fuzzy Vault
ROP	-	Random Orthogonal Projection

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Today, biometrics has become part of our everyday life. From the start of the day to the end of the night, biometrics has made our life easy. The closest example of biometric is in our smartphone where it is used as an authentication token. Biometrics can be classified as physical and behavioral based where face, fingerprints, palm print, palm vein, hand geometry, iris, and finger vein are examples of physical biometric based and signature, gaits, keystrokes, and voice are examples of behavioral-based biometric.

Figure 1.1 Examples of biometric traits.

Biometric is widely used in authentication and identification as it possesses beneficial properties which are reliability, convenience, and universality (Andalib & Abdulla-Al-Shami, 2013). The properties are unique and measurable which makes it the perfect model to represent an individual. Furthermore, the use of biometrics is

much more convenient as the user no longer needs to remember a password or carry any token as the biometric lies within themselves. According to Chin et al., (2014), there are four main components in a biometric authentication system where number one is the sensor module in which to obtain the raw biometric data. Next, preprocessing and feature extraction module where enhancement and extraction of important feature take place. After that, the matching module where the query feature is compared with the stored template and lastly is the decision module where the system decides to authenticate or reject a user.

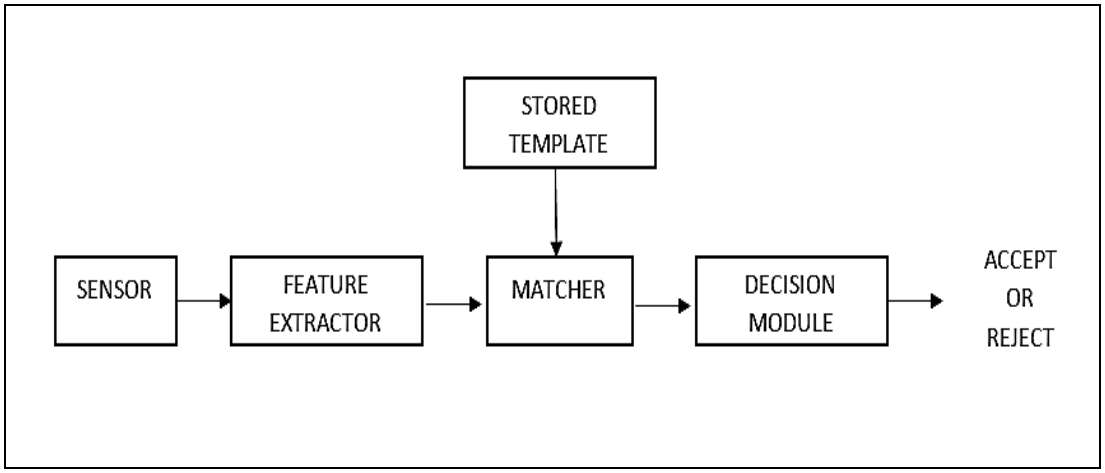

Figure 1.2 Different modules in biometric authentication system (Sarkar & Singh, 2020).

However, as the use of biometrics is rising, the security of raw biometrics is decreasing as there are many impostors out there who are trying to break the security of the biometric authentication system. Once a biometric template is compromised, it is considered broken as biometric cannot be revoked or canceled. Therefore, a biometric template protection authentication scheme is needed to protect the biometric template.

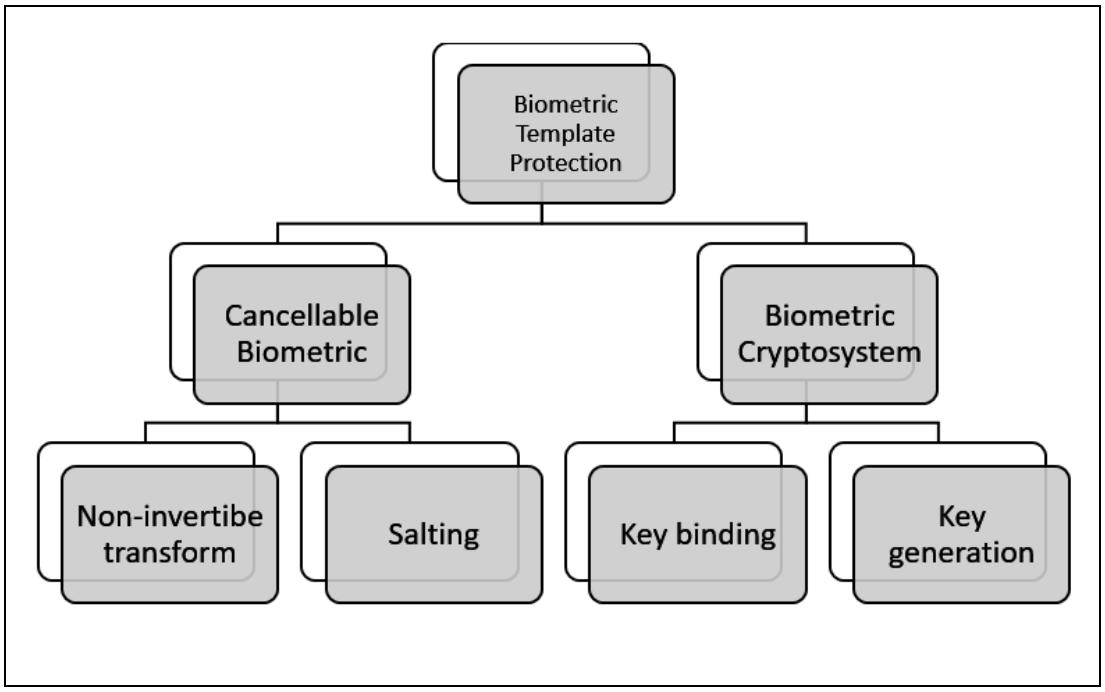

Figure 1.3 Classification of biometric template protection scheme.

Biometric template protection scheme can be categorized into two categories which are cancellable biometric and biometric cryptosystem. An example of cancellable biometrics is non-invertible transforms and salting. These methods provide security to templates by generating a transformed template that can be overridden whenever is needed (Chin et al., 2014). However, the security of this method depends on the secrecy of the key which makes it less suitable for authentication. Meanwhile, an example of a biometric cryptosystem is key binding and key generation. This method is categorized based on how the helper data is generated. In key binding schemes, helper data is derived by binding a chosen key to a biometric template while in the key generation scheme, helper data is derived directly from the biometric template. As fuzzy commitment only accepts binary features (Favre et al., 2015), the fuzzy vault is more popular in the key binding scheme as it can deal with an unordered set of data as biometric data possesses inherent fuzziness (Sarkar & Singh, 2020).

According to ISO/IEC standard 24745, a biometric template protection scheme has to fulfil certain requirements. The first requirement is diversity and is also known as unlinkability refers to the capacity to produce multiple unique templates from a single biometric feature such that none of them can be linked to either the original template or to each other in any way in order to prevent cross-matching and to ensure

user's privacy (Lahmidi et al., 2022; Sarkar & Singh, 2020). For example, the biometric template that undergoes transformation x should not link to a template from transformation y that came from the same original template.

The second requirement is revocability, which means that the mechanism employed to safeguard the template must be capable of obtaining a compromised template using the same biometric data. In other words, this attribute is demonstrated by replacing a biometric template that has been compromised with a new template created from the same biometric trait that is remarkably different from the compromised template (Lahmidi et al., 2022). For example, if biometric template is under attack from outsider, the system should be able to cancel the compromised template and replaced it with a new template generated from the same original template by changing the transformation parameter without affecting the user authentication process.

Meanwhile, the third requirement is irreversibility where the transformed template should not be able to revert to its original template in order to ensure the security of the biometric data and to guarantee the user privacy (Lahmidi et al., 2022; Sarkar & Singh, 2020). For example, if the attacker gained information on the transformed template, the information should not lead to the original template and forbid the recreation of the original template.

The last requirement is performance where the method used to secure the biometric template should not affect the performance of the authentication system. For example, the accuracy of the improved authentication system should not be lower from the previous authentication system. Simply put, a biometric template protection system provides methods and answers for a variety of biometric templates without compromising the system's performance (Sandhya & Prasad, 2017).

However, it is difficult for a biometric template protection scheme to fulfill all the requirements stated (Sarkar & Singh, 2020). For example, the fuzzy vault key binding scheme is unable to fulfill the revocability requirements of the biometric template protection scheme (Ponce-Hernandez et al., 2019). This attack happens when

the attacker is aware of other vaults that use the same biometric traits to safeguard them. The correlation between the vaults could be used by the attacker to find the genuine point set and discover the original template. A compromised template cannot be cancelled or issued again since biometric traits are limited and unchangeable (Bansal et al., 2015). As a result, the original template may be permanently deleted and unable to be used for any further authentication.

Many improvement methods have been suggested to improve the revocability requirements in the fuzzy vault scheme. Among them, a hybrid of cancellable and cryptosystem methods has been employed and reported to performed robustly in many studies (Bansal et al., 2015; Kaur & Sofat, 2017; Leng & Teoh, 2015; Li & Hu, 2016; Mahendran & Velusamy, 2020; Ponce-Hernandez et al., 2019, 2020; Singla et al., 2017; Sree, 2016; J. Zhang & Fang, 2018). This is due to the fact that a new template can be used to replace the compromised one by altering the index vector based on the same biometric in a non-invertible transform, providing diversity and revocability (Bansal et al., 2015).

Previous study shows that the selection of cancellable biometric methods is important. This is because, the process of combining cancellable biometric and biometric cryptosystem will increase the processing time of the overall authentication process (Jegede, 2017). Therefore, it is important to choose methods that can limit the processing time. Singla et al., (2017) for example used fast walsh hadamard transformation with fuzzy vault as fast Walsh Hadamard transformation is easy to compute. However, their fuzzy vault construct used Cyclic redundancy check (CRC) instead of error correcting codes. The used of CRC adds to the time complexity as each authentication attempt requires evaluating a large number of point combinations (Ponce-Hernandez et al., 2019).

Thus, this research proposed hybridization of fuzzy vault with fast Walsh Hadamard transformation function to enhance the fuzzy vault template protection scheme with the used of palm vein biometric.

1.2 Problem Statement

The increasing usage of biometrics as an authentication mechanism is indeed a stepping stone towards a modern era in this world. However, keeping the biometric template safe is a continuous challenge. The success of keeping the security of biometric authentication is to be able to satisfy all the biometric template protection scheme requirements which are diversity, revocability, security, and performance as mentioned in the problem background. The challenge is that not all the template protection scheme is able to satisfy all the requirement stated (Sarkar & Singh, 2020). Fuzzy vault template protection scheme is able to provide irreversibility and performance to biometric templates. However, it does not offer revocability and diversity. Therefore, this study aims to enhance the fuzzy vault template protection scheme that is able to meet all the biometric template protection requirements as well as improve the security of the authentication scheme.

1.3 Research Question

The research question for this study is as below:

(a) What are the limitations of the existing fuzzy vault scheme?

(b) What is the best method to overcome the limitation of fuzzy vault scheme?

(c) How does an improved fuzzy vault scheme can satisfy the biometric template protection requirements in terms of revocability and diversity?

1.4 Objectives

In order to achieve the goals of this study which is to enhance the fuzzy vault template protection scheme, the objectives are as below:

(d) To study the limitation of the existing Fuzzy Vault Scheme to protect biometric templates.

(e) To propose an improved Fuzzy Vault Scheme that can provide revocability and diversity.

(f) To evaluate and validate the performance of the improved fuzzy vault scheme in terms of revocability and diversity.

1.5 Scope of Research

The scopes of the research are as follows:

(a) Tongji palm vein datasets were used (Zhang et al., 2018). The dataset consists of 600 palms from 300 volunteers from Tongji University, Shanghai, China. The total images used for authentication are 6000 palm vein images.

(b) The resolution of all the images used are of 128x128 ppi.

(c) Feature extraction method used for all the images is Local Binary Pattern (LBP).

(d) Fast Walsh Hadamard transformation and random orthonormal transformation is used to transform 6000 palm vein images respectively.

(e) Fuzzy vault scheme is used as the authentication mechanism.

(f) False acceptance rate and false rejection rate is used to evaluate the performance of the authentication scheme.

1.6 Significant of Research

This research introduced the hybrid of fuzzy vault scheme and fast Walsh Hadamard Transformation (FWHT) function to enhance the fuzzy vault scheme. The proposed method increases the performance of the fuzzy vault scheme and is able to meet the revocability and diversity requirements of the biometric template protection scheme.

The hybrid of non-invertible transformation and fuzzy vault enable fuzzy vault to utilize the advantages of non-invertible transformation which is revocability and diversity. Therefore, fuzzy vault scheme can be equipped with revocability and diversity properties in biometric template protection scheme.

In addition, this research is important to benefit the society and industries as biometric has become one of the most popular authentication mechanism. Therefore, it is important to make sure that the template security is at the highest level in order to overcome attacks from unauthorized parties.

1.7 Thesis Organization

This thesis has been organized into several chapters as follows:

(a) Chapter 1 discusses the problem background, problem statement, objectives, scopes, and significance of the study.

(b) Chapter 2 reviews the details of the biometric template protection scheme which includes an explanation of biometric authentication, feature transformation approach, and issues related to biometric template protection.

(c) Chapter 3 describes the methodology used in each phase of the research. The research framework, the data and software used as well as the method for performance measures used in this research.

(d) Chapter 4 presents the proposed scheme and discusses the result and validation of the research. The results are compared between the types of feature transformation method and the proposed method.

(e) Chapter 5 summarizes and concludes the study which includes several findings and contributions of the research. The suggestion for future work is also provided in this chapter.

REFERENCES

Aberni, Y., Boubchir, L., & Daachi, B. (2020). Palm vein recognition based on competitive coding scheme using multi-scale local binary pattern with ant colony optimization. *Pattern Recognition Letters*, *136*, 101–110. https://doi.org/10.1016/j.patrec.2020.05.030

Adnan, S., & Alhayani, B. (2021). Materials Today : Proceedings A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. *Materials Today: Proceedings*, *xxxx*. https://doi.org/10.1016/j.matpr.2021.07.005

Aglio-Caballero, A., Rios-Sanchez, B., Sanchez-Avila, C., & De Giles, M. J. M. (2017). Analysis of local binary patterns and uniform local binary patterns for palm vein biometric recognition. *Proceedings - International Carnahan Conference on Security Technology*, *2017-Octob*, 1–6. https://doi.org/10.1109/CCST.2017.8167808

Ai, T., Nguyen, T., Nguyen, D. T., & Dang, T. K. (2015). *A Multi-factor Biometric Based Remote Authentication Using Fuzzy Commitment and Non-invertible Transformation*. 77–88. https://doi.org/10.1007/978-3-319-24315-3

Al-Assam, H., Sellahewa, H., & Jassim, S. (2009). A lightweight approach for biometric template protection. *Mobile Multimedia/Image Processing, Security, and Applications 2009*, *7351*(March), 73510P. https://doi.org/10.1117/12.818291

Alrahawe, E. A. M., Humbe, V. T., & Shinde, G. N. (2021). A contactless palm veins biometric system based on convolutional neural network. *2021 1st International Conference on Emerging Smart Technologies and Applications, ESmarTA 2021*. https://doi.org/10.1109/eSmarTA52612.2021.9515726

Andalib, A. S., & Abdulla-Al-Shami, M. (2013). A novel key generation scheme for biometric cryptosystems using fingerprint minutiae. *2013 International Conference on Informatics, Electronics and Vision, ICIEV 2013*, 0–5. https://doi.org/10.1109/ICIEV.2013.6572670

Arrahmah, A. I., Gondokaryono, Y. S., & Rhee, K. H. (2017a). Fast non-random chaff point generator for fuzzy vault biometric cryptosystems. *Proceedings of the 2016*

6th International Conference on System Engineering and Technology, ICSET 2016, 199–204. https://doi.org/10.1109/FIT.2016.7857565

Arrahmah, A. I., Gondokaryono, Y. S., & Rhee, K. H. (2017b). Fast non-random chaff point generator for fuzzy vault biometric cryptosystems. *Proceedings of the 2016 6th International Conference on System Engineering and Technology, ICSET 2016*, 199–204. https://doi.org/10.1109/FIT.2016.7857565

Babalola, F. O., Bitirim, Y., & Toygar, Ö. (2021). Palm vein recognition through fusion of texture-based and CNN-based methods. *Signal, Image and Video Processing*, *15*(3), 459–466. https://doi.org/10.1007/s11760-020-01765-6

Bansal, D., Sofat, S., & Kaur, M. (2015). *Transformation*. 1830–1834.

Bhateja, A. K., Chaudhury, S., & Saxena, P. K. (2014). A Robust Online Signature Based Cryptosystem. *Proceedings of International Conference on Frontiers in Handwriting Recognition, ICFHR, 2014-Decem*, 79–84. https://doi.org/10.1109/ICFHR.2014.21

Boult, T. E., Scheirer, W. J., & Woodwork, R. (2007). Revocable fingerprint biotokens: Accuracy and security analysis. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, *June 2007*. https://doi.org/10.1109/CVPR.2007.383110

Butt, M., & Damer, N. (2014). Helper data scheme for 2D cancelable face recognition using bloom filters. *International Conference on Systems, Signals, and Image Processing*, *May*, 271–274.

Chang, D., Garg, S., Ghosh, M., & Hasan, M. (2021). BIOFUSE: A framework for multi-biometric fusion on biocryptosystem level. *Information Sciences*, *546*, 481–511. https://doi.org/10.1016/j.ins.2020.08.065

Chin, Y. J., Ong, T. S., Teoh, A. B. J., & Goh, K. O. M. (2014). Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. *Information Fusion*, *18*, 161–174. https://doi.org/10.1016/j.inffus.2013.09.001

Choudhary, S. K. (2019). *Multimodal Biometric Authentication with Secured Templates – A Review*. *Icoei*, 1062–1069.

Dahake, P., & Nimbhorkar, S. (2015). Hybrid cryptosystem for maintaining image integrity using biometric fingerprint. *2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015*, *00*(c), 1–5. https://doi.org/10.1109/PERVASIVE.2015.7087177

Dandawate, Y. H., & Inamdar, S. R. (2015). Fusion based Multimodal Biometric cryptosystem. *2015 International Conference on Industrial Instrumentation and Control, ICIC 2015, Icic*, 1484–1489. https://doi.org/10.1109/IIC.2015.7150984

Dong, X., Khan, M. K., & Member, S. (2022). *Co-Learning to Hash Palm Biometrics for Flexible IoT Deployment*. *14*(8), 8–16. https://doi.org/10.1109/JIOT.2022.3190020

Eskander, G. S., Sabourin, R., & Granger, E. (2014). Improving Signature-Based Biometric Cryptosystems Using Cascaded Signature Verification-Fuzzy Vault (SV-FV) Approach. *Proceedings of International Conference on Frontiers in Handwriting Recognition, ICFHR, 2014-Decem*, 187–192. https://doi.org/10.1109/ICFHR.2014.39

Favre, M., Picard, S., Bringer, J., & Chabanne, H. (2015). Balancing is the Key - Performing Finger Vein Template Protection using Fuzzy Commitment. *2015 International Conference on Information Systems Security and Privacy (ICISSP)*, 304–311. https://doi.org/10.5220/0005241403040311

Feng, Y. C., Yuen, P. C., & Jain, A. K. (2010). *Discriminating Face Template*. *5*(1), 103–117.

Fronitasari, D., & Gunawan, D. (2017). Palm vein recognition by using modified of local binary pattern (LBP) for extraction feature. *QiR 2017 - 2017 15th International Conference on Quality in Research (QiR): International Symposium on Electrical and Computer Engineering, 2017-Decem*, 18–22. https://doi.org/10.1109/QIR.2017.8168444

Fuksis, R., Kadikis, A., & Greitans, M. (2011). Biohashing and fusion of palmprint and palm vein biometric data. *2011 International Conference on Hand-Based Biometrics, ICHB 2011 - Proceedings*, 268–273. https://doi.org/10.1109/ICHB.2011.6094334

Geetika, & Kaur, M. (2013). Multimodal based fuzzy vault using iris retina and fingervein. *2013 4th International Conference on Computing, Communications and Networking Technologies, ICCCNT 2013*, 1–5. https://doi.org/10.1109/ICCCNT.2013.6726786

Gupta, P., & Gupta, P. (2014). A vein biometric based authentication system. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8880*, 425–436. https://doi.org/10.1007/978-3-319-13841-1_24

Hidano, S., Ohki, T., & Takahashi, K. (2012). Evaluation of security for biometric guessing attacks in biometric cryptosystem using fuzzy commitment scheme. *Proceedings of 2012 International Conference of the Biometrics Special Interest Group, BIOSIG*, 1–6.

Jegede, et al. (2017). Cancelable and hybrid biometric cryptosystems: current directions and open research issues. *International Journal of ADVANCED AND APPLIED SCIENCES*, *4*(11), 65–77. https://doi.org/10.21833/ijaas.2017.011.010

Jin, Z., Teoh, A. B. J., Goi, B. M., & Tay, Y. H. (2016). Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation. *Pattern Recognition*, *56*, 50–62. https://doi.org/10.1016/j.patcog.2016.02.024

Juels, A. (2007). Fuzzy commitment. *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, 45–56. https://doi.org/10.1007/978-1-84628-984-2_3

Juels, A., & Sudan, M. (2006). A fuzzy vault scheme. *Designs, Codes, and Cryptography*, *38*(2), 237–257. https://doi.org/10.1007/s10623-005-6343-z

Kang, W., Liu, Y., Wu, Q., & Yue, X. (2014). Contact-Free Palm-Vein Recognition Based on Local Invariant Features. *PLoS ONE*, *9*(5), e97548. https://doi.org/10.1371/journal.pone.0097548

Kaur, M., & Sofat, S. (2017). Secure fingerprint fuzzy vault using hadamard transformation to defy correlation attack. *Proceedings - 2016 6th International Symposium on Embedded Computing and System Design, ISED 2016*, 122–126. https://doi.org/10.1109/ISED.2016.7977067

Kaur, M., & Sofat, S. (2018). Real-time chaff generation for a biometric fuzzy vault. *Turkish Journal of Electrical Engineering and Computer Sciences*, *26*(1), 89–100. https://doi.org/10.3906/elk-1610-255

Khalil-Hani, M., Marsono, M. N., & Bakhteri, R. (2013). Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm. *Future Generation Computer Systems*, *29*(3), 800–810. https://doi.org/10.1016/j.future.2012.02.002

Kubanek, M., Smorawa, D., & Holotyak, T. (2015). Feature extraction of palm vein patterns based on two-dimensional density function. *Lecture Notes in Artificial Intelligence (Subseries of Lecture Notes in Computer Science)*, *9120*, 101–111.

https://doi.org/10.1007/978-3-319-19369-4_10

Ladoux, P. O., Rosenberger, C., & Dorizzi, B. (2009). Palm vein verification system based on SIFT matching. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5558 LNCS*, 1290–1298. https://doi.org/10.1007/978-3-642-01793-3_130

Lahmidi, A., Moujahdi, C., Minaoui, K., & Rziza, M. (2022). On the methodology of fingerprint template protection schemes conception : meditations on the reliability. *Eurasip Journal on Information Security*, *2022*(1). https://doi.org/10.1186/s13635-022-00129-6

Lawand, S. J., & Chatterjee, M. (2013). *Computer Networks & Communications (NetCom). 131*, 489–498. https://doi.org/10.1007/978-1-4614-6154-8

Leng, L., & Teoh, A. B. J. (2015). Alignment-free row-co-occurrence cancelable palmprint Fuzzy Vault. *Pattern Recognition*, *48*(7), 2290–2303. https://doi.org/10.1016/j.patcog.2015.01.021

Li, C., & Hu, J. (2016). A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures. *IEEE Transactions on Information Forensics and Security*, *11*(3), 543–555. https://doi.org/10.1109/TIFS.2015.2505630

Lin, S., Xu, T., & Yin, X. (2017). Region of interest extraction for palmprint and palm vein recognition. *Proceedings - 2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics, CISP-BMEI 2016*, *4*, 538–542. https://doi.org/10.1109/CISP-BMEI.2016.7852769

Liu, H., Sun, D., Xiong, K., & Qiu, Z. (2014). A hybrid approach to protect Palmprint templates. *The Scientific World Journal*, *2014*. https://doi.org/10.1155/2014/686754

Mahendran, R. K., & Velusamy, P. (2020). A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things. *Computer Communications*, *153*(January), 545–552. https://doi.org/10.1016/j.comcom.2020.01.077

Mehmood, R., & Selwal, A. (2020). Polynomial based fuzzy vault technique for template security in fingerprint biometrics. *International Arab Journal of Information Technology*, *17*(6), 926–934. https://doi.org/10.34028/iajit/17/6/11

Mirmohamadsadeghi, L., & Drygajlo, A. (2011). Palm vein recognition with Local

Binary Patterns and Local Derivative Patterns. *2011 International Joint Conference on Biometrics, IJCB 2011*, 3–8. https://doi.org/10.1109/IJCB.2011.6117804

Mirmohamadsadeghi, L., & Drygajlo, A. (2014). Palm vein recognition with local texture patterns. *IET Biometrics*, *3*(4), 198–206. https://doi.org/10.1049/iet-bmt.2013.0041

Nagar, A., Nandakumar, K., & Jain, A. K. (2010). A hybrid biometric cryptosystem for securing fingerprint minutiae templates. *Pattern Recognition Letters*, *31*(8), 733–741. https://doi.org/10.1016/j.patrec.2009.07.003

Nguyen, M. T., Truong, Q. H., & Dang, T. K. (2016). Enhance fuzzy vault security using nonrandom chaff point generator. *Information Processing Letters*, *116*(1), 53–64. https://doi.org/10.1016/j.ipl.2015.08.012

Nguyen, T. A. T., Dang, T. K., & Nguyen, D. T. (2019). A new biometric template protection using random orthonormal projection and fuzzy commitment. *Advances in Intelligent Systems and Computing*, *935*(May), 723–733. https://doi.org/10.1007/978-3-030-19063-7_58

Ou, W. F., Po, L. M., Zhou, C., Xian, P. F., & Xiong, J. J. (2022). GAN-based Inter-Class Sample Generation for Contrastive Learning of Vein Image Representations. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *4*(2), 249–262. https://doi.org/10.1109/TBIOM.2022.3152345

Ponce-Hernandez, W., Blanco-Gonzalo, R., Liu-Jimenez, J., & Sanchez-Reillo, R. (2020). Fuzzy Vault Scheme Based on Fixed-Length Templates Applied to Dynamic Signature Verification. *IEEE Access*, *8*, 11152–11164. https://doi.org/10.1109/ACCESS.2020.2965165

Ponce-Hernandez, W., Blanco-Gonzalo, R., Sanchez-Reillo, R., & Liu-Jimenez, J. (2019). Template protection approaches: Fuzzy Vault scheme. *Proceedings - International Carnahan Conference on Security Technology*, *2019-Octob*, 5–9. https://doi.org/10.1109/CCST.2019.8888405

Pratiwi, A. Y., Tjokorda Agung Budi, W., & Ramadhani, K. N. (2016). Identity recognition with palm vein feature using local binary pattern rotation Invariant. *2016 4th International Conference on Information and Communication Technology, ICoICT 2016*, *4*(c), 1–6. https://doi.org/10.1109/ICoICT.2016.7571952

Ranjan, R., & Singh, S. K. (2013). Improved and innovative key generation algorithms

for biometric cryptosystems. *Proceedings of the 2013 3rd IEEE International Advance Computing Conference, IACC 2013*, *i*, 943–946. https://doi.org/10.1109/IAdCC.2013.6514353

Rathgeb, C., & Uhl, A. (2011). *A Survey on Biometric Cryptosystems*. 1–25.

Raut, S. D., & Humbe, V. T. (2016). A novel approach for palm vein feature extraction using Gabor and canny edge detector. *2015 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2015*, 0–3. https://doi.org/10.1109/ICCIC.2015.7435689

Raut, S. D., Humbe, V. T., & Mane, A. V. (2017). Development of biometric palm vein trait based person recognition system: Palm vein biometrics system. *Proceedings - 1st International Conference on Intelligent Systems and Information Management, ICISIM 2017*, *2017-Janua*, 18–21. https://doi.org/10.1109/ICISIM.2017.8122140

Salas, M. (2013). A Secure Framework for OTA Smart Device Ecosystems Using ECC Encryption and Biometrics. *Communications in Computer and Information Science*, *381 CCIS*, 204–218. https://doi.org/10.1007/978-3-642-40597-6_18

Sandhiya, D., & Thiyaneswaran, B. (2018). Extraction of dorsal palm basilic and cephalic hand vein features for human authentication system. *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2017*, *2018-Janua*, 2231–2235. https://doi.org/10.1109/WiSPNET.2017.8300156

Sandhya, M., & Prasad, M. V. N. K. (2017). *Biometric Template Protection : A Systematic Literature Review of Approaches and Modalities*. https://doi.org/10.1007/978-3-319-47301-7

Sarala, S. M., Karki, M. V., & Sharath Yadav, D. H. (2017). Blended substitution attack independent;fuzzy vault for fingerprint template security. *2016 International Conference on Circuits, Controls, Communications and Computing, I4C 2016*. https://doi.org/10.1109/CIMCA.2016.8053301

Sarkar, A., & Singh, B. K. (2020). A review on performance,security and various biometric template protection schemes for biometric authentication systems. *Multimedia Tools and Applications*, *79*(37–38), 27721–27776. https://doi.org/10.1007/s11042-020-09197-7

Selwal, A. (2015). *Performance Analysis of Template Data Security and Protection in Biometric Systems*. *December*.

Setiawan, H., & Yuniarno, E. M. (2016). Features extraction of palm vein image using phase symmetry. *Proceedings - 2015 4th International Conference on Instrumentation, Communications, Information Technology and Biomedical Engineering, ICICI-BME 2015*, 59–64. https://doi.org/10.1109/ICICI-BME.2015.7401335

Sidiropoulos, G. K., Kiratsa, P., Chatzipetrou, P., & Papakostas, G. A. (2021). *Feature Extraction for Finger-Vein-Based Identity Recognition*.

Singla, N., Kaur, M., & Sofat, S. (2017). Secure fingerprint fuzzy vault including novel chaff point generation method. *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2017*, *2017-Janua*(4), 1098–1103. https://doi.org/10.1109/CCAA.2017.8229959

Sree, S. R. S. (2016). *User Authentication System With Fuzzy Vault*.

Sun, S., Cong, X., Zhang, P., Sun, B., & Guo, X. (2021). Palm Vein Recognition Based on NPE and KELM. *IEEE Access*, *9*, 71778–71783. https://doi.org/10.1109/ACCESS.2021.3079458

Teoh, A. B. J., & Goh, A. (2006). Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *28*(12), 1892–1901. https://doi.org/10.1109/TPAMI.2006.250

Van Hoang, T., Duong, C. M., Van Vu, G., & Le, T. H. (2019). Palm Vein Recognition Using Enhanced Symmetry Local Binary Pattern and SIFT Features. *Proceedings - 2019 19th International Symposium on Communications and Information Technologies, ISCIT 2019*, 311–316. https://doi.org/10.1109/ISCIT.2019.8905179

Vo, T. T. L., Dang, T. K., & Küng, J. (2014). A hash-based index method for securing biometric fuzzy vaults. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8647 LNCS*, 60–71. https://doi.org/10.1007/978-3-319-09770-1_6

Wang, S., Deng, G., & Hu, J. (2017). A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. *Pattern Recognition*, *61*, 447–458. https://doi.org/10.1016/j.patcog.2016.08.017

Wang, S., & Hu, J. (2013). A Hadamard transform-based method for the design of cancellable fingerprint templates. *Proceedings of the 2013 6th International*

Congress on Image and Signal Processing, CISP 2013, *3*(Cisp), 1682–1687. https://doi.org/10.1109/CISP.2013.6743947

Wu, W., Wang, Q., Yu, S., Luo, Q., Lin, S., Han, Z., & Tang, Y. (2021). Outside Box and Contactless Palm Vein Recognition Based on a Wavelet Denoising ResNet. *IEEE Access*, *9*, 82471–82484. https://doi.org/10.1109/ACCESS.2021.3086811

Wu, W., Yuan, W. Q., Guo, J. Y., Lin, S., & Jing, L. T. (2012). Contact-less palm vein recognition based on wavelet decomposition and partial least square. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7701 LNCS*(March), 176–183. https://doi.org/10.1007/978-3-642-35136-5_22

Wu, X., & Zhang, D. (2006). Palm line extraction and matching for personal authentication. *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*, *36*(5), 978–987. https://doi.org/10.1109/TSMCA.2006.871797

Yang, W., Hu, J., & Wang, S. (2013). A finger-vein based cancellable bio-cryptosystem. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7873 LNCS*, 784–790. https://doi.org/10.1007/978-3-642-38631-2_71

Yasuda, M., Shimoyama, T., Abe, N., Yamada, S., Shinzaki, T., & Koshiba, T. (2016). Privacy-preserving fuzzy commitment for biometrics via layered error-correcting codes. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9482*, 117–133. https://doi.org/10.1007/978-3-319-30303-1_8

Yoon, E. J., & Yoo, K. Y. (2013). Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. *Journal of Supercomputing*, *63*(1), 235–255. https://doi.org/10.1007/s11227-010-0512-1

Yuan, L. (2015). Multimodal cryptosystem based on fuzzy commitment. *Proceedings - 17th IEEE International Conference on Computational Science and Engineering, CSE 2014, Jointly with 13th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2014, 13th International Symposium on Pervasive Systems*, , 1545–1549. https://doi.org/10.1109/CSE.2014.286

Zhang, J., & Fang, P. (2018). Two encryption schemes of finger vein template.

Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification, ASID, *2018-Novem*, 169–173. https://doi.org/10.1109/ICASID.2018.8693220

Zhang, L., Cheng, Z., Shen, Y., & Wang, D. (2018). Palmprint and palmvein recognition based on DCNN and a new large-scale contactless palmvein dataset. *Symmetry*, *10*(4), 1–15. https://doi.org/10.3390/sym10040078

Zhang, L., Li, L., Yang, A., Shen, Y., & Yang, M. (2017). Towards contactless palmprint recognition: A novel device, a new benchmark, and a collaborative representation based identification approach. *Pattern Recognition*, *69*, 199–212. https://doi.org/10.1016/j.patcog.2017.04.016

Zhou, X., Kuijper, A., & Busch, C. (2012). Retrieving secrets from iris fuzzy commitment. *Proceedings - 2012 5th IAPR International Conference on Biometrics, ICB 2012*, 238–244. https://doi.org/10.1109/ICB.2012.6199814

LIST OF PUBLICATIONS

(a) Alyanis N, Razak S, and Al-Dhaqm A (2020). Biometrics authentication techniques: A comparative study. International Journal of Advanced and Applied Sciences, 7(9): 97-103

(b) N. A. Farhaida Mohd Zainon and S. A. Razak, "Region of Interest Extraction for Biometric Cryptosystem," 2018 IEEE Conference on Application, Information and Network Security (AINS), 2018, pp. 33-37, doi: 10.1109/AINS.2018.8631495.

(c) N. A. F. M. Zainon and S. A. Razak, "Master and child key generation from palm vein," 2017 IEEE Conference on Application, Information and Network Security (AINS), 2017, pp. 37-41, doi: 10.1109/AINS.2017.8270421.