A NOVEL METHOD FOR SECURE FINGER VEIN BIOMETRIC DURING USER AUTHENTICATION PROCESS BASED ON BLOCKCHAIN-PSO-AES TECHNIQUES

ALI HADI MOHSIN ALKINANI

SULTAN IDRIS EDUCATION UNIVERSITY

2019

A NOVEL METHOD FOR SECURE FINGER VEIN BIOMETRIC DURING USER AUTHENTICATION PROCESS BASED ON BLOCKCHAIN-PSO-AES TECHNIQUES

ALI HADI MOHSIN ALKINANI

THESIS SUBMITTED IN FULFILLMENT OF THE REQUIREMENT FOR THE
DEGREE OF DOCTOR OF PHILOSOPHY (SOFTWARE ENGINEERING)

FACULTY OF ART, COMPUTING & CREATIVE INDUSTRY
SULTAN IDRIS EDUCATION UNIVERSITY
2019

UNIVERSITI PENDIDIKAN SULTAN IDRIS
اونيۏرسيتي ڤنديديقن سلطان ادريس
SULTAN IDRIS EDUCATION UNIVERSITY

Please tick (✓)
Project Paper □
Masters by Research □
Masters by Mix Mode □
Ph.D. ☑

INSTITUTE OF GRADUATE STUDIES

DECLARATION OF ORIGINAL WORK

This declaration is made on the 25 /09 /2019

i. Student's Declaration:

I'm Ali Hadi Mohsin -P20161001022-Faculty of Art, Computing, and Creative Industry Hereby declares that the dissertation /thesis for titled (A Novel Method for Secure Finger Vein Biometric During User Authentication Process Based on Blockchain-PSO-AES Techniques) is my original work. I have not plagiarized from any other scholar's work and any sources that contain copyright had been cited properly for the permitted meanings. Any quotations, excerpt, reference or re-publication from or any works that have copyright had been clearly and well cited.

____
Signature of the student

ii. Supervisor's Declaration:

I'm Dr. Aos Alaa Zaidan- hereby certify that the work entitled (A Novel Method for Secure Finger Vein Biometric during User Authentication Process Based on Blockchain-PSO-AES Techniques) was prepared by the above-named student, and was submitted to the Institute of Graduate Studies as a partial / full fulfillment for the conferment of the requirements for Doctor of Philosophy (By Research), and the aforementioned work, to the best of my knowledge, is the said student's work.

______________________ ______________________________
Date:25/09/2019 Signature of the Supervisor

UNIVERSITI PENDIDIKAN SULTAN IDRIS
SULTAN IDRIS EDUCATION UNIVERSITY

INSTITUT PENGAJIAN SISWAZAH /
INSTITUTE OF GRADUATE STUDIES

BORANG PENGESAHAN PENYERAHAN TESIS/DISERTASI/LAPORAN KERTAS PROJEK
DECLARATION OF THESIS/DISSERTATION/PROJECT PAPER FORM

Tajuk / *Title*: A Novel Method for Secure Finger Vein Biometric during User Authentication Process Based on Blockchain-PSO-AES Techniques.

No. Matrik /*Matric No.*: P20161001022

Saya / *I* : Ali Hadi Mohsin Alkinani

mengaku membenarkan Tesis/Disertasi/Laporan Kertas Projek (Kedoktoran/Sarjana)* ini disimpan di Universiti Pendidikan Sultan Idris (Perpustakaan Tuanku Bainun) dengan syarat-syarat kegunaan seperti berikut:-
acknowledged that Universiti Pendidikan Sultan Idris (Tuanku Bainun Library) reserves the right as follows:-

1. Tesis/Disertasi/Laporan Kertas Projek ini adalah hak milik UPSI.
   The thesis is the property of Universiti Pendidikan Sultan Idris

2. Perpustakaan Tuanku Bainun dibenarkan membuat salinan untuk tujuan rujukan dan penyelidikan.
   Tuanku Bainun Library has the right to make copies for the purpose of reference and research.
3. Perpustakaan dibenarkan membuat salinan Tesis/Disertasi ini sebagai bahan pertukaran antara Institusi Pengajian Tinggi.
   The Library has the right to make copies of the thesis for academic exchange.
4. Sila tandakan (√) bagi pilihan kategori di bawah / Please tick (√) from the categories below:-

□	**SULIT/*CONFIDENTIAL***	Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub dalam Akta Rahsia Rasmi 1972. / *Contains confidential information under the Official Secret Act 1972*
□	**TERHAD/*RESTRICTED***	Mengandungi maklumat terhad yang telah ditentukan oleh organisasi/badan di mana penyelidikan ini dijalankan. / *Contains restricted information as specified by the organization where research was done.*
□	**TIDAK TERHAD / *OPEN ACCESS***	

______________________________ ______________________________

(Tandatangan Pelajar/ Signature)

(Tandatangan Penyelia / *Signature of Supervisor*)
& (Nama & Cop Rasmi / *Name & Official Stamp*)

Tarikh: _____25/09/2019_____

Catatan: Jika Tesis/Disertasi ini **SULIT @ TERHAD**, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh laporan ini perlu dikelaskan sebagai **SULIT** dan **TERHAD**.

Notes: If the thesis is CONFIDENTAL or RESTRICTED, please attach with the letter from the related authority/organization mentioning the period of confidentiality and reasons for the said confidentiality or restriction.

ACKNOWLEDGMENT

"In the name of Allah, the Most Gracious and the Most Merciful"

Alhamdulillah, first and foremost, praise be Allah, the Cherisher and Sustainer of the World and to the Prophet Muhammad (Peace and Blessings of Allah Be Upon Him, His Family and His Righteous Companions) who was sent by Allah to be a great teacher to the mankind.

I would like to extend my appreciation to who involved and give a helpful hand in ensuring the success of this research. This research would not have come to fruition without all your help and supports. Special thanks to my supervisor, Dr. Aos Alaa Zaidan, for his guidance, support, patience and advise me during my work on this research, very thanks to Dr. Bilal Alaa Zaidan and Multimedia Lab in Chonbuk National University, South Korea.

My warmest appreciation to my parents and soul friend, lovely wife Zainab Mizaal Hussain for always being beside me and never give up in supporting me, and my brother Adel beloved who support me with their love. This research would not have come to fruition without all their help and supports.

Thank you. Allah blesses you.

ABSTRACT

This research aims to develop a new method to secure finger-vein (FV) biometric information during user authentication process against different types of network security attacks. Hence, a novel method was proposed to solve the existing problem in biometric authentication systems, which is the leakage of biometric information. Our proposed method meets information security definition standard requirements (CIA). The research design was carried out in two stages. In the first stage, the researcher developed a new merge algorithm in order to produce a new hybrid biometric pattern by merging Radio Frequency Identification (RFID) features with FV biometric features to increase the randomization, and enhance the security and structure of the new pattern. While, in the second stage, a new secure user verification method is developed based on blockchain technique, AES algorithm and a new steganography method that is based on Particle Swarm Optimization (PSO) algorithm. A dataset was used comprising of 6000 samples of FV images. The experimental results showed the effectiveness of the proposed authentication method. Where, this method achieved a high level of performance accuracy of 97.9% during the implementation of this method using FV biometric for 106 users. Furthermore, the proposed method has an advantage 55.56% higher than the benchmark method as a result of the comparison between the proposed method and benchmark method, depending on some security issues where, the proposed method covered 100% of these issues. Whereas, the benchmark method covered only 44.44% as indicated in Chapter 5. Moreover, the results showed that the structure of hybrid pattern is robust and immune towards detection by the attacker, and is flexible to being cancelable and reconstructed again in case of loss of this pattern. More so, the proposed method showed high resistance against spoofing and brute-force attacks. Clearly, such empirical results suggest that the FV information are confidential, integrated and available only for specific authorized persons only in the entire steps of the authentication process.The implication of this study is that, the proposed method can be applied in decentralised network architectures by eliminating the central point, and addressing the network failure problem and security at the same time.

.

KAEDAH TERKINI UNTUK BIOMETRIK VENA-JARI SEMASA PROSES PENGESAHAN PENGGUNA BERDASARKAN TEKNIK BLOKCHAIN-PSO-AES

ABSTRAK

Kajian ini bertujuan untuk membangunkan suatu kaedah baru untuk mencapai sekuriti keselamatan biometrik jari-vena (FV) semasa proses pengesahan pengguna terhadap pelbagai jenis serangan sekuriti keselamatan rangkaian. Oleh itu, suatu kaedah terkini telah dicadangkan untuk menyelesaikan masalah yang sedia ada di dalam sistem pengesahan biometrik seperti kebocoran maklumat biometrik. .Kaedah cadangan penyelidik memenuhi keperluan piawaian definisi keselamatan maklumat (CIA). Suatu reka bentuk kajian telah dijalankan berdasarkan dua peringkat. Pada peringkat pertama, penyelidik telah membangunkan algoritma penggabungan baru untuk menjana corak biometrik hibrid baru, dengan menggabungkan ciri pengenalan frekuensi radio (RFID) dengan ciri biometrik FV untuk mempertingkatkan penyelesaian yang rawak, serta mempertingkatkan keselamatan dan struktur corak baru. Sementara dalam peringkat kedua, kaedah pengesahan pengguna baru yang selamat telah dibangunkan berdasarkan *blokchain*, algoritma AES , dan suatu kaedah steganografi baru berdasarkan algoritma Pengoptimuman Kerumuman Partikel (Particle Swarm Optimization - PSO).Satu set data telah diguna, yang terdiri daripada 6,000 sampel imej. Hasil kajian eksperimental menunjukkan keberkesanan kaedah pengesahan yang dicadangkan. Di mana, kaedah ini telah mencapai prestasi ketepatan yang tinggi sebanyak 97.9% semasa pelaksanaan kaedah ini dengan penggunaan jari-vena (FV) biometrik untuk 106 pengguna.Tambahan pula, kaedah yang dicadangkan mencapai kelebihan 55.56% lebih tinggi berbading kaedah penanda aras sebagai hasil perbandingan di antara kaedah yang dicadangkan dan kaedah penanda aras, bergantung kepada beberapa isu keselamatan di mana, kaedah yang dicadangkan meliputi 100% daripada isu-isu ini. Manakala, kaedah penanda aras hanya meliputi 44.44% seperti yang ditunjukkan di dalam Bab 5. Selain itu, hasilnya menunjukkan bahawa struktur corak hibrid adalah mantap dan kebal terhadap pengesanan oleh pihak penyerang, dan fleksibel untuk dibatalkan dan dibina semula sekiranya berlaku kehilangan corak ini. Lebih-lebih lagi, kaedah yang dicadangkan menunjukkan rintangan yang tinggi terhadap serangan *spoofing* dan *brute-force.* Jelas sekali, keputusan empirikal menunjukkan bahawa maklumat FV adalah sulit, bersepadu dan hanya tersedia untuk orang yang diberi kuasa tertentu sahaja dalam keseluruhan langkah proses pengesahan. Implikasi kajian ini adalah, kaedah yang dicadangkan boleh digunakan dalam arkitektur rangkaian desentralisasi dengan menlenyapkan titik pusat dan menangani masalah kegagalan rangkaian serta sekuriti pada masa yang sama.

TABLE OF CONTENT

Page

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBERVIATIONS

ANN	Artificial Neural Network
BLPOC	Band Limited Phase-Only Correlation
BP	Bit Pole
CNN	Convolutional Neural Network
CCD	Charge Coupled Device
CN	Crossing Number
CS	Compressing Sensing
CI	Compressive Imaging
DBC	Discriminative Binary Code
DES	Data Encryption Standard
DMD	Digital Micromirror Device
EER	Equal ErrorRrate
ECC	Error Correcting Code
FAR	False Acceptance Rate
FCS	Fuzzy Commitment Scheme
FRR	False Reject Rate
FVRS	Finger Vein Recognition System
FPGA	Field Programmable Gate Array
FVHS	Fountain Valley High School
FVT	Finger Vein Textures
FV	Finger Vein
GA	Genetic Algorithm
HF	high frequency
HVS	Human Visual System
IOT	Internet of Think
KMP	Knuth-Morris-Pratt String Matching Algorithm
LBP	Local Binary Pattern
LED	Light Emitting Diode
LSB	Last Significant Bit

MCM	Maximum Curvature Method
MD5	Message-Digest algorithm 5
MSE	Mean Sequare Error
NIR	Near-Infrared
OPM	Occurrence Probability Matrix
P2P	Pear to Paer
PSO	Particle Swarm Optimization
PSNR	Peak Signal-to-Noise Ratio
PCA	Principal Component Analysis
RFID	Radio Frequency Identification
ROI	Region of Interest
ROC	Receiver Operating Characteristic Curve
RSA	Rivest–Shamir–Adleman
SB	Secret Bit
SVDMM	Singular Value Decomposition-Based Minutiae Matching
SVM	Support Vector Machine
UHF	Ultra High Frequency
WORM	Write One Read Many

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Research Background

In the last two decades,in term of software engineering there are many researches work regarding human being biometrics used in individual authentication have been conducted (Qiu, Kang, Tian, Jia, & Huang, 2018). We can divide biometrics into two groups, namely, physiological and behavioural biometric characteristics, which have been both developed and implemented by many researchers. Behavioural biometrics include voice, signature and gait, whilst physiological biometrics are fingerprint, facial and palm prints, hand shape and iris, some of which are shown in Figure 1.1. Although many biometrics are available, most are unsecure, unreliable or uncomfortable for users; for example, the aforementioned biometrics, such as fingerprints, palm prints, voice, signatures and hand shapes, are easy to forge, whilst iris scanning is uncomfortable to users. Moreover, face recognition can be bypassed via 3D printing(Y. Wang, Wang, & Xue, 2018).

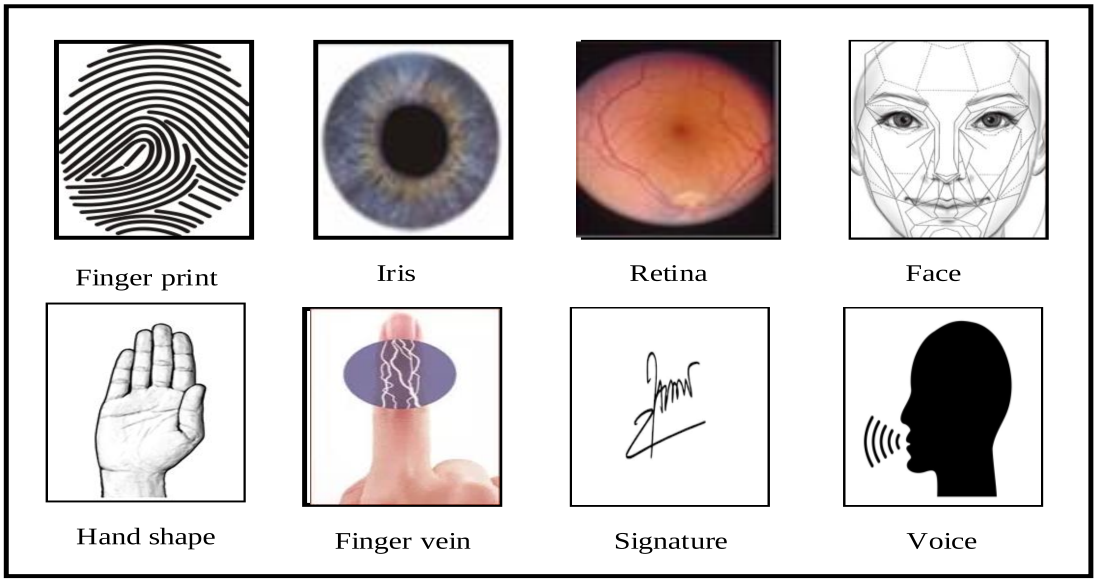


Figure 1.1. Examples of Human Biometrics

Furthermore, all aforementioned biometrics are susceptible to spoofing attacks, wherein a copy of biometrics can be taken by any intruder and used to obtain permission for access to the system in the future (Z. Liu, Yin, Wang, Song, & Li, 2010). Amongst various biometric techniques, finger vein (FV) recognition is newly developed and has inherent superiority in terms of accuracy, speed and security. Remarkable achievements have been observed in recent decades. In 2000, medical scientists Kono and Ueki proposed a way of capturing FV images using near-infrared rays; these images can be used for personal identification. In the same and coming years, (Miura, Nagasaka, & Miyatake, 2004) introduced an effective way to extract features from FV images. This algorithm considerably influenced majority of the following researchers. By 2007, Japanese researchers had presented all the pioneering research works of FV recognition and had proposed various devices, algorithms and patents. Since 2008, a considerable amount of research has been performed by Korean and Chinese researchers. In recent years, multimodal biometrics using FV and other biometric features has been proposed (Tang, Huang, Li, Li, & Li, 2012). Amongst various hand biometrics, hand vein biometrics has been proven useful for personal identification and has several advantages compared with other methods. Table 1.1. illustrates the comparsion of various biometric characteristics in term of authentication.

Table 1.1

Characteristics Comparison of Various Biometric Authentications

Type	Properties	Shortcoming	Security	Sensor device	Cost
Voice	Natural/comfortable	Noise/cold diseases	Normal	No contact required	Low
Face	Remote-controlled/comfortable	Light	Normal	No contact required	Low
Fingerprint	Extensively usage/comfortable	Skin diseases	Good	Contact required	Low
Iris	High accuracy/uncomfortable	Eyeglasses/side effect	Excellent	No contact required	High
Finger vein	**High accuracy/ comfortable**	**Few**	**Excellent**	**No contact required**	**Low**

The skin condition on the finger generally does not hinder the acquisition of clear FV images. Moreover, vein biometrics uses vascular patterns inside the human body, making it insusceptible to forgery. Vein biometrics is also contactless; no physical contact is required between the finger and the sensor in the authentication process. Thus, no hygiene issue must be addressed in relation to body health. Overall, FV is the best method because hand and palm veins require a sufficiently large camera aperture size to obtain the vein image from the entire hand (William, Ong, Lau, & Goh, 2016). Human FV biometrics is a type of physiological biometric used to identify individuals based on physical characteristics and some properties of the blood veins. FV biometrics is also a new technology employed in security systems and has been applied in different fields, such as medicine, finance, law and various commercial applications, to identify criminals and perform other tasks that require high levels of security and privacy. This new technology has a higher level of accuracy compared with other types of biometrics (Nandhinipreetha & Radha, 2016). FV image quality is inherently affected by numerous factors that can be split into two categories: 1) extrinsic factors, which are associated with environmental illumination, ambient temperature, physiological changes, light scattering and user behaviour, and 2) intrinsic factors, which are associated with inaccurate parameter estimation during the image preprocessing stage. For example, FV image enhancement and segmentation schemes have been developed to extract vein patterns in most FV verification systems. Incorrect estimation of orientation, scale and rotation angle of vein patterns may produce false FV features, thus resulting in failure to detect some genuine vein features. Various FV quality schemes have been recently developed to solve the aforementioned problem (Qin & El-Yacoubi, 2015). The principle of this system is shown in Figure 1.2.

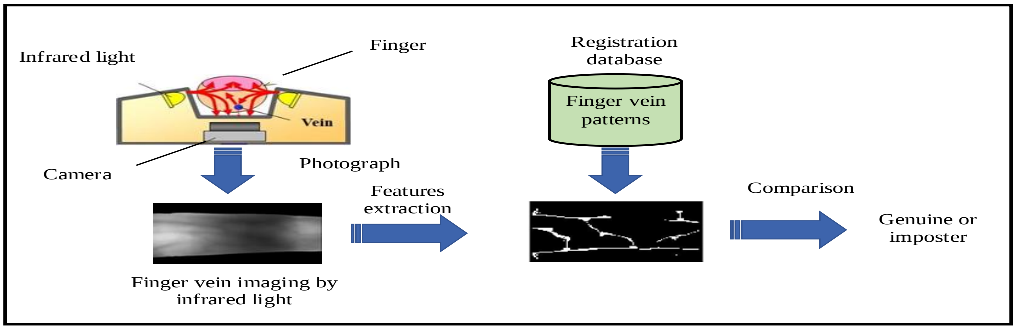


Figure 1.2. Principle of Work in the Finger Vein Biometric Verification

FV verification comprises four main stages, as shown in Figure 1.3. These stages include image acquisition, preprocessing, processing and matching.

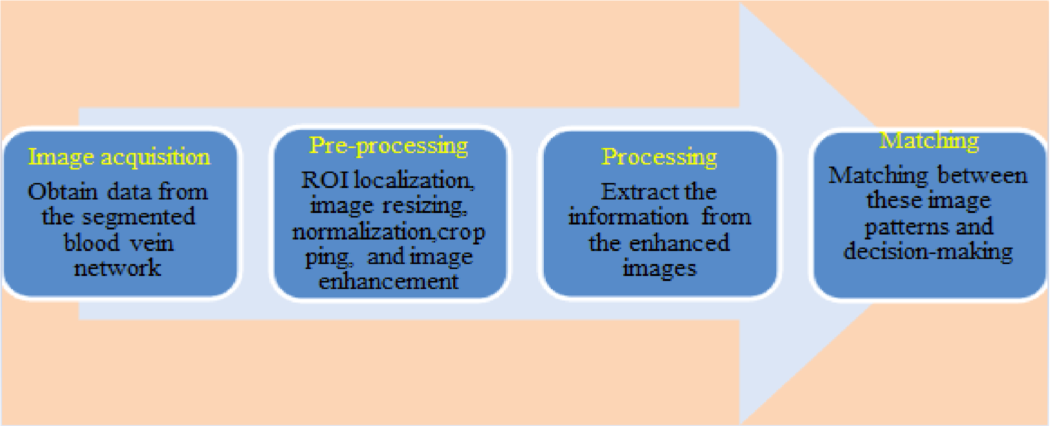
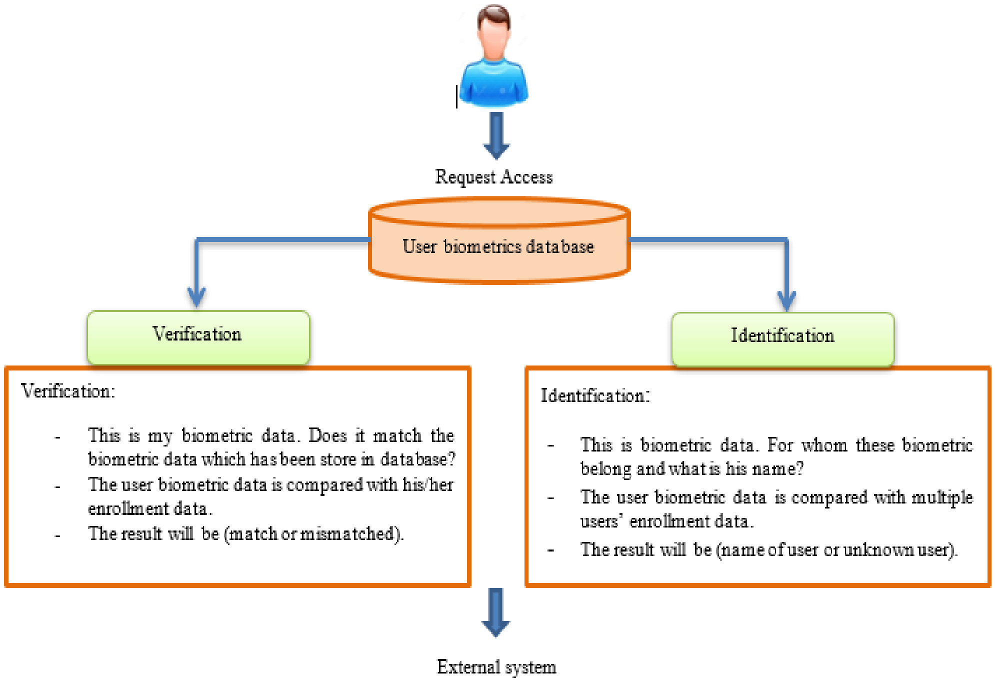


Image acquisition
Obtain data from the segmented blood vein network
Pre-processing
ROI localization, image resizing, normalization,crop ping, and image enhancement
Processing
Extract the information from the enhanced images
Matching
Matching between these image patterns and decision-making

Figure 1.3. Block diagram of Finger Vein Biometric Verification System

Infrared cameras are normally used to capture FV images, where these vein appear as dark lines because the haemoglobin in the blood absorbs the infrared light (Chavez-Galaviz, Ruiz-Rojas, & Garcia-Gonzalez, 2015). This light has a wavelength of 760–850 nm and can penetrate deep into the finger skin (J. Yang, Shi, & Yang, 2011). Next, preprocessing operations, such as normalisation and segmentation, are applied to remove noise from vein images or resize them to a suitable size. The image background is also removed, and some filters are applied to enhance vein images and extract the region of interest (ROI) (Z. Wu et al., 2016). The most important challenge is the low quality of FV images, which leads to low-level accuracy in verification results. Then, the processing operation, which comprises FV feature extraction, is performed. Finally, matching is conducted to compare the extracted features from the FV pattern during user registration and the stored pattern in the server database, which determines whether the user is genuine or an impostor. In this study, we focus on using FV biometrics in user verification operation, which is different from user identification. We briefly describe the differences between the two operations in Figure 1.4 to emphasise our findings.



Verification:

- This is my biometric data. Does it match the biometric data which has been store in database?
- The user biometric data is compared with his/her enrollment data.
- The result will be (match or mismatched).

Identification:

- This is biometric data. For whom these biometric belong and what is his name?
- The user biometric data is compared with multiple users' enrollment data.
- The result will be (name of user or unknown user).

Figure 1.4. Identification vs Verification

The use of each type of the aforementioned systems depends on the type of field and required level of security.The threat in authentication systems based on biometrics technology lies in the leakage of biometric templates (Jialiang Peng, Qiong Li, Ahmed A. Abd El-Latif, 2014). Where can attack these systems by using stolen information because replacing the raw biometric information after these data are stolen is impossible (Suzuki, Suzuki, Urabe, & Obi, 2013) and (W. Yang, Huang, Zhou, & Liao, 2014). Therefore, these systems require the security of biometric templates. Biometric patterns stored in databases, which are extracted as biological biometrics through authentication processes, should be effectively secured and protected from all attacks. In the real world, billions of devices are connected through networks; thus, the issue lies in protecting and securing personal information and keeping this information secure; this challenge is becoming a popular topic in all kinds of systems, especially authentication ones (Lu et al., 2017).

1.2 Research Problem

We look forward to the development and design of a robust FV biometric verification framework that has a high level of resistance against different types of attacks and maintains the verification framework performance within an acceptance level of error rate, that is, the equal error rate (EER) is between 2.14 and 0.0009 (W. Yang et al., 2014) (N.Sugandhi, M.Mathankumar, 2014). At this point, false acceptation rate (FAR) is equal to false rejection rate (FRR), as well as the accuracry between 93.5% and 99.7% (Ong, Teng, Muthu, & Teoh, 2013)(Z. Li, Sun, Di, & Hao, 2010). However, a critical problem in relation to this technology is the security of the FV data inside the verification framework. This problem is considered to be a big challenge in this type of technology, where leakage of biometrics leads to serious risks when stolen FV templates are used in various attacks, such as spoofing and brute-force attacks (Suzuki et al., 2013). This problem will also have an impact on the reliability of the verification framework and the rights of stakeholders. Biometric data are prone to different types of attack either during an individual’s enrolment step, wherein the user attempts to obtain services from cloud computing or IOT (Z. Wu et al., 2016)**,** or during data transmission between client and server, wherein databases of the FV biometrics are stored. Finding a solution to this problem is important because changing this biometric is impossible after it is stolen. This type of biometric is a part of the human body and remains stable for a long time (from birth to death), making it difficult to change or modify (Cheng, Chen, & Cheng, 2016). Most of the studies that have been attempted used different ways to secure FV biometric (Murakami, Ohki, & Takahashi, 2016) in the verification framework, such as uni-biometrics (FV biometrics) or multi-biometrics, which include FV biometrics as part of the verification framework. These methods have been applied in two steps according to the literature review.

Researchers have been attempting to create user patterns via extracted features from FV images, which have unique individual identities. The collected features from the FV intersection points and the angles bounded between veins using different descriptor methods are considered unique information used to generate unique and cancellable keys (bio-key). Data patterns are then encrypted based on this key using encryption functions (Chavez-Galaviz et al., 2015)(Z. Wu et al., 2016). Observation matrices are also used to extract the information of pattern features, and random keys are utilised to encrypt such information (Suzuki et al., 2013). Some researchers used multi-biometrics to obtain additional biometrics features, such as FV, retina and fingerprint, which have been employed by individuals for identification; features are extracted from all biometrics, and then, an encryption algorithm is employed to secure pattern information (Jagadiswary & Saraswady, 2016). Moreover, some systems use more four biometrics, such as FV, fingerprint, knuckle and finger shape, along with a key for encrypting pattern information (Jialiang Peng, Qiong Li, Ahmed A. Abd El-Latif, 2014). Some systems employ multimodal biometric systems, such as FV and signature image, to obtain unique features from the individual and cryptography to secure these data (Nandhinipreetha & Radha, 2016). All the aforementioned attempts used encryption methods to protect FV biometric information. However, some vulnerabilities are observed in biometric encryption systems; for example, the attacker can regenerate an estimate of the enrolled biometric template and use it to release the stored secret (Marius Iulian Mihailescu, 2011). Moreover, these attempts do not use random biometrics to create undetectable biometrics in case of encryption loss or breakage. Additional details regarding the research problem are presented in Section 2.5.3.

Figure 1.5 shows the research gap and the general problem extracted from the literature review. Moreover, the specific problem, which is extracted from the critical analyses in Sections 2.5 and 2.6, is discussed. All attempts in the literature to secure FV information are still insufficient when the system connects online to the World Wide Web and in standalone frameworks because these attempts used cryptography to secure biometric information without consideration of information security standard requirements (CIA) which are confidentiality, integrity and availability, this definition is international standard ISO/IEC 27002 (2005). This definition states that secret information must be meet requirements of CIA triangle (Von Solms & Van Niekerk, 2013) and CIA are respectively explained in 2 and 3 in Figure 1.5.

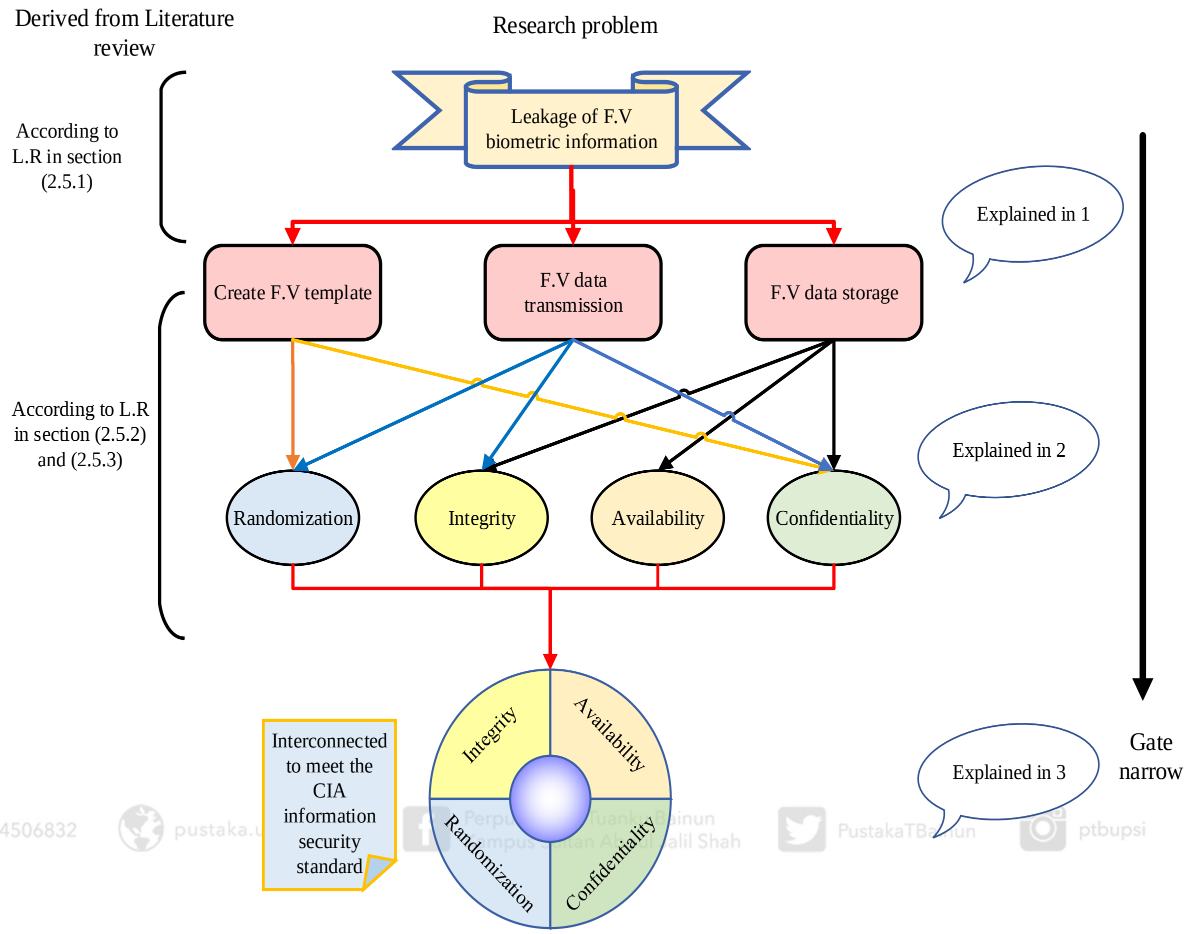


Figure 1.5. Shown General Problem and Describe the Specific Problem

1. According to the literature review in chapter (2) the research gap is protecting F.V biometric patterns against leakage of biometric information within authentication systems.

2. According to the literature review, previous studies attempted to protected F.V biometric information through extract pure and non-randomize features from F.V and send these features as information to the central point for authentication purpose. Therefore, we need to secure F.V information during transmission. Moreover, it is very important to enhancement pattern randomization and meet the standard security requirements which are confidentiality, integrity and availability.

3. The randomization for confidentiality, integrity and availability need to interconnect in order to protect the F.V pattern information ageinst attacks during the individual's authentication operation which start from client, data transmission as well as inside the server database according to the research problem definition. More details in recommended solution section 2.6.1.

1.3 Research Questions

The following research questions are formulated to set the direction of this research.

1. What are the researches that have been conducted in last 10 years in term of authentication based on F.V biometric?

2. What are the research gap and weak points in the existing authentication methods in FV biometrics?

3. What are the FV template problems and issues that represent serious challenges in terms of security?

4. How we can be achieving the information security definition standard (CIA) requirments regarding to secure F.V information?

5. What are the suitable technologies which can be used in order to enhance the weakness points and find the solution for defined problem?

6. Are the results of proposed solution (new framework), is appropriate for the security purpose?

7. Is the performance of proposed methods are acceptable?

1.4 Research Objectives

This study is beneficial for companies and different organisations working in various fields, such as medical, financial, law enforcement, airports and other applications that need high-level security and privacy to ensure customer data protection by securing verification data through the hiding of data from intruders. The main goal of this research is to develop an efficient FV biometric framework with high level of security and secure individual data during transmission as well as that inside the database. The specific research objectives are as follows:

1. To investigate existing researches and technologies that used FV biometric in terms of user authentication in order to highlight the gaps and weaknesses.
2. To design new secure FV biometric pattern through enhance the FV pattern structure and content randomisation.
3. To develop a new and secure user authentication method based on the proposed FV biometric pattern.
4. To validate and evaluate the proposed method that used for secure user authentication.

1.5 Relationship among Research Objectives, Research Questions and Research Problem

In this section, we interconnect the research questions formulated for the research direction and the research objectives provided to obtain answers for the questions. In Table 1.2, we present the research questions and the answers that can aobtain via the objectives because they determine the part of the research problem that is solved by the fulfilment of each objective.

Table 1.2

Relationship Among Research Questions, Research Objectives and Research Problem

			Research problem mapping
Research questions	Research objectives	Specific problem	General problem
1. What are the researches that have been conducted in last 10 years in term of authentication based on F.V biometric? 2. What are the research gap and weak points in the existing authentication methods in FV biometrics?	To investigate existing researches and technologies that used FV biometric in terms of user authentication in order to highlight the gaps and weaknesses.		Secure F.V templates during authentication process
3. What are the FV template problems and issues that represent serious challenges in terms of security?	To design new secure FV biometric pattern through enhance the FV pattern structure and content randomisation	Randomization in F.V templates information	

(*Continued)*

Table 1.2 (*Continued)*

			Research problem mapping
Research questions	Research objectives	Specific problem	General problem
4. How we can be achieving the information security definition standard (CIA) requirements regarding to secure F.V information? 5. What are the suitable technologies which can be used in order to enhance the weakness points and find the solution for defined problem?	To develop a new and secure user authentication method based on the proposed FV biometric pattern	Enhance finger vein information security in term of confidentiality, integrity and availability	Secure F.V templates during authentication process
6. Are the results of proposed solution (new framework), is appropriate for the security purpose? 7. Is the performance of proposed methods are acceptable?	To validate and evaluate the proposed method that used for secure user authentication		

1.6 Scope of the Study

The scope of this research is defined by the following considerations.

1. This study focuses on the development of a new hybrid and random FV biometric model that uses the proposed merge algorithm for application in individual verification frameworks.

2. A new steganography method based on particle swarm optimisation (PSO) is developed.

3. A novel secure biometric verification framework for individuals based on encryption, block chain and the proposed steganography techniques is established.

4. Experimental work is performed to hide FV pattern information and evaluate the proposed steganography method and the entire verification framework performance.

The general view for this research can be represented via three factors, namely, research method, research type and research domain, as shown in Figure 1.6.

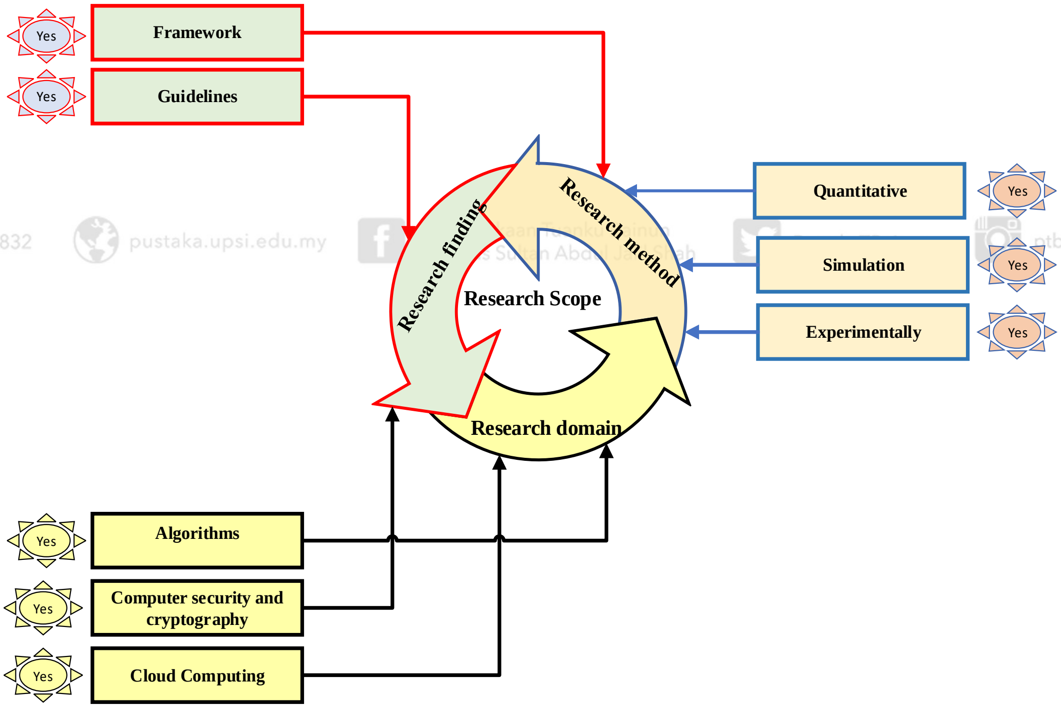


Figure 1.6. Research Scope

This study is multidisciplinary because it combines two fields of sciences, namely, information technology and biology, where biometrics mean biological measurement in computer technology (Jaiswal, Bhadauria, & Jadon, 2011). This study develops a new secure verification framework for individual authentication based on human blood FV, which is a human biometric model. This research is conducted to address the leakage problem of FV biometric patterns in verification systems. This study uses a quantitative research method; the proposed framework is verified to have a high level of protection and performance via experimental results. The output of the research indicates the research type, and two outputs are presented in this study, namely, the guideline for securing any information system and a secure framework for individual authentication. The research domain involves three computer science domains: the algorithm domain, the proposed merge algorithm and the proposed framework for the cloud computing environment. Finally, this study focuses on data security based on the standard information security definition. Consequently, computer security and encryption are the main domain of this study.

1.7 Motivations

The F.V biometric technology is a product of the development of the modern society to satisfy the requirements in many applications of human biometric verification. Where F.V biometric has some advantages over other types of biometrics (Dong, Yang, Yin, Liu, & Xi, 2012) such as:

1. No need to contact between user and device sensor so, there is no ability to trace the user in future and try to copy his biometric by any attacker, moreover this feature makes using this biometric very comfortable to the users.

2. It can be used only for live body because it depends on the hemoglobin in the blood.

3. This biometric are reliable have high level of security.

4. unique among all the people even the twins and stable for long time.

5. Small and cheap devices need to work and portable so can be easy use in different locations.

6. F.V are hidden under the skin surface so it is invisible and cannot be prone to external distortion and it is very hard to replicate. In general, the most important motivation which is *security motivations* which is related to F.V biological attributes.

Where references (Mohd Asaari, Suandi, & Rosdi, 2014), (J. Da Wu & Liu, 2011b) and (Peng, El-Latif, Li, & Niu, 2014) referred that biometrics technology authentication system is extensively popular because this system provides a high level of security and reliability for individual authentication system; these types systems are more reliable than the traditional technology used in authentication systems, which has been used to secure critical and secret organizations, such as password and access cards; these types of authentication technologies are easy to copy and replicate and are prone to counterfeit; thus, criminals can easily use the stolen information. In addition, the incidence of forgetting passwords or cards is high; by contrast, F.V biometrics demonstrates numerous attributes in terms of security purposes, such as the uniqueness of each person and long-term stability during human life; F.V are invisible to the human eye because veins are located underneath the skin; thus, F.V are not prone to external distortion or modification; moreover, Studies in (J. Da Wu & Ye, 2009) and (Ong et al., 2013) defined that F.V biometric is unique to every person; thus, it is more reliable in verifying identity than other techniques, such knowledge- or token-based verification systems. References (N.Sugandhi, M.Mathankumar, 2014),(Peng, Wang, El-Latif, Li, & Niu, 2012),(F. Liu, Yang, Yin, & Wang, 2014)and(Ibrahim, Al-namiy, Beno,

& Rajaji, 2011) mentioned that F.V biometrics exhibits various characteristics; biometrics information is invisible, difficult to copy, provides high level of accuracy and security moreover, this biometrics information is incomparable between the same fingers of each hand in the same person.

References (Fayyaz, Hajizadeh-Saffar, Sabokrou, Hoseini, & Fathy, 2016), (Pflug, Hartung, & Busch, 2012), (Xi, Yang, & Yin, 2017) and (Raghavendra, Surbiryala, Raja, & Busch, 2014) The motivation for using F.V biometrics is attributed to its natural state, uniqueness, and universality; moreover, F.V biometrics has high spoofing resistance and provides a wide range of advantages, such as (1) suitability and easy to capture, (2) unique personal information and high verification accuracy, and (3) only for live body verification. Moreover, in (Fateme Saadat, 2015) During user registration step, contact with the sensor device is unnecessary; thus, leaving traces in the sensor is infeasible; therefore cannot be traces the user in the future. This fact mean that stealing and forging biometrics information are very difficult. Skin condition is not a hindrance to obtaining a clear image; thus, F.V biometrics is robust against finger surface condition (William et al., 2016) (J. Wang, Xiao, Lin, & Luo, 2015). This biometric have rich piecewise line attributes and are stable to use, which clearly describe F.V for individual verification (Lu et al., 2017). Another feature is that obtaining vein information using artificial vein rather than the natural vein is infeasible because this system depends on the musculature energy (J. Yang et al., 2011). this feature of invisibility provides additional security because patterns are concealed from other individuals or machines compared with other verification technologies; the replication of vein patterns is difficult for an intruder; thus, the F.V biometrics verification system has high resistance to spoofing compared with other biometrics systems (Song et al., 2011) (Raghavendra, Surbiryala, et al., 2014). Where revealed that F.V patterns are captured inside the finger, hence cannot be stolen or forged easily (Huang et al., 2017)(Xin, Liu, Zhang, & Zhang, 2012). The favorable features of the F.V biometrics are its non-intrusive nature and resistance to skin diseases because these diseases cannot affect vein biometrics information during image capture (J. Wang et al., 2015)(L. Yang, Yang, Yin, & Xi, 2014)

There is ability to extract additional biological information from F.V, such as blood pressure, oxygen concentration in the blood, and heart rate, can be obtained. Moreover, human vein texture distribution is permanent from birth and rarely changes during the human lifetime; thus, this security technology is robust and stable (Cheng et al., 2016). The biometrics information is extensively stable (from birth to death), rarely change under any circumstance, located underneath the skin, hence is invisible, and not prone to external distortion, except for cases of deep wounds or intense burns this is reported in (M. Khalil-Hani, Eng, 2010)(Qin & A. El Yacoubi, 2017) . Finally, In the authentication phase, an individual should be present at the location of the sensor device when he/she must enroll his pattern to gain access to a system (Khalil-Hani & Eng, 2011).

1.8 Significance of the Study

We divide the research significance into three, as shown in Figure 1.7, to provide a clear description and identify the importance of this study. A brief explanation is presented in the following paragraphs.

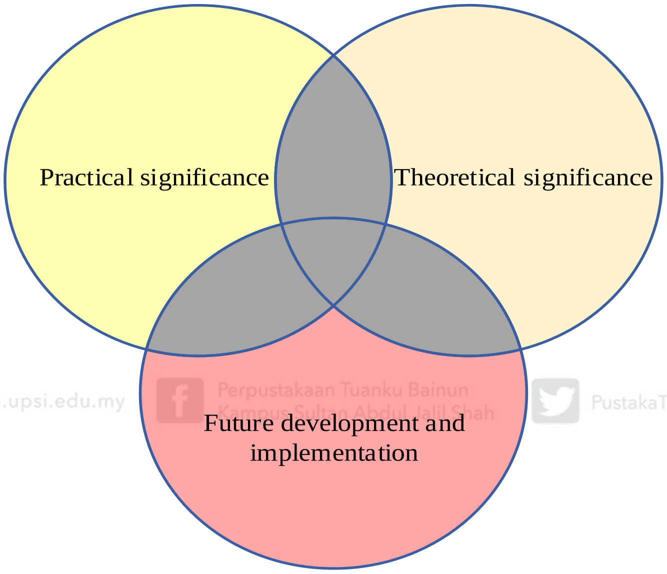


Figure 1.7. Significance of Study Categories

1.8.1 Practical Significance

Biometric technology authentication systems are extensively popular because they provide a high level of security and reliability for individual authentication systems; biometrics are more reliable than traditional technology in security systems used to protect any information or person authentication system (Mohd Asaari et al., 2014) (J. Da Wu & Liu, 2011a). A new secure FV biometric verification framework is proposed in this study. The practical significance is that various organisations in different fields, such as military, financial, medical and customer, can use this technology after the research gap is filled and the weak points are enhanced via the aforementioned solution. Moreover, using an individual's biometrics without his knowledge is difficult. Therefore, FV biometrics is highly reliable for individual verification and has low failure during individual enrolment and verification (Gupta & Gupta, 2015). Furthermore, FV biometric technology will be rapidly developed in various applications that deal with security issues, such as electronic and physical access control, digital rights management, electronic commerce and background checking (Chavez-Galaviz et al., 2015), especially after the challenges of this technology are addressed.

1.8.2 Theoretical Significance

This study follows PRISMA protocol and conducted systematic review that provides an overview of existing FV biometric technology and presented detailed information about FV datasets available for scientific research as shown in Appendix A. It highlights the trend of research work on this topic. Another contribution of this study is the creation of a taxonomy for contacted studies within the scope of the literature review in Chapter 2. The proposed taxonomy introduces several advantages and imposes a sort of organisation on the massive publication by sorting out these works into a meaningful and coherent layout and providing the researchers with important insights regarding the subject field in several ways. Moreover, outlining the potential research directions in the field can help reveal research gaps, and mapping the literature on authentication methods of user verification based on FV biometrics can highlight the weak points. This study serves as a reference on the important requirements that should be adopted to secure individual authentication frameworks.

1.8.3 Future Development and Implementation Significance

The significance of this study in the future concerns the use of the proposed method to secure FV patterns, which can be employed with different types of human biometric verification systems to enhance the level of biometric protection and motivate companies to create small and portable devices (Song et al., 2011). Furthermore, the proposed steganography technique, which is integrated with block chain technology, can be implemented in various fields to address the security problem of sensitive information and network failure case (disaster times) simultaneously. These problems are the critical challenges in various information system environments (Section 5.2).Moreover, this type of biometrics is sufficiently distinctive for verification systems to differentiate amongst individuals and can obtain additional biological information from FVs, such as blood pressure, oxygen concentration in blood and heart rate (Cheng et al., 2016).

1.9 Organization of Research

The structure of this study comprises six chapters, as shown in Figure 1.8. The following discussion presents a brief description of these chapters.

Chapter One: This chapter shows the introduction and research background, providing the reader with an idea regarding the types of human biometrics, especially FV biometrics, and a historical review of this technology. FV biometrics is also compared with other types of biometrics. Moreover, the processing steps in relation to this technology are explained. Next, the research gap, problem and objectives are defined according to the literature review. Furthermore, the relationship amongst the research questions, objectives and problem is illustrated. The scope of this study is also defined using three factors, namely, research method, type and domain. Finally, the motivations and significance of this study are highlighted. Chapter Two: In this chapter, the systematic literature review conducted to determine the research gap is presented. The research problem and challenges are determined, and the existing methods, techniques and datasets are investigated. Chapter Three: This chapter comprises the four methodology phases followed to achieve the research objectives of this study. The proposed phases are implemented as sequential phases, where the output of the first phase is the input of the second phase, and so on. The findings of this study are evaluated in the fourth phase. All these phases represent the recommended solution for the research problem.

Chapter Four: This chapter presents the results and discussion for each part from the proposed FV biometric verification framework. The results of the proposed steganography method are also presented and discussed. Chapter Five: This chapter presents the validation and evaluation of the proposed FV biometric framework. The validation stage is conducted during the discussion of two scenarios, and the evaluation stage is performed through three subphases. Moreover, the related issues are discussed during the evaluation, and the coverage percentage of these issues is comprehensively illustrated by the proposed methods and the corresponding benchmark methods. Chapter Six: This chapter presents the conclusion, contributions and summary of the research goals, contributions and findings. Moreover, the limitation of this study and future research directions are reported.

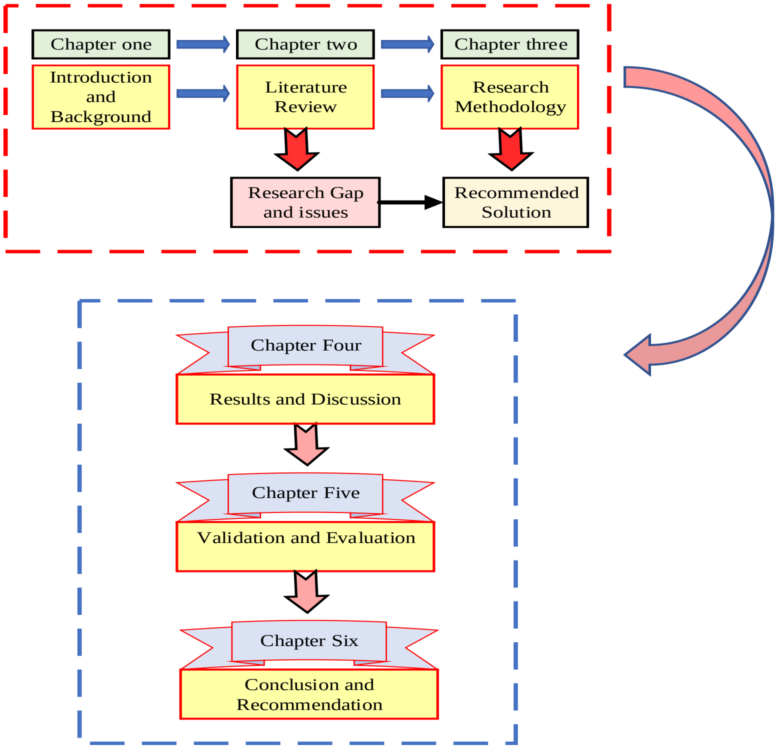


Figure 1.8. Structure of Thesis