

Cancelable biometrics using hand geometry-based steganographic techniques

LP Shahim



orcid.org 0000-0001-6079-7857

Dissertation submitted in partial fulfilment of the requirements for the degree *Master of Science in Computer Science* at the North-West University

Supervisor:	Mr DP Snyman
Co-supervisor:	Prof JV du Toit
Co-supervisor:	Prof HA Kruger

"Make your parents proud, your enemies jealous and yourself happy." - Anon

I would like to dedicate this dissertation to my loving parents and wonderful sister. Without all of you, this would not have been possible. I am extremely blessed to have been given this opportunity.

To my late grandfather, and my namesake, I know you are looking down at me and smiling.

Thank you for all of your love and support. I would have loved to celebrate this accomplishment with you over a whisky.

Lastly, to my Lord God Almighty for the continuous blessings, protection and guidance bestowed upon me. I am eternally grateful.

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. During the study period, parts of the dissertation have been published in a peer reviewed conference proceedings (Appendix A) and a peer reviewed journal (Appendix B). These articles are presented in the format of the publication venue. The contributions of each of the authors are clearly indicated and the contributions of the supervisors were kept within the same reasonable limits as expected for this dissertation. This dissertation was sent for professional language editing in accordance with the University's requirements and the certificate of confirmation follows this declaration.

This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified above, in the text, and Acknowledgements.

Louis-Philip Shahim

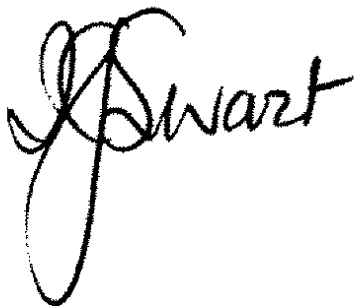
November 2018

This serves to confirm that I, Isabella Johanna Swart, registered with and accredited as professional translator by the South African Translators' Institute, registration number 1001128, language edited the dissertation (excluding the References) with the following registered title:

Cancelable biometrics using hand geometry-based steganographic techniques

by

Louis-Philip Shahim

A handwritten signature in black ink, appearing to read 'J Swart'. The signature is stylized with a large, looping initial 'J' and a cursive 'Swart'.

Dr Isabel J Swart

Date: 13 November 2018

23 Poinsettia Close
Van der Stel Park
Dormehlsdrift
GEORGE
6529
Tel: (044) 873 0111
Cell: 082 718 4210
e-mail: isaswart@telkomsa.net

Acknowledgements

I would first like to thank my supervisor, Dirk. The door to your office was always open, whether I needed help with my research or just to have a chat. You consistently encouraged me to take initiative and make this research not only a reflection of my hard work, but also of my character. I am truly grateful for that.

Thank you to Prof du Toit and Prof Kruger for your constant feedback and motivation. My illustrative example has finally come to fruition.

Endless thanks, from the bottom of my heart, goes to my amazing family. All of those times that I said to you, "I think I've figured it out" actually mean something now.

Abstract

Biometrics have long been used as an accepted user authentication method and have been implemented as a security measure in many real-world systems including personal computers, mobile devices, and physical access control. By encoding a person's physical attributes the disadvantages of traditional password based security, like passwords being lost or stolen, can be overcome. One of the factors that hampers the acceptance of biometric authentication systems is that users have to submit private biometric data to the authentication systems and should these systems be compromised, a digital copy of their biometrics becomes available for exploitation.

The concept of Cancelable Biometrics has to do with the obfuscating of biometric information that is used for biometric authentication, whether the information is in storage or in transit. This ensures that biometric information of a person cannot be reconstructed when it is observed by a third party. With the use of a cancelling technique, one can assure anonymity of users within the system and prevent unauthorised usage of digitised biometric information.

The primary aim of this study was to develop a technique that ensures cancelability of biometrics based on hand geometry information from a *Leap Motion Controller* and steganographic storage techniques. To achieve the primary aim, the following secondary objectives were addressed: i) Perform a literature study to discuss the use and implementation of cancelable biometrics, steganography, hand geometry authentication and the *Leap Motion*

Controller. ii) Design and implementation of the system. iii) Evaluation of the created system using error-based metrics and iterative validation testing.

Based on the recommendations from literature, a biometric authentication system was designed and implemented which uses latent hand geometry information from a *Leap Motion Controller* to construct biometric templates. The cancelability of the biometric templates were ensured by implementing user-specific transforms to the templates and employing steganography techniques for a novel storage solution. The system's performance was evaluated both in terms of the various components that were integrated in the system, and in terms of its overall performance. Even though the *Leap Motion Controller* proved to be an effective an efficient biometric sensor, the use of hand geometry as the source of user biometrics in this context did not exhibit the required level of uniqueness. Given varying levels of tolerance that the system allows for, biometric authentication can still be performed, however, with a trade-off between the true acceptance and false acceptance rates. The negative effect of the tolerance levels were mitigated by introducing a user PIN as a second authentication factor.

Key terms: CANCELABLE BIOMETRICS, INFORMATION SECURITY, LEAP MOTION CONTROLLER, MULTIFACTOR AUTHENTICATION, STEGANOGRAPHY, HAND GEOMETRY.

Opsomming

Biometrie word al vir 'n geruime tyd gebruik as 'n aanvaarde gebruikerverifikasiemetode en word geïmplementeer as 'n sekuriteitsmaatreël in baie regtewêreld stelsels, insluitende persoonlike rekenaars, mobiele toestelle en fisiese toegangsbeheer. Deur persoon se fisiese eienskappe te encodeer kan die nadele van tradisionele wagwoordgebaseerde sekuriteit, soos wagwoorde wat verlore raak of gesteel word, uitgeskakel word. Een van die faktore wat die aanvaarding van biometriese verifikasie belemmer, is dat gebruikers private biometriese data in die verifikasiestelsels moet indien en as hierdie stelsels gekompromitteer word, word 'n digitale kopie van hul biometriese eienskappe beskikbaar vir uitbuiting deur derde partye.

Kanselleerbare biometrie het te make met die verdoeseling van biometriese inligting wat gebruik word vir biometriese verifikasie waar die inligting gestoor word of wanneer die inligting versend word. Dit verseker dat biometriese inligting van 'n persoon nie herbou kan word wanneer dit deur 'n derde party waargeneem word nie. Deur gebruik te maak van kansellasietegniek, kan die anonimiteit van gebruikers binne die stelsel verseker word en die ongemagtigde gebruik van gedigitaliseerde biometriese inligting verhoed word.

Die primêre doel van hierdie studie was om 'n tegniek te ontwikkel wat die kanselleerbaarheid van biometrie, gebaseer op handgeometrie-inligting vanaf 'n *Leap Motion Controller*, verseker en steganografiese stoortegnieke gebruik. Om die primêre doel te bereik, word die volgende sekondêre doelwitte aangespreek: i) Doen 'n literatuurstudie om die gebruik en implementering van kanselleerbare biometrie, steganografie, handgeometrie en die *Leap Motion Controller* te bespreek. ii) Die ontwerp en implementering van die stelsel.

iii) Evaluering van die resulterende sisteem aan die hand van foutgebaseerde metrieke en iteratiewe valideringstoetse.

Op grond van die aanbevelings uit die literatuur was 'n biometriese verifikasiesisteem ontwerp en geïmplementeer wat gebruik maak van latente handgeometriese inligting van 'n *Leap Motion Controller* om biometriese template saam te stel. Die kansellering van die biometriese template is verseker deur gebruiker-spesifieke transformasies op die template toe te pas en steganografiese tegnieke te gebruik vir 'n nuwe stooroplossing. Die stelsel se prestasie is geëvalueer beide in terme van die verskillende komponente wat in die stelsel geïntegreer is, en in terme van die prestasie van die stelsel in geheel. Alhoewel die *Leap Motion Controller* effektief en doeltreffend was as biometriese sensor, het die gebruik van handgeometrie as die bron van gebruikerbiometriese inligting in hierdie konteks, nie die vereiste vlak van uniekheid getoon nie. Gegewe die vlakke van toleransie wat die stelsel voorvoorsiening maak, kan biometriese verifikasie egter steeds uitgevoer word, maar met 'n kompromis wat aangegaan word tussen die egteaanvaardingskoers en valsaanvaardingskoers. Die negatiewe uitwerking van die toleransievlakke op die valsaanvaardingskoers is teëgewerk deur 'n gebruikers PIN as 'n tweede verifikasie faktor in te sluit.

Sluteltermes: KANSELLEERBARE BIOMETRIE, INLIGTINGSEKURITEIT, LEAP MOTION CONTROLLER, MULTIFAKTOR VERIFIKASIE, STEGANOGRAFIE, HAND-GEOMETRIE.

Table of contents

List of figures	xii
List of tables	xiv
List of algorithms	xv
List of abbreviations	xvi
1 Introduction	1
1.1 Contextualisation	1
1.2 Problem statement	3
1.3 Research statement	5
1.4 Aim and objectives	5
1.5 Research method	6
1.5.1 Introduction	6
1.5.2 Interpretivistic paradigm	6
1.5.3 Positivistic paradigm	9
1.5.4 Design science research	12
1.5.5 Reflection	15
1.6 Chapter deployment	16
1.7 Chapter summary	16

2	Related research	17
2.1	Introduction	17
2.2	Biometrics	18
2.3	Cancelability	20
2.3.1	Non-invertible transforms	24
2.3.2	Biometric salting	24
2.3.3	Biometric template attacks	26
2.3.4	Secure hashing algorithm	28
2.4	Steganography	36
2.5	Leap motion controller	40
2.6	Chapter summary	42
3	System design	43
3.1	Introduction	43
3.2	Process overview	43
3.3	System development life cycle - Iterative and incremental model	44
3.4	Proposed framework	48
3.5	System development process	50
3.5.1	Development using the leap motion controller	50
3.5.2	Steganographic development	56
3.5.3	Stego-image contextualisation	61
3.5.4	Random PIN generation	63
3.5.5	Stego-image generation	63
3.5.6	Cancelable biometric development	64
3.5.7	Pseudocode for system algorithm	64
3.5.8	Discussion	66
3.6	Illustrative example	67

3.7 Chapter summary	70
4 Evaluation and data analysis	71
4.1 Introduction	71
4.2 Testing methodology	71
4.2.1 Leap motion controller performance evaluation	73
4.2.2 Comparative vector tolerance	74
4.3 Algorithm evaluation	75
4.4 Overall system evaluation	77
4.5 Discussion	78
4.6 Chapter summary	79
5 Conclusion	80
5.1 Introduction	80
5.2 Research objectives	80
5.3 Contribution to field	83
5.4 Limitations	85
5.5 Future work	86
5.6 Chapter summary	87
References	88
Appendix A SECURWARE2016	93
Appendix B IARIA	99
Appendix C Minimum system requirements	112

List of figures

1.1	Basic authentication process model	2
1.2	DSR Process Model	13
2.1	System structure for biometric authentication	22
2.2	Cancelable biometric system structure	25
2.3	Vulnerability points for biometric system attacks	26
2.4	Conventional image steganography flow	37
2.5	Example of LMC generated hand model	41
3.1	Iterative and incremental model	45
3.2	Requirements	46
3.3	Development life cycle for proposed authentication system	47
3.4	System structure flowchart	49
3.5	LMC device structure and orientation	51
3.6	LMC-presented hand objects during extraction	52
3.7	UML object structure	53
3.8	Example of biometric vector reading and transformation	68
3.9	Randomly generated image versus stego-image	70
4.1	Simulation for time taken to authenticate users	73
4.2	Five second hand scan	74

4.3	Comparative vector tolerance	75
4.4	System tolerance versus acceptance rates	78

List of tables

2.1	Technique vulnerabilities	27
2.2	SHA comparisons	29
2.3	SHA phases	30
2.4	Pre-processing bit block example	33
2.5	Pre-processing bit block divided into 32 bit words	34
2.6	Initial hashes and K-Constants	35
2.7	Steganography methods	38
2.8	Relevant LMC readings	42
3.1	LMC hand object mapping according to infrared scan	53
3.2	Stego-image 1: User IDs vs their pixel correlation (10 IDs x 8 pixels per ID x 5 rows	62
4.1	Randomly-selected data from five-second scan	73

List of Algorithms

3.1	Leap motion controller algorithm to extract hand geometry	54
3.2	Create user hand geometry vector during enrolment	56
3.3	Create stego-image for PINs	57
3.4	Create four-digit user PINs	58
3.5	Create stego-image for users	60
3.6	Generate hash algorithm	64
3.7	Transform algorithm	65
3.8	Pseudocode for system algorithm	65
4.1	Recursive algorithm to find possible vector combinations	77

List of abbreviations

The abbreviations that are used in this dissertation and their descriptions are listed below:

DSR –Design science research

LMC –Leap motion controller

CB –Cancelable biometrics

BCS –Biometric crypto systems

ARGB–Alpha-Red-Green-Blue

RGB –Red-Green-Blue

FPS –Frames per second

PIN –Personal identification number

BBP –Bits per pixel

ID –Identifying number

SHA –Secure hashing algorithm

NIST –National institute of standards and technology

SHS –Secure hash standard

Chapter 1

Introduction

1.1 Contextualisation

The general consensus regarding information security appears to be largely focussed on the technical aspects and approaches to implementing a holistically secure system that caters for any/all breaches (Anderson, 2001). One needs to consider that security within a system has to do largely with what is being protected, as well as what malicious incentives attackers may have for wanting to gain access to information within that particular system. Incentives for attack tend to skew largely in favour of financial gain. However, another common incentive includes supporting an activist approach against organisations by gaining unauthorised access into their information systems and exposing private information to the public. As human beings our innate fear of exposure drives our motivation to protect private information that is directly/indirectly related to us, our family members and/or possessions. In order to achieve this, authentication systems were developed and implemented for information systems.

Within the security field, authentication can occur using knowledge (such as a PIN), physical possession (such as an RFID tag) and biometrics (Liu and Silverman, 2001). Biometric information remains the most personal of assets. By using biometric information to

authenticate users the system removes problem areas such as forgotten passwords and loss of tags etc. The most basic authentication process model can be seen in Figure 1.1 below.

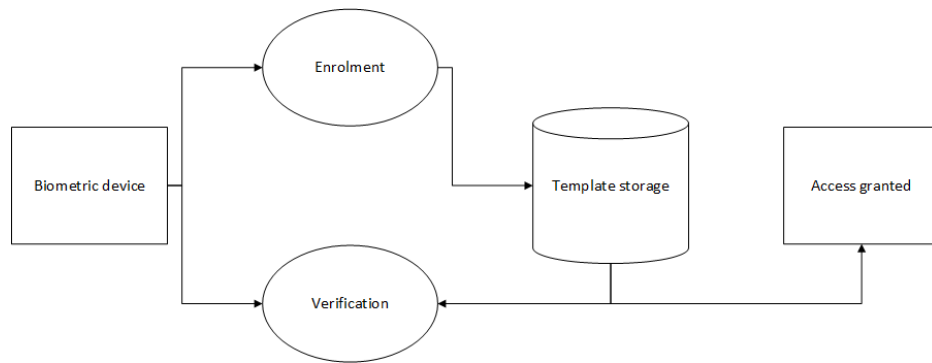


Figure. 1.1 Basic authentication process model

The use of basic authentication systems can almost be classified as defunct, due to the fraudulent attacks becoming more commonplace (Kashyap and Sharma, 2016). It is because of this that researchers are continuously looking for more secure forms of information protection. One of the main disadvantages of basic authentication systems is the vulnerability that occurs in storage and in transit with attackers being able to intercept sensitive authentication information at these critical points. Cryptosystems were thus initiated. A biometric cryptosystem is an implementation technique for authenticating users by incorporating template protection (Uludag *et al.*, 2004). One template protection scheme is known as cancelable biometrics. To classify a biometric template as cancelable, the biometric information should contain various template versions, while simultaneously being computationally irreversible.

The concept of cryptography is predominant in steganography. Steganography is the art of surreptitiously inserting information into multimedia without changing the quality of the said multimedia (Kishor *et al.*, 2016). This brings about the concept of combining cancelable biometrics with steganography. The purpose of this study is to determine whether or not it is possible to improve upon biometric cancelability by using user-specific transforms, along with steganographic techniques to store biometric information.

1.2 Problem statement

Biometrics have long been used as an accepted user-authentication method and have been implemented as a security measure in many real-world systems including personal computers, mobile devices (cell phones and tablets), and physical access control (Liu and Silverman, 2001). By encoding a person's physical attributes the disadvantages of traditional password-based security, such as passwords being lost or stolen, can be overcome (Jain and Boaddh, 2016). One of the factors that hampers the acceptance of biometric authentication systems is that users have to submit private biometric data to the authentication systems and should these systems be compromised, a digital copy of their biometrics becomes available for exploitation (Rathgeb and Uhl, 2011).

The concept of Cancelable Biometrics (CB) has to do with the obfuscating of biometric information that is used for biometric authentication, whether the information is in storage or in transit. This ensures that biometric information of a person cannot be reconstructed when it is observed by a third party (Shahim *et al.*, 2016). With the use of a cancelling technique, one can assure the anonymity of users in the system and prevent unauthorised usage of digitised biometric information. One of the more common methods to ensure CB is known as biometric salting (Rathgeb and Uhl, 2011). Biometric salting entails the introduction of random bits of data into the existing biometric information. Only when the random bits have been removed can the original data be obtained for use in a biometric system. This approach usually relies on a static salting algorithm which can be relatively easily reverse engineered (Shahim *et al.*, 2016). Another approach to CB is presented by Dlamini *et al.* (2016), who posit that one can ensure the protection of user credentials in transit and in storage by using steganography to hide user information in images rather than in commonly used user databases. However, the approach of Dlamini *et al.* (2016) suffers

from the same problem as that of biometric salting where the steganography process may be reverse engineered and biometric information can be reconstructed.

To address these shortcomings, this study will include the incorporation of user biometric information as transform parameters for use in such a steganography engine as implemented by Dlamini *et al.* (2016). This results in a steganography algorithm that encodes a user's biometric information in a picture based on their own unique traits rather than on arbitrary algorithm parameters which may be computationally deduced. The premise is that each set of biometric information is stored in a different manner or location in an image and even when one user's information is identified from the image, the fidelity of other users' information remains intact because the transform parameters are unique to each user. This is opposed to when a common user database is breached and all the users' information contained therein may be exposed. With the combination of steganography and CB this study can contribute to bridging the gap in biometric information storage and use in security systems.

To capture biometric information, Chan *et al.* (2015) present the implementation of a leap motion controller (LMC) to assume the role of a biometric authentication device. This is due to traditional biometric devices (such as fingerprint readers) having a high cost implication. The LMC is a relatively low-cost input device that is usually used for motion control of computer systems. By harnessing the biometric information that is implicitly captured when the LMC is used, biometric authentication can be performed.

This research proposes the development of a novel CB algorithm by employing a steganography approach for the storage and retrieval of biometric user information based on individual users' physical traits where the information is obtained from an LMC. Investigation into the underlying hardware and software topics is warranted to determine the feasibility of these technological aspects before experimental implementation and testing can commence.

1.3 Research statement

Biometric cancelability can be enhanced using user-based transform parameters (obtained from an LMC) for a steganography algorithm that stores biometric information.

In this study, the aim is to justify this statement using this research, development and testing in order to create a system that is capable of achieving the desired result.

1.4 Aim and objectives

The primary aim of this study is to develop a technique that ensures cancelability of biometrics based on hand geometry information from an LMC and steganographic storage techniques. To achieve the primary aim, the following secondary objectives need to be met:

- i. *Objective 1:* By means of a literature review, discuss the use and implementation of cancelable biometrics, steganography, hand geometry authentication and the leap motion controller.
- ii. *Objective 2:* Design and implement an authentication system that utilises the techniques from literature.
- iii. *Objective 3:* Evaluate the resulting authentication system using error-based metrics and iterative validation testing.

These aims and objectives are set out prior to initiating the research process in such a way that the process happens seamlessly. However, one must determine what kind of research needs to be done before the process itself begins. This is discussed in the following section.

1.5 Research method

A research method needs to be selected prior to conducting research in order to maintain a standard that can be justified accordingly. This is regarded as a pattern that a researcher follows throughout the study. This section focuses on differentiating between research paradigms and their respective properties.

1.5.1 Introduction

In this section various research paradigms that were considered for this study are discussed, followed by the chosen paradigm and research method for this study. The following research conducted on the paradigms is predominantly based on Oates (2006). The discussion entails an overview of the design science research method, preceded by a summary of both the interpretivistic and positivistic approaches.

1.5.2 Interpretivistic paradigm

According to De Villiers (2005), interpretivism attempts to discover various, novel manners in which ontological inferences are established due to the time and context of the aforementioned inference.

1.5.2.1 Introduction to interpretivism

According to Oates (2006), interpretivism refers to the researcher's ability to analyse an information system by means of comprehending the processes in its development in terms of social factors. These social factors involve the people that created the systems and the dependencies from a social standpoint in a particular framework. It can, therefore, be concluded that an interpretivistic approach to research is not focused on the proof or disproof of a particular theory. Instead, interpretivism has to do with the identification,

researching techniques and the explanation of the social factors that contribute to holistically understanding a particular social context.

1.5.2.2 Ontology and epistemology

The ontology of interpretivism has to do with being able to comprehend various kinds of opinions and interpretations in an attempt to combine multiple versions of the truth. The researcher should, therefore, accept that his/her own personal perspectives and understanding of the particular topic will contribute to the final results that will be gained from the study. The particular researcher should ensure that he/she possesses a non-neutral perspective in order to interpret the topic in a manner that is influenced by the various social factors.

1.5.2.3 Characteristics of an interpretivistic approach

Since interpretivism does not intend to prove or disprove a particular theory, it can be stated that once a social setting has been critically analysed, a researcher has the ability to illustrate how social factors in the setting are associated and unified. Interpretivistic research paradigms have the following characteristics (Oates, 2006):

- i. Realities that are subjective. The concept of ‘truth’ is based on perspectives and that one researcher’s perception is likely to differ from that of another, simply because of the construction of knowledge that takes place within each of their own minds.
- ii. Volatile construction to meaning based on social factors. The researcher is therefore able to observe the world according to his/her own realities. Information may be subject to change in terms of context, time and culture.
- iii. Non-neutrality. This means that the researcher should maintain his/her right to make assumptions, to enforce his/her beliefs and to act upon these social factors in an attempt to conclude the research. Such research is dependent on the researcher’s personal opinions.

- iv. Analysis of research subjects in their social settings. This means that the researcher attempts to comprehend people in their natural setting rather than creating an artificial setting. This is focused on trying to gain a perspective from the participant within that setting, as well as the observers and to merge the various perceptions using interpretation.
- v. Data analysis using qualitative methods. Within the interpretivistic approach, the preferred data analysis technique is that of a qualitative nature. This involves the use of language, metaphors and imagery to gain multiple results and observations to be interpreted.
- vi. Numerous interpretations. Ultimately, the researcher does not expect to come to one specific conclusion, but rather combine all the extracted information and focus on the results that provide the most powerful evidence. This allows the researcher to interpret bulk quantities of information and finally conclude the study.

1.5.2.4 Interpretivistic critique

Interpretivism involves studying social factors relating to specific social settings and behaviours in that setting. Therefore, interpretivism is an approach to research that involves multiple perspectives and relies on the above critique for the research to be viable rather than basing its credibility on the accuracy of data, like a positivistic approach would.

1.5.2.5 Interpretivistic methods

The methods used in interpretivism include ethnography and case studies. In these methods, it can be assumed that subjectivity is crucial to the research.

- i. Ethnography is successful if the researcher has the ability to successfully understand the activities of humans in interrelated cultures and to comprehend their social settings.

- ii. A case study has the focal point that ensures one specific ‘target’ is examined. This target can be analysed in-depth using various data-gathering techniques.

1.5.2.6 Data-gathering techniques and analysis

Because interpretivistic researchers need to focus on the plausibility of a research topic, the data-gathering techniques are crucial in providing evidence for the conclusions that are drawn by the researcher. This evidence can be regarded as valid if it is obtained using the following techniques (Oates, 2006):

- i. Interviews;
- ii. Observation;
- iii. Document analysis; and
- iv. Field notes.

With the use of these data-gathering techniques and analyses, one is able to justify conclusions based on what is observed at that specific time and in that particular context.

1.5.3 Positivistic paradigm

According to De Villiers (2005), the positivistic approach explicitly proclaims that there is a single reality that is objective, absolute and exists independently of human beings.

1.5.3.1 Introduction to positivism

According to Jakobsen (2013), positivism refers to the positions in philosophy that accentuate both scientific methods, as well as data that is empirical. In Dictionary (2016), positivism is a concept that perceives true knowledge to be that which is directly linked to scientific knowledge, based on what is observed. It is then stated that empiricism is extended in

positivism (Schrag, 1992). It can, therefore, be concluded that a positivistic approach to research is based on empiricism and the use of scientific methods to infer knowledge based on observations that are made once data has been gathered and analysed.

1.5.3.2 Ontology and epistemology

The ontology of positivism has to do with the way in which the world is observed, measured and modelled by a specific researcher. This specific researcher should also ensure that he/she takes a neutral point of view and is objective in his/her approach. With regards to epistemology in positivism, it can be stated that knowledge is classified into two basic forms. These forms include only knowledge that is empirical and knowledge that is logical (Oates, 2006). It can be concluded that with a positivistic approach, the researcher should proceed in a neutral and objective manner while observing the world, using logic and empiricism as a guide for the conducted research.

1.5.3.3 Characteristics of the positivistic approach

Due to positivism being based on a 'scientific approach' to research, the researcher is expected to share a worldview with that of other positivistic researchers. Various assumptions can be made by these researchers that include common characteristics. According to Oates (2006), these characteristics include the following :

- i. Measuring and creation of models. The researcher is able to observe the world and create models of this perceived world according to the 'facts' obtained through scientific methods.
- ii. The objective approach. The researcher should maintain impartiality as an observer throughout his/her research. This research must be independent of the researcher's personal opinions.

- iii. The testing of hypotheses. This refers to the use of empiricism in the testing of various theories or the refuting of these theories.
- iv. Data analysis using quantitative methods. In the positivistic approach, the preferred data analysis technique is of a quantitative nature. This involves the creation of mathematical models to logically and objectively analyse the results and observations.

1.5.3.4 Positivism critique

As positivism involves studying aspects relating to the natural world, researchers who prefer other methods are likely to criticise this technique. Positivism takes a broad approach to research and it cannot always be used to generalise the ontology of things. Thus, there are seldom predictable patterns and that research can evolve around various natural interpretations.

The general method used in the positivistic approach is discussed in the following section.

1.5.3.5 Positivistic methods

One of the methods used in positivism is a scientific method. In this method, it can be assumed that objectivity is crucial in the investigation, and that the world could be viewed as an ordered entity that does not operate in a random fashion (Oates, 2006). With the use of the scientific method, it can be stated that various characteristics of positivism are presented. Such characteristics include reducing problems, repeatability of processes and finally refuting theories. The scientific method uses an iterative cycle which involves the following basic steps to ensure that knowledge is gained in the process:

1. Create a theory from the perceived world;
2. Instantiate an assumption or hypothesis;
3. Use objectivity as a researcher to test the assumption;

4. Analyse the results through observation;
5. Use refutation or confirmation of the given assumption; and
6. Deem the assumption accepted or rejected.

In conclusion, the method used in positivism are structured and involve a set process by stating the research assumption and then either accepting or rejecting the assumption based on objective observation and analysis. Observation and analysis are achieved by means of the following data-gathering techniques.

1.5.3.6 Data-gathering techniques and analysis

Various data-gathering techniques may be used in positivistic research. Such techniques mainly involve experiments. However, other methods, such as sending out of surveys and questionnaires may also be utilised. Once these techniques have been used to gather data, the analysis of this data can then be described as quantitative. The second form of data analysis may be described as qualitative. This involves results obtained from interviews, observed data, narrations and documentation. Qualitative research focusses on data that is not always measurable and includes data such as textual data, images and audio when using techniques such as interviews etc.

In conclusion, these data-gathering techniques include methods such as interviews and surveys with the results being analysed in either a quantitative manner or a qualitative manner.

1.5.4 Design science research

Design science research (DSR) aims to consider artefacts in context and to provide holistic design and investigation on that artefact (Wieringa, 2014).

1.5.4.1 Design science research overview

A general definition for research would be an activity that aids in the detailed comprehension of a specific phenomenon (Vaishnavi and Kuechler, 2015). In contrast to the aforementioned definition, DSR allows for the creation of the phenomenon rather than the understanding thereof. Furthermore, research typically involves the comprehension of a phenomenon and allows the research to make some sort of prediction regarding the phenomenon's outcome to contribute theory of knowledge that is deemed valid (based on knowledge and understanding gained throughout the process). Owen (1998) proposes that through action, knowledge can be generated. Critics occasionally consider this approach to lack in rigour. However, the process is far from unstructured. What differentiates DSR from conventional design approaches is that it targets the unknown areas and explores the problems that may not have been solved yet. This is purely to challenge intellectual risk and to fill the void of missing knowledge in a research community (Vaishnavi and Kuechler, 2015).

1.5.4.2 Design science research process model

The DSR process model is depicted below in Figure 1.2 (Vaishnavi and Kuechler, 2015). This precedes the descriptions of each of the phases in the next section.

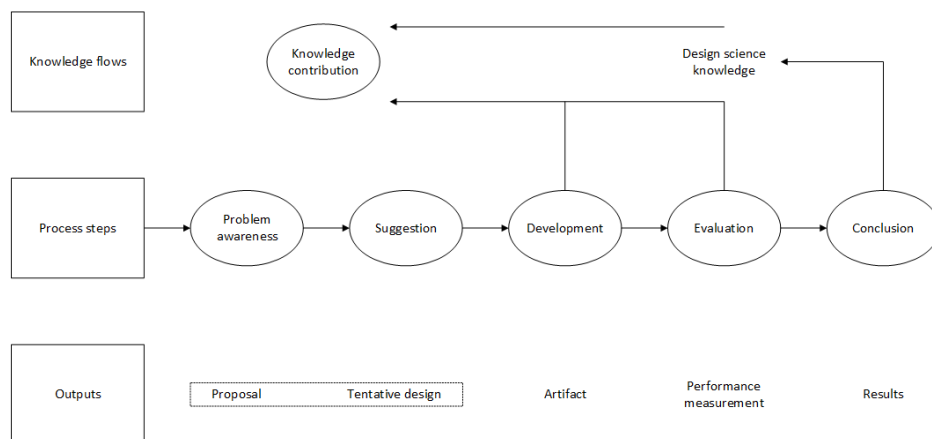


Figure. 1.2 DSR Process Model

1.5.4.3 Phases

When using the DSR process model, it is important to understand the various phases that are associated with the model. These phases will now be discussed.

i. *Awareness of the problem*

To be sufficiently aware of the problem at hand it is the researcher's responsibility to maintain constant and consistent knowledge relating to the problem from various sources (such as in allied disciplines). In this way, the researcher may come across new developments to propose improved approaches. As seen in Figure 1.2, the output for a researcher's awareness to a problem is ultimately a proposal.

ii. *Suggestion*

This is directly linked to the proposal as the researcher creatively displays the envisioned solution to the problem based on the awareness thereof. After having spent a considerable amount of time and effort on sufficiently comprehending the problem, if the researcher fails to produce an idea or design that suffices then the proposal will be set aside, thus possibly saving time that may have been spent on further research and development. This step also cohesively ties into the positivistic approach of materialising the researcher's curiosity relating to the phenomenon at hand.

iii. *Development*

The development phase merely attempts to expand on the tentative design that was created in the suggestion phase. Implementing this phase is strongly dependent on the type of artefact to be produced. The design of the artefact may be a novelty rather than the construction thereof.

iv. *Evaluation*

Once the development of the artefact is complete, a researcher commences with

evaluation thereof. This evaluation is based implicitly on criteria set out in the initial proposal. This phase is crucial to the research because any aberrations from initial anticipations must be carefully noted and thoroughly explained. It is during this phase that this positivistic approach to research statement may be confirmed or acquitted.

v. *Conclusion*

By concluding the study, the researcher typically states whether the results support the hypothesis or 'research statement' to have been accurate and justifiable by proof. These results are strengthened with knowledge gained throughout the research process and confirmed by facts observed throughout extensive studies. By concluding the study, it can be expected that a knowledge contribution be made to the specific research field.

These phases serve as a guideline for the manner in which the methodology relating to this study and its own life cycle from conception until completion progresses.

1.5.5 Reflection

Upon completing the analysis of the previously discussed approaches, it was concluded that this study is positivistic in nature and should follow the DSR method. This can be motivated by the awareness of the problem that exists within biometric authentication systems. This research intends to use that positivistic approach to verify whether or not the suggested solution will be able to enhance biometric cancelability through the development of a biometric authentication system using an LMC and steganographic techniques. Once the development of this system is complete, evaluation thereof will follow and based on the statistical data obtained, the research process can be concluded by determining whether the results justify the hypothesis.

Therefore, due to the nature of this study and the context of the associated problem, a biometric authentication system is designed and developed according to the positivistic paradigm.

1.6 Chapter deployment

In Chapter 2, a literature study is conducted on topics related to the explored problem. Related research is discussed along with the various subsections that relate to the tentative design that was created. These subsections include the concepts of biometrics, cancelability, steganography and the LMC. Furthermore, these subsections include what each element entails, how each works, how each suits this study and finally, how each element is implemented. In Chapter 3, the system design is described with regards to its various elements and the chosen approach for each element is discussed at length. In Chapter 4, experimentation commences by analysing data extraction techniques, as well as testing algorithm efficiency based on extraction, processing and storing biometric information in the suggested system. In Chapter 4, the evaluation of the system based on implicit criteria set out within the proposal and design of the suggested model is undertaken. Finally, the study is concluded in Chapter 5 by justifying the research statement based on results attained.

1.7 Chapter summary

In this chapter, the basic concepts relating to this study were explained. This chapter introduced the purpose of the study, explained what the preliminary aims and objectives are and what research method(s) will be followed. Finally, a brief overview regarding the layout for the remainder of the study, is given.

Chapter 2

Related research

2.1 Introduction

Complex methods are often used in an attempt to rectify basic security aspects that should be prevalent in all authentication systems but are lacking. Biometric information remains unique to each individual and it is for that reason that it should be protected, yet many developers neglect the importance of securing biometrics effectively. Due to this negligence, this research aims to present a novel approach for authentication systems to protect biometric information using a combination of transformation techniques and steganography encryption methods subsequent to the biometric information being captured by a leap motion controller.

In this chapter, an overview of the related topics will be given, followed by their current uses, implementations and relevance to this particular study. These topics include biometrics, cancelability, steganography and the use of a leap motion controller peripheral device. Finally, the chapter will be concluded by coalescing the various techniques to provide theoretical proof of concept for the proposed authentication system.

2.2 Biometrics

Biometrics have long been used as an accepted user authentication method and have been implemented as a security measure in many real-world systems including personal computers, mobile devices (cell phones and tablets), and also physical access control systems (Shahim *et al.*, 2016).

Biometrics are the digitalisation and analysis of a person's innate physical or biological characteristics and the use thereof to distinguish between persons who are to be afforded access to specific systems, information or physical areas (Rathgeb and Uhl, 2011). By encoding a person's physical attributes the disadvantages of traditional password-based security, such as passwords being lost or stolen, can be overcome (Verma and Sinha, 2016). One of the factors that hampers the acceptance of biometric authentication systems is that the cost of the development and implementation has traditionally been high due to factors such as biometric hardware, computational processing power, infrastructure integration, user training, and research and testing (Verma and Sinha, 2016). Furthermore, biometric systems present a unique challenge in terms of user privacy due to the personal nature of the biometric information that is stored in and used by the system (Paul and Gavrilova, 2012).

The cost factor is one that decreases as continued development in the related hardware takes place. Alongside this development of dedicated biometric hardware there is an influx of new augmented computer interaction possibilities (i.e., new and non-traditional ways to control computers). A wide range of technological facets, such as voice, imaging and movement control are receiving considerable attention (Paul and Gavrilova, 2012; Verma and Sinha, 2016). Voice control consists of verifying who the speaker is with the use of voice biometrics. This type of biometric has shown vast improvement recently and is often used to prove that low error rates combined with high accuracy are achievable with its use. Image control typically refers to facial recognition implementations, retina scanners

and/or eye-tracking software that implement infrared imaging. In order to facilitate these interactions, the hardware is implicitly working with information that can be harnessed for biometric authentication. Hardware peripherals (such as the leap motion controller (LMC)) that extend the basic functionality of computers to include support for voice and imaging facets are becoming more commonplace (Rathgeb and Uhl, 2011). These peripherals are even used in biometrics research. For instance, Chan *et al.* (2015) use an LMC for hand scanning and biometric authentication whereby a user would be able to gain access to a system, physical area or information by having his/her hand geometry scanned and analysed. They also posit the use of an LMC in multifactor authentication systems in combination with traditional passwords and PIN approaches. Typically, this type of biometric authentication process follows the protocol of matching prior biometric templates (i.e. digitally formatted biometric features) that are stored in a database to the biometrics that are presented to the system during the biometric scanning process.

This study proposes a system that expands on the existing techniques for biometric authentication with an LMC. This expansion uses techniques from steganography to store binary representations of the biometrics within an image as a biometric template alternative. The system does not merely store the raw biometric data in the image, but rather applies transform parameters to it. Only once the transform parameters have been added to the original biometrics are they stored/matched to authenticate and authorise the user. This ensures that each users' biometric information is neither compromised, nor exposed.

Cancelable biometrics refers to protecting the biometric information from third party scrutiny by obfuscating this information. This addresses the challenge of privacy of biometric information as mentioned above and is discussed further in the next section.

2.3 Cancelability

With the use of authentication systems becoming more prevalent, real-time processing of transmitted information in order to verify a user's identity becomes a primary concern. The authentication process itself in traditional systems has evolved and often resorts to biometric information rather than passwords, tokens and/or secret keys (Verma and Sinha, 2016). This is primarily due to the inability of these traditional schemes to differentiate between an authentic user and an impostor. By authenticating users using biometric information the privacy of biometric data becomes important. Should attackers manage to gain access to the recognition system and its underlying data, the user-specific biometric information becomes readily available for identity theft. A possible solution would be to use multifactor biometric authentication with two or more biometric traits being employed. However, adding more biometric features will only add to the possible losses (should the system be compromised). In the information security industry, one of the long acclaimed benefits of using biometric authentication has been that with post-enrolment biometric templates, user-specific biometric information (matching the stored template) could not be reconstructed. The benefit was refuted and once biometric templates become compromised, the biometric template is rendered useless (Rathgeb and Uhl, 2011). This is because unlike passwords, biometric templates cannot simply be re-assigned due to their unique personal nature. Considering the susceptibility of such biometric authentication systems, an approach to enhance the robustness known as cancelable biometrics (CB) can be used. This approach improves upon standard encryption algorithms that expose biometric templates during the authentication attempt by not supporting the comparison of templates in the encrypted domain (Rathgeb and Uhl, 2011). Simply put, the encrypted domain referred to by CB ensures that data will remain secure in transit and in storage. Furthermore, CB allows for re-issuing and/or regenerating biometric information with a unique and independent identity. This is achieved

by the process of transforming or repeatedly distorting the biometric feature using transform parameters that are predetermined rather than using the original biometric (Shahim *et al.*, 2016). In order to meet some of the major requirements regarding biometric information protection, biometric cryptosystems (BCS) and CB are designed so that biometric features are (Rathgeb and Uhl, 2011; Verma and Sinha, 2016):

- i. Diverse – Unable to be applied in multiple applications;
- ii. Reusable – Reused/replaced in the event of compromise; and
- iii. Irreversible – Computationally challenging to reconstruct the original biometric template, but simultaneously rudimentary to generate the protected biometric template.

Various approaches may be adopted when considering an implementation schema for biometric systems. However, one must consider the alternatives to an approach to ensure that the chosen method is feasible. Both BCS and CB are therefore presented in order to gain an objective understanding. BCSs are systems designed so that digital keys can be directly bound to a particular biometric (Rathgeb and Uhl, 2011). One BCS approach is relevant to this particular study, namely biohashing which implements biometric key-generation. However, Rathgeb and Uhl (2011) state that an implementation should not exist that directly generates keys from biometric templates. They elaborate that biometric features cannot provide sufficient information to reliably obtain lengthy and renewable keys without relying on helper data.

Helper data is public information that is used in the key generation/retrieval process in a BCS (Rathgeb and Uhl, 2011). This is useful to the study because helper data can be used to transform and obscure biometric information. Another approach to BCS is a biometric key-bind cryptosystem. This involves a secret key that relates to a biometric model by using helper data. To successfully implement this approach, facts regarding both the biometric model and the secret key may not be disclosed (Sadkhan *et al.*, 2016). According to Paul

et al. (2014) and Rathgeb and Uhl (2011), implementation of key-binding cryptosystems can occur through a "fuzzy" commitment and a fuzzy vault. The concept of fuzzy incorporates the generation of helper data extracted from biometric features using a secrecy key. The above-mentioned helper data, combined with the secrecy key are then both encrypted and stored in the database. In order to authenticate a user, the helper data then uses the model and biometric features to rebuild the key (Sadkhan *et al.*, 2016). A structural representation of this method can be seen below in Figure 2.1.

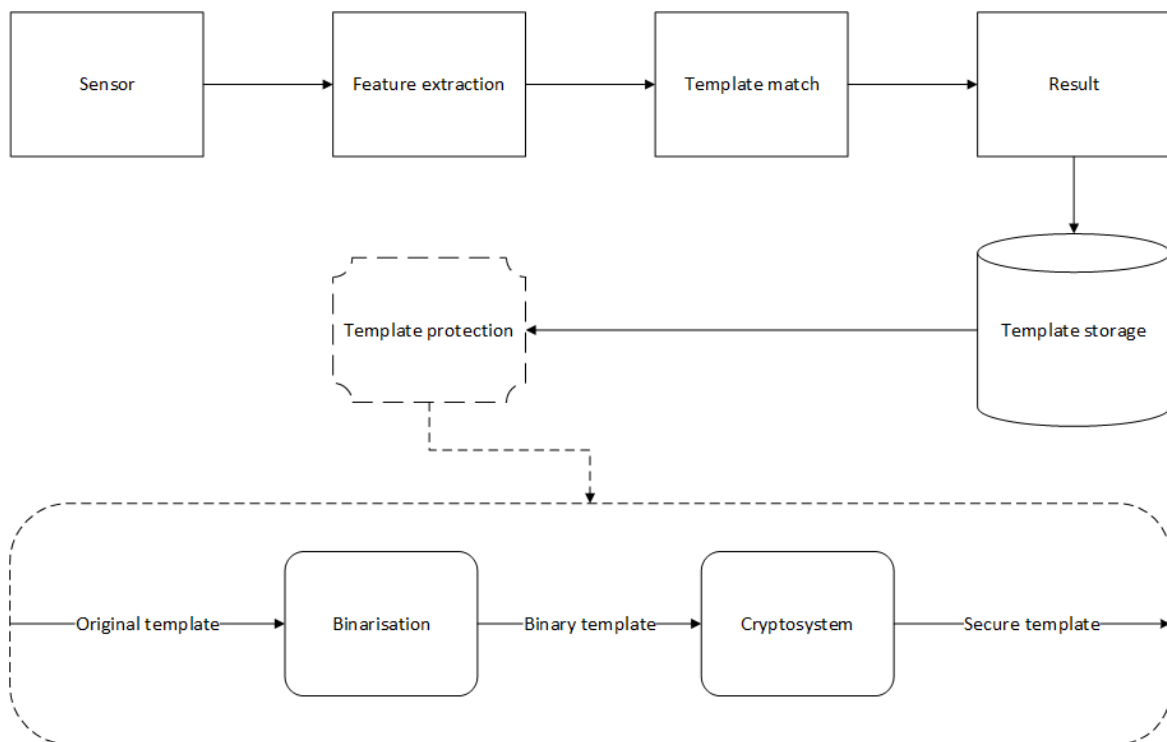


Figure. 2.1 System structure for biometric authentication

Initially, the sensor extracts the specific biometric features from the user (post-enrolment). Once the features have been extracted from the users, the current information in the system is then matched to that of the template that is stored in the database. However, during enrolment of the user in a BCS, the template that was created for each user undergoes a protection process that transforms the template into a secure template. The above-mentioned template-protection process includes the binarisation of the extracted biometric features. Once the

binary template is created, the template is then further processed by the cryptosystem to ultimately generate the secure template. This means that each time the user attempts to be authenticated, the extracted features use the helper data to rebuild the key and match the generated template to the secure template. Finally, if the templates match then the result will be positive and the user will gain access.

Having considered a BCS, one needs to weigh up the options regarding the possible approaches to cancelability and implementations thereof. Cancelability, too, has the sole purpose of ensuring computational challenges when attempting to retrieve/recover the original biometric data by a third party (Rathgeb and Uhl, 2011). The focal point regarding cancelability remains that biometric characteristics should remain innately robust so that even when transform parameters are applied the biometric features do not lose value/individuality. Along with individuality, by transforming biometrics one should ensure tolerance to intra-class variance so that the false rejection rate is not too high.

Another important feature that cancelability has to offer is unlinkability (Rathgeb and Uhl, 2011). This ensures that multiple transformed templates do not reveal any information relating to the original biometrics. In the unlikely event of data compromise, the transform parameters are simply altered which simultaneously implies biometric template updates. With regards to transforms in a CB implementation, two categories are forthcoming, namely (Jain and Boaddh, 2016):

- i. Non-invertible transforms; and
- ii. Biometric salting.

The above-mentioned approaches differ in performance, accuracy and security. Depending on the system that is to be implemented, a weighted feasibility analysis should be conducted on those particular factors in order to select the most suitable approach. These approaches are briefly discussed below.

2.3.1 Non-invertible transforms

This approach involves the use of a non-invertible function that is applied to the biometric template. By applying this function, stored templates can be updated when transform parameters are modified (Piciuccio *et al.*, 2016; Rathgeb and Uhl, 2011). Therefore, security is increased due to the inability to reconstruct the biometric data even though transforms may have been compromised. With this advantage comes an equal and opposite disadvantage, namely a loss of accuracy noticeably decreased a system's performance. This is due to transformed biometric templates becoming laborious in comparison processing, which ultimately provides fewer biometric results to process during matching (thereby influencing the accuracy thereof).

2.3.2 Biometric salting

Biometric salting commonly involves biometric template transforms that are preferred invertible as opposed to the non-invertible approach (mentioned above). The term “salting” refers to the act of merging specific data (such as passwords) with unique random values (“salt”) in order to make all the original data distinct (Syed Ahmad *et al.*, 2012). In this particular context, this technique may be applicable when a four-digit PIN is used as the salt to be combined with the hand geometry vector prior to hashing the combination of data. This means that regardless of what biometric feature vector is chosen, the biometric template extraction cannot be reconstructed to the original biometric template (Paul *et al.*, 2014; Rathgeb and Uhl, 2011). The commands that transform parameters have to remain private. Variations of the approach may appear if user-specific transforms are applied (Teoh *et al.*, 2008). However, this demands that each authentication attempt requires transform parameters which may result in discrepancies if attackers successfully attain transform parameters. Ultimately, a decrease in performance is likely if the system implementation does not contain efficient

biometric algorithms with high accuracy regarding private transform parameters. In contrast to non-invertible transforms, this approach maintains high recognition performance; however, the latter excels in terms of security (Radha and Karthikeyan, 2011; Rathgeb and Uhl, 2011).

According to Rathgeb and Uhl (2011), even though it is more common to adopt non-invertible approaches to system implementation schemes, biometric salting proves superior. Not only does biometric salting increase performance, but in user-specific transform applications one can also improve both security and accuracy by incorporating two-factor authentication.

By taking a closer look at the general structure of using cancelable biometrics it can be seen that during the enrolment phase, the features are extracted, transformed and then stored (Patel *et al.*, 2015). This structure is shown in Figure 2.2 below.

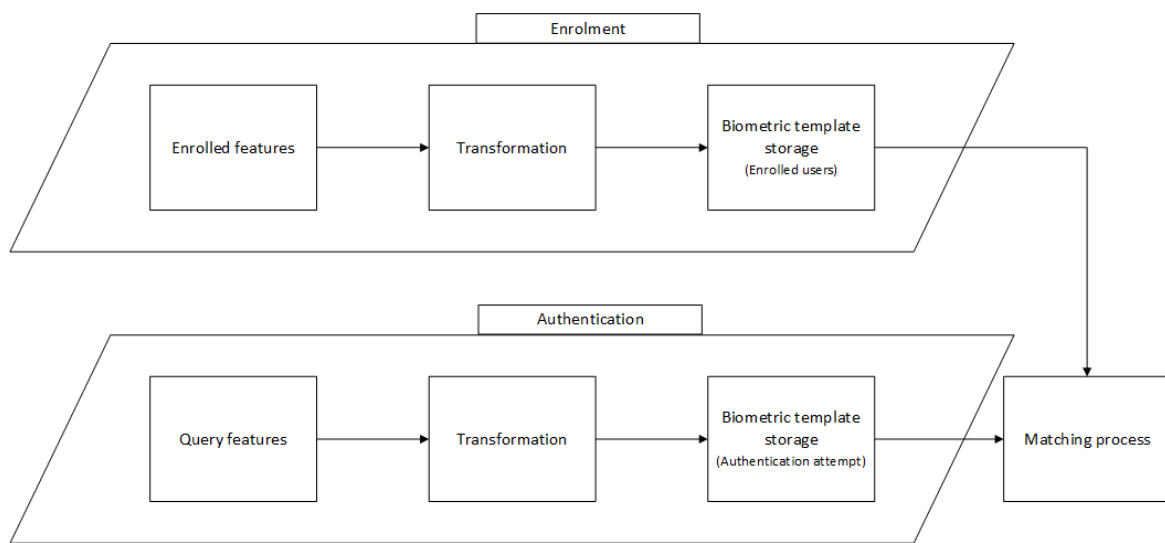


Figure. 2.2 Cancelable biometric system structure

The CB system structure is closely related to that of the BCS structure; however, the fundamental differences between the two are noticeable when attention is given to the timing of template protection. To argue these differences notice that in Figure 2.1 the template protection occurs post-storage, whereas in Figure 2.2 the template protection occurs after the feature extraction and prior to the storage during the transformation phase. Template

protection is crucial in an authentication system with regard to attacks conducted upon the system. These template attacks will be discussed further below.

2.3.3 Biometric template attacks

Conventional biometric systems have been subjected to numerous infiltration attacks that technologies such as BCS and CB appear to have been able to avert (Rathgeb and Uhl, 2011). However, these techniques are known to have vulnerabilities. By analysing the structure of a generic biometric system, one is able to determine which particular processing points are vulnerable to attacks. Figure 2.3 below illustrates some of the above-mentioned vulnerabilities (Patel *et al.*, 2015).

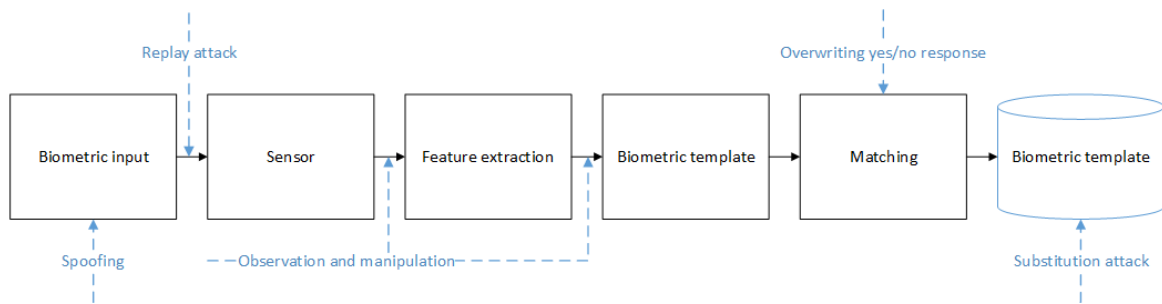


Figure. 2.3 Vulnerability points for biometric system attacks

Research shows that there are numerous vulnerable points to attack a generic biometric system (Ratha *et al.*, 2001). However, an overview of the five points of attack mentioned above in Figure 2.3 is presented as follows (Karimovich and Turakulovich, 2016; Patel *et al.*, 2015; Ratha *et al.*, 2001; Rathgeb and Uhl, 2011):

- i. Spoofing – This type of attack is implemented through the presentation of a biometric to the biometric input (sensor). An example of this type of attack includes presenting a fake finger to the sensor and so forth.

- ii. Replay attack – The use of this form of attack generally involves the resubmission of biometric data that is digitally stored which ultimately bypasses the biometric input device.
- iii. Observation and manipulation – There are two entry points combined for this particular attack. The first entry point would attempt to attack the feature extractor with a Trojan horse in order to produce multiple feature sets that are specified by the attacker. The second entry point attempts to corrupt the manner in which the features are represented (with the assumption that the attacker is aware of the layout produced during feature extraction). Typically, the transition from extraction to matching is seamless, but should this process occur using the Internet, then this attack becomes a real concern.
- iv. Overwriting yes/no response – The process of gaining access to the internal decision module and overwriting the final authentication decision, also called a false acceptance attack.
- v. Substitution – This process is also referred to as a blended substitution attack. During this attack, the stored template is amalgamated with that of the attacker and used to authenticate.

With the above-mentioned potential attacks in mind, the affected techniques and their potential attack formats should be classified. The attacks in correlation to BCS and CB can be seen in Table 2.1 below.

Table 2.1 Technique vulnerabilities

Potential attacks	Affected techniques(s)
Spoofting	BCS and CB
Replay attack	BCS and CB
Observation and manipulation	BCS and CB
Overwriting yes/no response	CB

By considering both techniques and how each technique is vulnerable to diverse forms of attack, it is important to consider how to protect user biometrics against reconstruction. While analysis of template protection schemes is often rigorous, the methods used for biometric feature transformation have not been the focal point of most approaches (Nagar and Jain, 2009). The protection of the user information throughout the use of information remains crucial to this particular system.

In an attempt to meet the requirement of non-invertible transforms, the use of a one-way hash algorithm could be applied to the transformed parameters as a final step prior to the matching process. The chosen algorithm standard will now be discussed.

2.3.4 Secure hashing algorithm

Cryptographic hash functions are designed to block malicious attempts at data modification (Pfleeger *et al.*, 2015). The National Institute of Standards and Technology (NIST), as a part of the U.S. Department of Commerce, is responsible for publishing the Secure Hash Standard (SHS) and is implemented in an attempt to overcome various attacks.

The term Secure Hashing Algorithm (SHA) is used to describe the above-mentioned standard that can be further divided into four specific algorithms, namely SHA-0, -1, -2, and -3. The purpose of such an algorithm is to compute electronic data in a manner that produces a condensed representation of a message (National Institute of Standards and Technology, 2015). The aforementioned representation is commonly known as a “message digest” or “hash.” The length of this message digest remains constant, regardless of the length of the original electronic input data. The algorithmic process that is followed (by all four algorithms as seen below) is one that is both iterative, as well as, unidirectional. By processing electronic data in such a manner, the algorithm ensures the integrity thereof. This is because in the event that the original data should be altered in the slightest, the resulting message digest will be completely contrasting to the message digest of the original data.

To liken the various versions of the SHA algorithms, a further analysis of each of the algorithms in terms of maximum input message size, block size, number of rounds executed and message digest size is presented. The SHA comparisons can be seen in Table 2.2

Table 2.2 SHA comparisons

Algorithm	Maximum input message size (bits)	Block size(bits)	No. of rounds executed	Message digest size (bits)
SHA-1	2^{64}	512	80	160
SHA-2-224	2^{64}	512	64	224
SHA-2-256	2^{64}	512	64	256
SHA-2-384	2^{128}	1024	80	384
SHA-2-512	2^{128}	1024	80	512
SHA-3-256	Unlimited	1088	24	256
SHA-3-512	Unlimited	5761	24	512

It is important to note that prior to this study, the SHA-1 algorithm was broken by Google¹. A hash function is considered broken when two files happen to produce the same hash value (collision). The way in which this particular attack on SHA-1 occurred was through the use of a chosen-prefix attack. Google managed to use a precise piece of data that was injected into one of the files. This caused the files to numerically align during the calculation process (Stevens *et al.*, 2017).

It was decided that SHA-2-256 would be further studied and implemented upon learning of the aforementioned collision and analysis of Table 2.2. Supplementary reasons for this choice include:

- i. SHA-2 is yet to be broken (unlike its predecessors);
- ii. SHA-2-256 has a lower block size than those that follow;
- iii. SHA-2-256 executes 64 rounds of hashing rather than 80; and
- iv. A message digest of 256 bits is produced.

¹<https://www.theverge.com/2017/2/23/14712118/google-sha1-collision-broken-web-encryption-shattered>

Regardless of which SHA algorithm is chosen, the core functionality remains similar in the generation of unique hash values for any input that is fed into the algorithm. Each algorithm can be further divided into two phases, namely pre-processing and hash computations. To better explain the process followed in each of the two phases, see the Table 2.3 below (National Institute of Standards and Technology, 2015).

Table 2.3 SHA phases

Pre-processing	Hash computation
<ol style="list-style-type: none"> 1. Padding a message; 2. Parsing the padded message into m-blocks; and 3. Setting initialisation values for hash computation. 	<ol style="list-style-type: none"> 1. Generates a message schedule from the padded message (along with functions, constants and word operations) to iteratively generate a series of hash values; and 2. Uses the final hash value to determine the message digest.

The entire SHA-2-256 algorithm can be summarised using the following set of equations, where:

a, b, \dots, h = Working variables that are the w -bit words used in hash computation $H^{(i)}$.

$H^{(i)}$ = The i^{th} hash value. $H^{(0)}$ is the initial hash value; $H^{(N)}$ is the final hash value.

$H_j^{(i)}$ = The j^{th} word of the i^{th} hash value, where $H_0^{(i)}$ is the left-most word of hash.

K_t = Constant value to be used for the iteration t of the hash computation.

k = Number of zeroes appended to a message during the padding step.

ℓ = Length of the message, M , in bits.

m = Number of bits in a message block, $M^{(i)}$.

M = Message to be hashed.

$M^{(i)}$ = Message block i , with a size of m bits.

- $M_j^{(i)}$ =The j^{th} word of the i^{th} message block.
 n =Number of bits to be rotated or shifted when a word is operated upon.
 N =Number of blocks in the padded message.
 T =Temporary w -bit word used in the hash computation.
 w =Number of bits in a word.
 W_t =The t^{th} w -bit word of the message schedule.
 $ROTL^n(x)$ =The rotate left (circular left shift) operation.

1.

$$W_t = \begin{cases} M_t^{(i)} & , 0 \leq t \leq 15 \\ ROTL[(W_{t-2}) + W_{t-7} + \sigma(W_{t-15}) + W_{t-16}] & , 16 \leq t \leq 63 \end{cases}$$

2. Initialise the eight working variables, a, b, c, d, e, f, g and h , containing hash values for (i-1):

$$\begin{aligned}
 a &= H_0^{(i-1)}, b = H_1^{(i-1)}, c = H_2^{(i-1)}, d = H_3^{(i-1)}, \\
 e &= H_4^{(i-1)}, f = H_5^{(i-1)}, g = H_6^{(i-1)}, h = H_7^{(i-1)}
 \end{aligned}$$

3. For $t = 0$ to 63:

$$\begin{aligned}
 T_1 &= h + \sum_1^{(256)} (e) + Ch(e, f, g) + K_t^{(256)} \\
 T_2 &= \sum_0^{(256)} (a) + Maj(a, b, c)
 \end{aligned}$$

$$h = g, g = f, f = e, e = d + T_1, d = c, c = b, b = a$$

$$a = T_1 + T_2$$

4. Compute the intermediate hash values:

$$H_0^{(i)} = a + H_0^{(i-1)}, H_1^{(i)} = b + H_1^{(i-1)}, H_2^{(i)} = c + H_2^{(i-1)}, H_3^{(i)} = d + H_3^{(i-1)}, \\ H_4^{(i)} = e + H_4^{(i-1)}, H_5^{(i)} = f + H_5^{(i-1)}, H_6^{(i)} = g + H_6^{(i-1)}, H_7^{(i)} = h + H_7^{(i-1)}$$

To better explain the algorithm functionality, a use-case for this study will be presented using the SHA-2-256 algorithm in the form of a digital representation of hand measurements. These measurements can be summarised in text format as *11, 12, 13, 14, 15*. Each number represents a transformed value for each of the five fingers.

2.3.4.1 Pre-processing

First, each letter will be converted to binary. A one is added to the end to mark the end of the phrase. Next, get the phrase size. In this case, 112 bits. Eight bits per character makes it 112 bits and the rest get padded with zeros to get the block to the correct size.

- i. 11, 12, 13, 14, 15 = 00110001 00110001 00101100 00110001 00110010 00101100
00110001 00110011 00101100 00110001 00110100 00101100 00110001 00110101
(112 bits);
- ii. Add 1 to mark the end of the phrase;
- iii. Pad the message with zeros (375 bits);
- iv. Get the size of the phrase (11, 12, 13, 14, 15) = 24 bits.

Upon completion of the four steps required for pre-processing, a block of 512 bits is formed and is presented in the Table 2.4 below:

The message scheduler needs 64 words to be created from the block, but with each word being only 32 bits long, there is only enough for 16 words.

Table 2.4 Pre-processing bit block example

[illegible]

Equation 2.1 formally describes how to create the other words.

$$\mathbf{ROTL}[(W_{t-2}) + W_{t-7} + \sigma_0(W_{t-15}) + W_{t-16}] \quad (2.1)$$

To get the 17th word, get the word 15 places back, in this case the second word, make two copies of it and right-rotate one of them by seven places. This means each number moves one place to the right, seven times, and when a number falls off the edge, it comes back on the other side. Right rotate the other by 18 places. Then right shift the last copy by three. Right shift means that when a number falls off the edge, it is replaced with zeros on the other side. Do the same for the word two places back, 15th word, except right rotate by 17 and 19 places. Then right shift by 10. Add it to the word 16 places back, the first word and the words seven places back, 10th word. Add all of these together and the 17th word is generated. Proceed like this until there are 64 words.

2.3.4.2 Hash computation

The last part of the algorithm (step 3) uses the eight initial hash values and the 64 constant values. By converting between base 2 and base 16 is ultimately what produces the complex final signature. Table 2.6 illustrates the aforementioned conversions with the final signature.

Table 2.5 Pre-processing bit block divided into 32 bit words

1.	00110001001100010010110000110001
2.	00110010001011000011000100110011
3.	00101100001100010011010000101100
4.	00110001001101011000000000000000
5.	00000000000000000000000000000000
6.	00000000000000000000000000000000
7.	00000000000000000000000000000000
8.	00000000000000000000000000000000
9.	00000000000000000000000000000000
10.	00000000000000000000000000000000
11.	00000000000000000000000000000000
12.	00000000000000000000000000000000
13.	00000000000000000000000000000000
14.	00000000000000000000000000000000
15.	00000000000000000000000000000000
16.	000000000001100010011000100110010

To get T1, use the value of e and create three new words by right rotating by six, 11 and 25. Then do an XOR on these values. Then run the Choose function of e, f and g . Get the first K constant, the value of h and the first word from the message scheduler and calculate the AND of all of these.

To get T2, run the Majority function over a, b and c . Then create three new words by right rotating a by two, 13 and 22. Then get the XOR of all of these and swap and modify the values as seen in the function.

This process is then repeated 64 times.

Lastly, AND the initial values for the hashes to the corresponding final values and concatenate them all together to produce the final message digest.

$$H_0^{(N)} || H_1^{(N)} || H_2^{(N)} || H_3^{(N)} || H_4^{(N)} || H_5^{(N)} || H_6^{(N)} || H_7^{(N)} \quad (2.2)$$

Table 2.6 Initial hashes and K-Constants

Initial hashes	K-Constants
H(0)=6a09e667	428a2f98 71374491 b5c0fbcf e9b5dba5 3956c25b 59f111f1
H(1)=bb67ae85	923f82a4 ab1c5ed5 d807aa98 12835b01 243185be 550c7dc3
H(2)=3c6ef372	72be5d74 80deb1fe 9bdc06a7 c19bf174 e49b69c1 efbe4786
H(3)=a54ff53a	0fc19dc6 240ca1cc 2de92c6f 4a7484aa 5cb0a9dc 76f988da
H(4)=510e527f	983e5152 a831c66d b00327c8 bf597fc7 c6e00bf3 d5a79147
H(5)=9b05688c	06ca6351 14292967 27b70a85 2e1b2138 4d2c6dfc 53380d13
H(6)=1f83d9ab	650a7354 766a0abb 81c2c92e 92722c85 a2bfe8a1 a81a664b
H(7)=5be0cd19	c24b8b70 c76c51a3 d192e819 d6990624 f40e3585 106aa070
	19a4c116 1e376c08 2748774c 34b0bcb5 391c0cb3 4ed8aa4a
	5b9cca4f 682e6ff3 748f82ee 78a5636f 84c87814 8cc70208
	90befffa a4506ceb bef9a3f7 c67178f2

An example of a message digest can be seen when hand geometry measurements that have undergone transforms produce an initial output (prior to hashing) of:

11, 12, 13, 14, 15

By using the SHA-1 hash algorithm, one sees a message digest (160 bits) of:

b4bf77f04af433a2ed748a44760f043acec04e35

With the same input string, using SHA-2-256 one sees a message digest (256 bits) of:

2c72ea316fc05ec89ede357ebe416fb80214396889462c07546978c18445310d

Ultimately, this message digest would then be stored rather than the plaintext of the original data.

To conclude this subsection, the aim is to combine the key-binding capabilities of a BCS, the secure hashing algorithm and the biometric salting of CB. Once the user-specific biometric information has been transformed and is secure, it is ready for storage. In order to store this sensitive biometric information, rather than using a conventional database (due to its vulnerabilities, i.e. username/password exploits) a technique known as steganography was utilised and is described in the next section.

2.4 Steganography

According to Kishor *et al.* (2016), secret information is hidden using a type of communication known as steganography. This is done through the use of multimedia files in conjunction with secret keys to embed information in these multimedia files. Steganography came about when it was realised that cryptography itself was incapable to securely transmit various forms of information across the Internet (Jain and Boaddh, 2016). The word steganography can be translated from Greek into “covered writing” (Pandit and Khope, 2016). When hiding sensitive information, the information in question is typically concealed using an alternative format to that of its original. This is done through regeneration of data using multimedia formats. Some of these formats include text, image, audio and even video. For the purposes of this particular study, focus will be maintained upon image steganography and the shrouding of sensitive biometric information by means of bit encryption in an image as the cover object. While cryptography disguises only the meaning of a message using code, steganography aims to hide the entire message from possible attackers (Kishor *et al.*, 2016; Pradhan *et al.*, 2016).

The conventional flow of image steganography (as seen in Figure 2.4) follows a combination of encryption and decryption (just as cryptography does), but aims to use a confidential communication channel while secretly storing data and protecting the alteration of that data. An application that also makes this technique crucial to this particular study is the use of steganography as a conventional database alternative (Pandit and Khope, 2016).

In image steganography, both the encryption process and the decryption process involve the use of a cover image and a stego-image. In short, the difference between the two is merely that the stego-image contains the sensitive information, while the cover image can be seen as an empty data storage location for the sensitive information. In Figure 2.4, the steganography process requires sensitive information that is to be stored within the cover media (in this case,

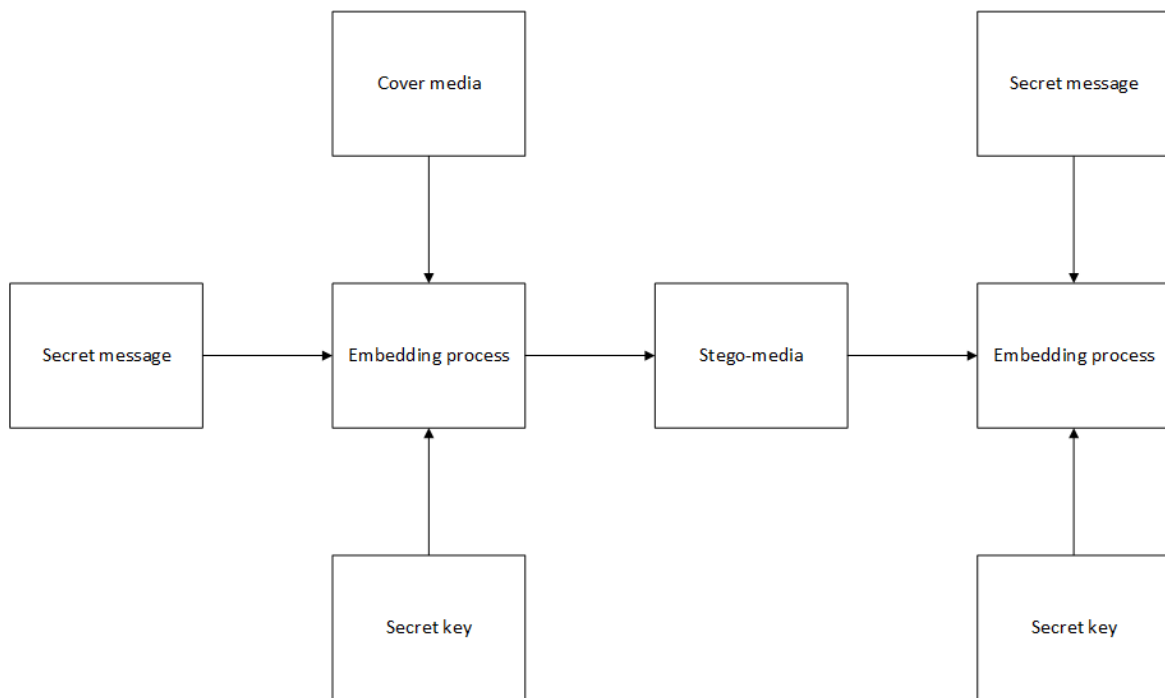


Figure. 2.4 Conventional image steganography flow

the image). This sensitive information is embedded into the image with the use of a secret key and a cover image in which to hide the information. With the embedded information, the image is then referred to as the “stego-image.” The sensitive information can then only be extracted if the secret key is known. Steganography can be implemented in various ways.

However, the two major techniques that will be discussed regarding image steganography involve the following (Paul and Gavrilova, 2012; Pradhan *et al.*, 2016):

- i. Spatial domain technique; and
- ii. Transform domain technique.

The main difference between the two techniques is that when implementing a spatial domain steganography, the pixels in the image are directly manipulated. This is juxtaposed to the transform domain steganography that uses distinct transformations to allow image transformation in the transform domain and then only is the sensitive information stored with the image (Pradhan *et al.*, 2016; Roy and Changder, 2016).

Literature broadens the scope of steganography even more in stating that spatial and transform domain techniques branch out into subcategories of implementation (Radha and Karthikeyan, 2011; Syed Ahmad *et al.*, 2012; Verma and Sinha, 2016). A few examples of these methods can be seen in Table 2.7.

Table 2.7 Steganography methods

Spatial Domain	Transform Domain
Least Significant Bit substitution	Discrete Cosine Transform
Pixel Value Differencing	Discrete Wavelet Transform
Random pixel selection	Discrete Fourier Transform

The purpose of modern steganography is to allow the host image protection so that the image itself, as well as the sensitive data it holds may not be recovered from the stego-image. By achieving this, the technique implemented is classified as irreversible steganography. The aforementioned objective is typically partnered with the ability to conceal sensitive information in a natural image in such a way that distortion of that image is minimal.

It is important to maintain that this particular study focusses on cancelable biometrics being stored using steganography techniques. This implies that, for the purposes of this

research, the image may be distorted without it being an issue because even if an attacker manages to access the stego-image, he/she should not know what type of information is being stored, nor how to recover to biometrics after the transforms.

According to Jain and Boaddh (2016) and Pradhan *et al.* (2016), steganography techniques are evaluated using various criteria. However, evaluation criteria that are relevant to this particular study are the following:

- i. Hiding capacity – This is the maximum amount of data that can be stored in an image with reference to bits per pixel (bpp). Comparatively speaking, a larger hiding capacity means the steganography technique is better.
- ii. Security Analysis – The technique should be able to withstand attacks on the image that include any attempt to alter the image.
- iii. Robustness – By being robust against attempts to attack the image statistically, as well as image manipulation attacks, the technique alone provides protection to the sensitive information hidden in the image.
- iv. Computational complexity – With an algorithmic implementation, it is always important to take the time and space complexity into consideration.

An image can be seen as a two-dimensional function, where the $F(x, y)$ is the image pixels that can be represented as a grid. Each pixel contains ARGB (Alpha-Red-Green-Blue) values. Alpha values represent the pixel's opacity and RGB values represent a particular colour in the colour system. These ARGB values range from (0, 0, 0, 0) to (255, 255, 255, 255). To embed data, one can either store information sequentially or randomly among various image pixels using the $F(x, y)$ grid layout. By using sequential embedding of data one makes the data more susceptible to steganalysis detection by clustering the sensitive information in the image grid (Laskar and Hemachandran, 2013). Randomly embedding data complicates the detection process by scattering the data using a random number sequence.

The proposed system aims to use steganography techniques in the storage and obscuring sensitive biometric information in an image or images once the biometric information has been transformed using CB techniques. In the next subsection, the means by which biometric information will be extracted using an LMC as the biometric scanner will be discussed.

2.5 Leap motion controller

With the LMC's advanced hand- and finger-tracking capabilities, the position, velocity and orientation of all ten fingers, supplemented by hand geometry information, are reported upon with accuracy and low latency (Syed Ahmad *et al.*, 2012). Chan *et al.* (2015) presented the implementation of an LMC to assume the role of a biometric authentication device by harnessing the above-mentioned information. The low-cost factor of this device makes this implementation even more favourable in situations where cost is of substantial concern. One drawback of this approach is that the LMC is a peripheral device that still requires a computer system to connect it to as the device cannot function in a stand-alone way. This disadvantage will add to the associated cost of implementation.

The LMC is able to scan a human hand at approximately 100 frames per second (FPS). With the use of an LMC it is possible to extract all finger/bone measurements of any given hand during an infrared scan. Any given combination of these measurements should be unique to every person (Chan *et al.*, 2015). As seen in Figure 2.5, a model of the hand is then created based on the readings taken by the LMC.

Information retrieved from the hand scans are summarised in Table 2.8. The LMC is capable of acquiring numerous metrics relating to any presented hand. A combination of Figure 2.5 and Table 2.8 provides an overview of the metrics that are relevant to the proposed system. The measurements i-iv can be further explained as the acquired lengths and widths of each of these bones.

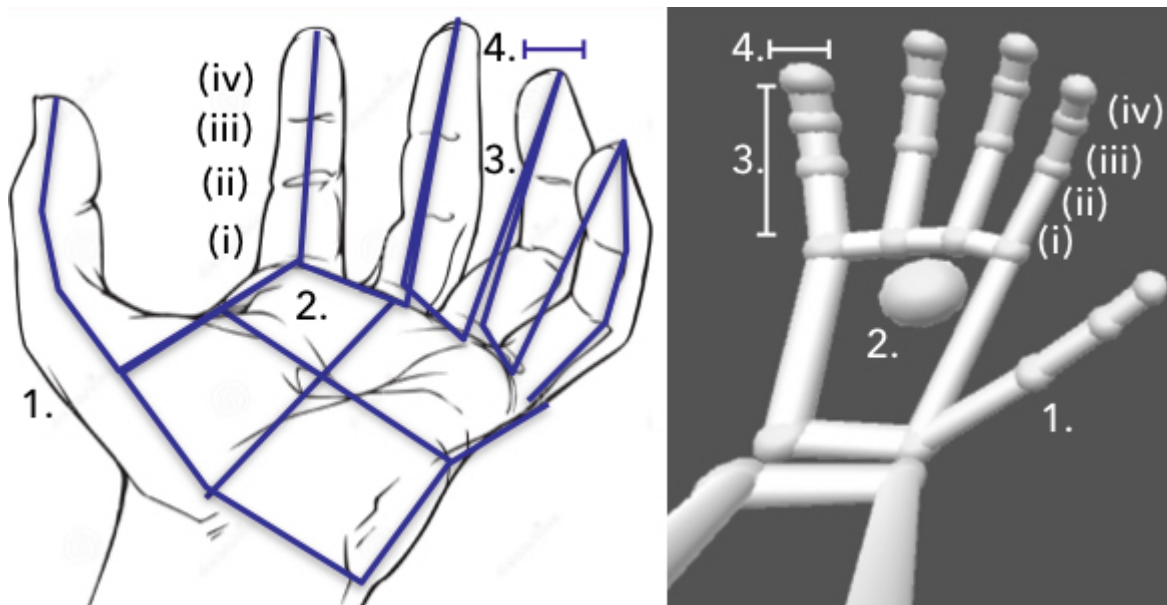


Figure. 2.5 Example of LMC generated hand model

All the above information becomes relevant when attempting to authenticate users based on their hand geometry. Although the LMC maintains great accuracy when gathering information regarding the presented hand, the readings tend to differ depending on the position of the hand in relation to the LMC device itself. The readings show minimal discrepancy (see Chapter 4); however, this could become an issue when statistically analysing the false acceptance rate and false rejection rate of the final authentication system (Nagar and Jain, 2009).

While scanning the hand using an LMC one can vary the length of the scans to acquire a larger data set for each user reading during the enrolment and storage phase. This allows for the system to iterate through the hand and its 19 bones (three bones per finger, except for the intermediate bone which is non-existent in the thumb) in the fingers and retrieve the lengths of each of those bones.

With the use of an LMC, features can be extracted from presented hands, transformed to implement CB and stored using steganography techniques. A proposed framework to implement such a system is discussed in the following section.

Table 2.8 Relevant LMC readings

Readings	Bone
1. Left/Right (Hand)	(i) Metacarpal
2. Palm Width (Hand)	(ii) Proximal
3. Length (Fingers)	(iii) Intermediate
4. Width (Fingers)	(iv) Distal

2.6 Chapter summary

The aim of this chapter was to provide sufficient background and insight into the various techniques that are to be used throughout the implementation of the cancelable biometric authentication system. The concepts and techniques that were explained are used in the chapters that follow. Cancelable biometrics (along with the secure hashing standard), steganography and the use of the leap motion controller were explained with comparisons between different implementations thereof. This was done in order to select the best suited method that combines all the techniques in a manner that achieves secure storage of users' hand geometry by using steganography. Chapter 2 serves as a basis for the decision-making process prior to the system implementation and offers the necessary literature to support the chosen techniques.

Chapter 3

System design

3.1 Introduction

The literature and background described in Chapter 2 are used as a basis for the decision making throughout the design and development phase of this cancelable biometric authentication system. In order to successfully implement a biometric authentication system, there are various fundamental characteristics that need to be taken into consideration. With these characteristics in place, one is only then able to amend the necessary techniques of cancelability and steganography in an attempt to provide a suitable working model for testing and evaluation.

In this chapter, the process followed during the design and development of the cancelable biometric authentication system and how the various techniques were implemented in this particular study are provided.

3.2 Process overview

Due to the nature of the study, it is necessary to ensure that the development of the cancelable biometric authentication system should follow certain protocols that pertain to the techniques

of cancelability and steganography. The relevant knowledge acquired by means of the literature review (Chapter 2) clarified the manner in which the system would be developed. During the design and development phase of this system, various increments occurred to allow for the continuous integration of the vast features correlating to each individual technique. Thus, the system development adopted the iterative and incremental model. This model and the aforementioned increments will now be discussed in more detail.

3.3 System development life cycle - Iterative and incremental model

This approach methodically attempts to develop software by gradually increasing functionality through planning multiple increments that produce deliverables. Each deliverable produced should ultimately contribute to the completed system (Anonymous, 2017).

By using this method, the proposed authentication system was initiated through the use of a detailed planning process that involved mapping out the various goals for each increment of development. The goals for each increment included appending functionality to the previous increment. It was determined early on that by reaching these smaller goals and ensuring that the system functionality for each increment was met, the final system integration would be simplified. The holistic approach is important when developing a system using multiple increments. Due to the nature of the requirements that were set out in the early stages of research, the final authentication system would have to be constructed. As indicated in Chapter 2, various techniques are required to function as expected to in their own regular circumstances before they can be implemented, tested and integrated to the final system. The iterative and incremental model is one that is based on producing deliverables. To illustrate the planning that went into the development of this final system, Figure 3.2 is presented and discussed.

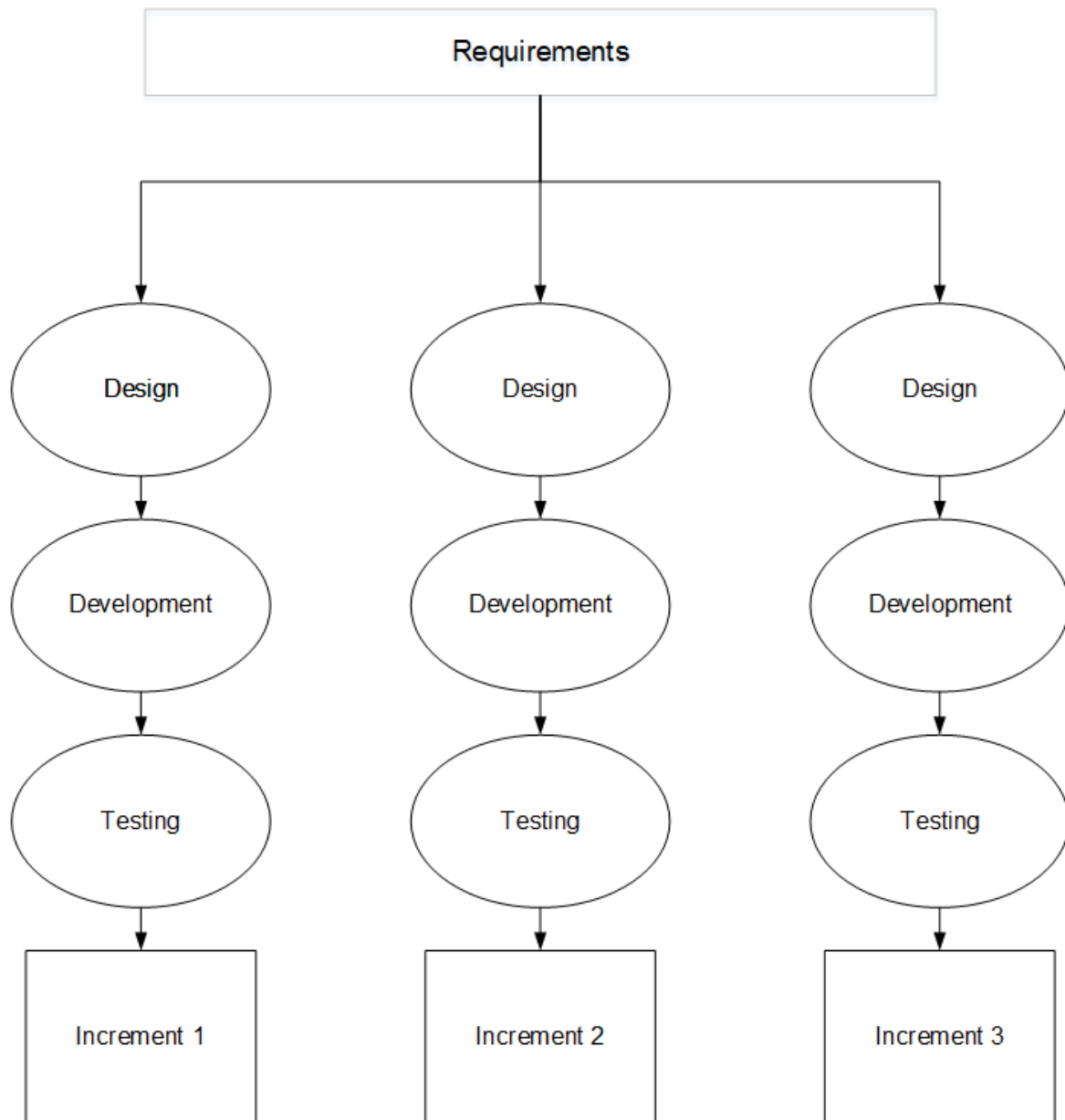


Figure. 3.1 Iterative and incremental model

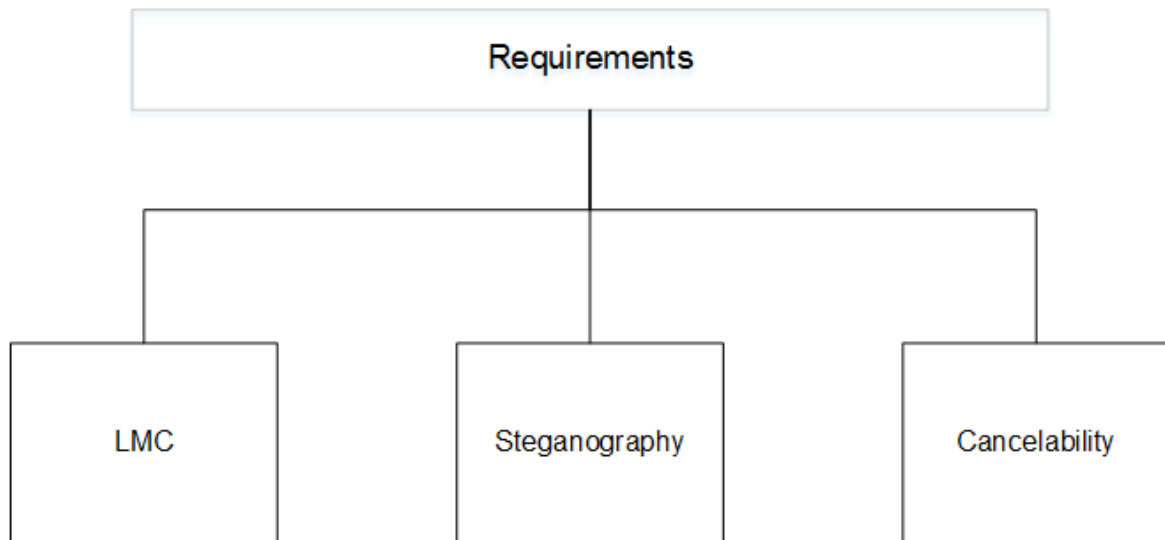


Figure. 3.2 Requirements

The way in which the requirements for this project were setup and maintained was largely determined with the final system in mind. From the inception of this study, it was decided that the final authentication had to function in the following ways:

- i. By using an inexpensive, functional peripheral device and an authentication sensor to provide a user-friendly and affordable alternative solution to biometric readers;
- ii. The system would have to use a novel approach to storing biometric information obtained from the aforementioned sensor; and
- iii. Due to the novelty of the biometric storage, the system users' biometrics should not be vulnerable to impersonation attacks.

With the functionality of the final authentication system established, the increments for the development phase became apparent. As seen in Figure 3.3, the increments for the project would evolve around meeting three main requirements, namely:

- i. Use the leap motion controller as the authentication sensor and ensure that it can read user hands efficiently and accurately;

- ii. Apply steganographic techniques as a storage mechanism for the biometric reading provided by the leap motion controller; and
- iii. Ensure that the users' original biometric readings are safely stored using the aforementioned CB techniques and that they are mathematically irreversible (as seen in Chapter 2).

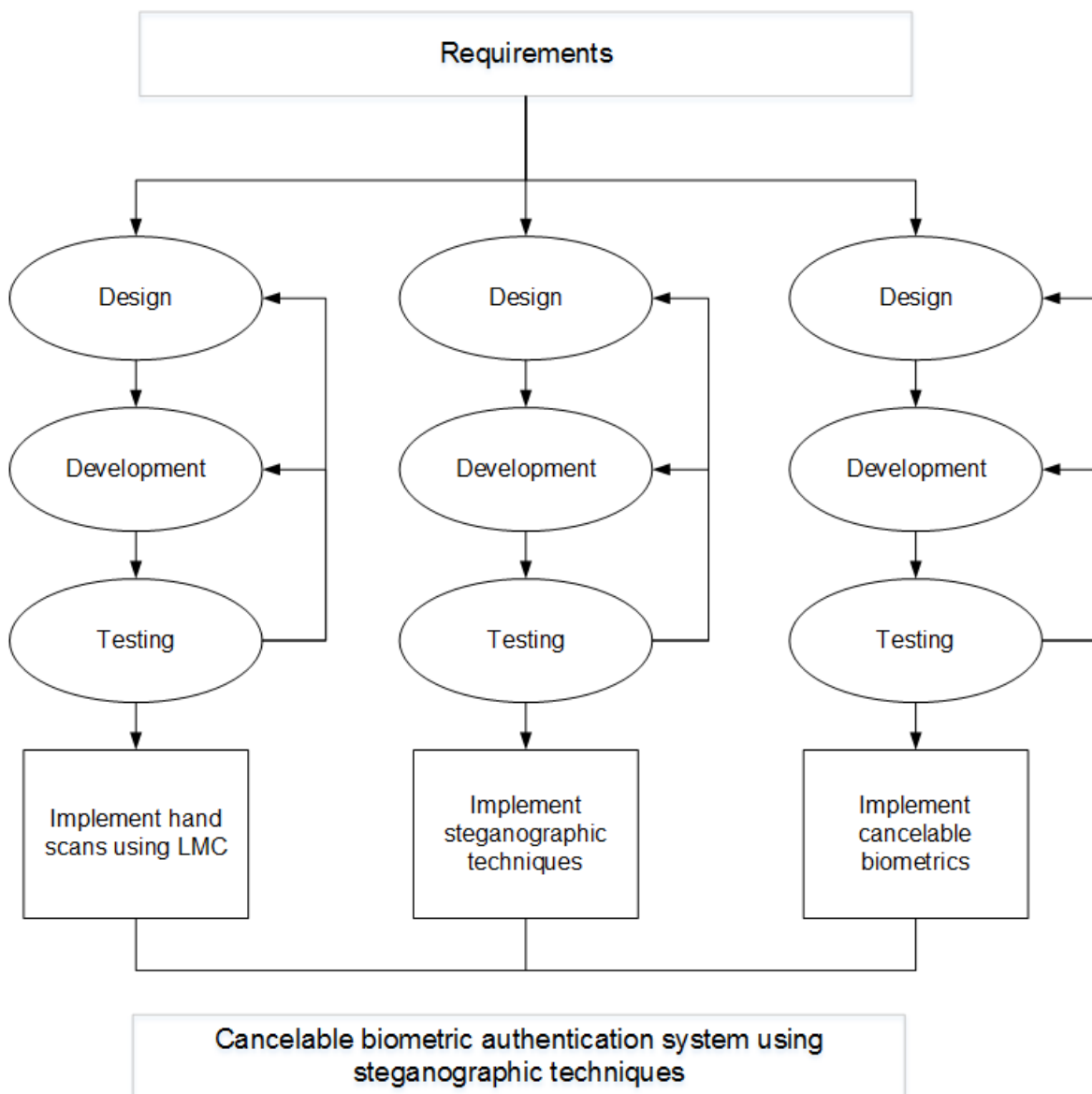


Figure. 3.3 Development life cycle for proposed authentication system

The development process will be discussed in more detail regarding each increment and its iterations. By using these requirements to guide the development process, the first increment was instantiated by attempting to learn how the leap motion controller can be used to extract more information regarding a user's hand. For this, the developer documentation ¹ was consulted regarding the setup thereof.

3.4 Proposed framework

The prevailing architectures of biometric authentication systems consist of two main phases. These phases involve enrolment and authentication. The reason these two phases are required is so that during the authentication phase, the system has a stored biometric to compare to the biometric currently being presented to the system. This comparative biometric is typically referred to as a biometric template. During the enrolment phase, the biometric template is created for the user and then stored in a database. The manner in which the biometric template is created consists of several images being taken of the hand and then algorithmically extracting features from those images to create a final model for the specified user (Varchol and Levick, 2007). This entire enrolment phase can be simplified through the use of an LMC due to its ability to extract hand features from the internal LMC hand model that is created upon presentation of the hand. In order to comply with CB practices, this hand model has its features transformed mathematically, such that the original biometric information is not used in the transit/storage processes. The authentication phase simply compares the presented hands' extracted features to those of the models in the database. This authentication process would, therefore, also need to transform the presented biometrics in order to match it to the stored model.

Figure 3.4 represents the information (system structure) flow in the authentication system. The LMC initiates the information flow for the system when the hand is presented and

¹<https://developer.leapmotion.com/documentation/>

immediately extracts features therefrom. Once the features are extracted, they can be transformed mathematically allowing for the enrolment phase to commence. In an attempt to further secure the biometric information, the decision was made to implement two-factor authentication. This is done by issuing a four-digit PIN to each new user that is enrolled into the system. For implementation purposes, the use of four-digit PINs allows for a maximum unique user capacity of nine thousand users (randomly generated and numbered from 1000 to 9999). The issued user PIN will determine where in the stego-image the biometric information is stored. By taking this approach, the system is then able to use two different images for storage (one for PINs and one for the biometrics).

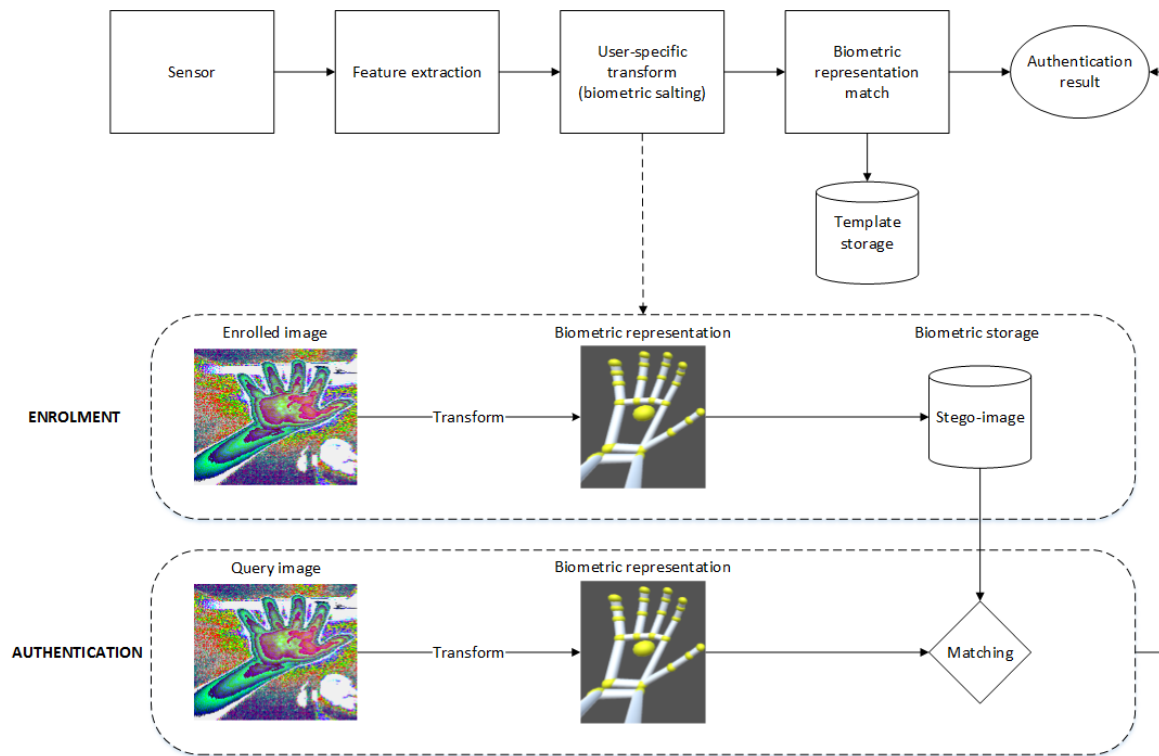


Figure. 3.4 System structure flowchart

In order to generate stego-images for sensitive information storage, one needs to specify exactly what images comprise of, how they are processed and how to programmatically generate them.

3.5 System development process

In the next section, an attempt is made to outline the process that was followed throughout the development of the proposed framework for the biometric authentication system. This is based on the objectives mentioned in Chapter 1, as well as the iterations mentioned earlier in this chapter.

3.5.1 Development using the leap motion controller

As seen in Figure 3.4, the overall system structure flow is initiated through the feature extraction through the use of a sensor. In this particular study, the sensor refers to the leap motion controller. To successfully extract features from the user, the LMC needs to be set up according to the particular environment that will be used throughout the development.

The environment chosen for the study was based on prior knowledge, the level of support documentation provided by Leap Motion and available resources in order to minimise the amount of time taken to learn and adapt to novelties.

3.5.1.1 Leap motion controller development environment

In order to reiterate the manner in which the LMC functions, one should refer to the API documentation for reference. For the purposes of feature extraction regarding the peripheral device, the hand detection can be summarised as follows:

Distances recorded by the LMC are measured in millimetres. To successfully extract accurate measurements pertaining to each individual hand that is presented to the LMC a Cartesian coordinate system is employed. This particular coordinate system manages to specify the various planes associated to the X-, Y- and Z-axis with regard to their orientation relative to the LMC device. This can be seen in Figure 3.5².

²<https://developer-archive.leapmotion.com/documentation/csharp/devguide/Leap-Overview.html>

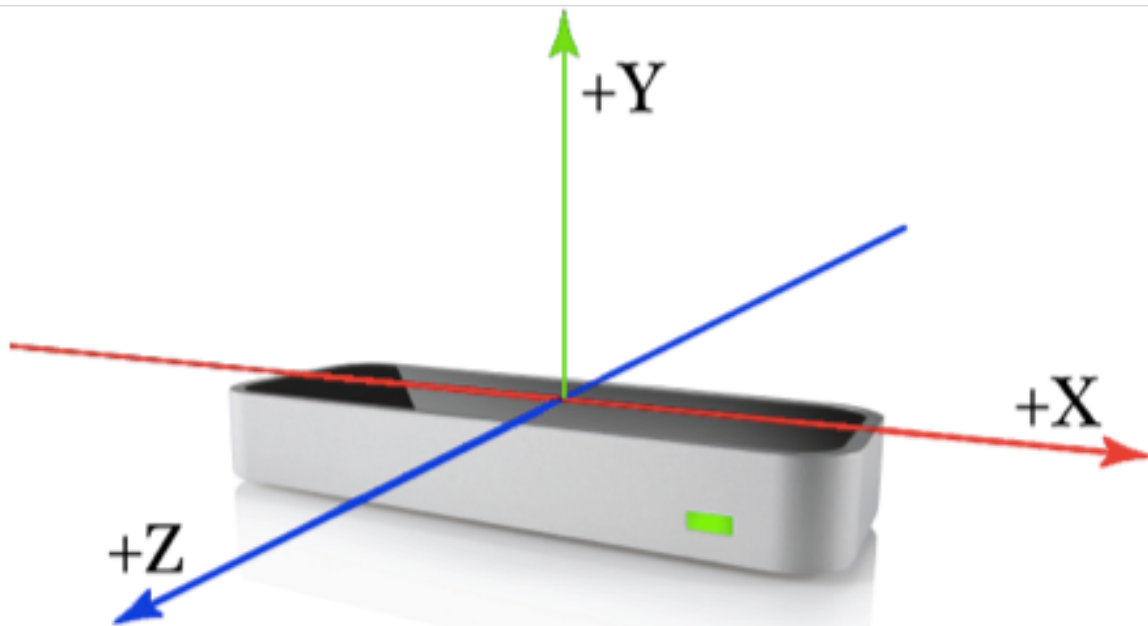


Figure. 3.5 LMC device structure and orientation

The LMC generates infrared light, with the use of optical sensors that originate directly from the centre, on top of the device. The Y-axis directs the sensors upwards and provides values that are incremented positively, contrasting to the downward orientation of the majority of computer graphics coordinate systems. The X- and Z-axis lie on the horizontal plane of the LMC device with the X-axis positioned along the horizontal face of the device. The Z-axis provides positive values that increment toward the user.

To provide further context as to how the LMC will be used to extract useful biometric information relating to the presented user hand, Figure 3.6 allows a visual representation of the measurements that will be extracted during a scan. It is important to note that the LMC is capable of extracting far more information than what will be used in this particular study. The information and measurements relevant to this study include (and are limited to) the information that can all be obtained from within the hand object. The hand object can further drill down into finger objects. These finger objects can then provide more information depending on the finger type. Each finger type then provides bone objects that list the bone type correlating to the specific finger type. From those bone types, one is then able to measure

those particular bones. As provided by the developer API documentation on Leap Motion's website, Figure 3.6³ provides a visual representation of how the hand object can be matched to suit the needs of this study.

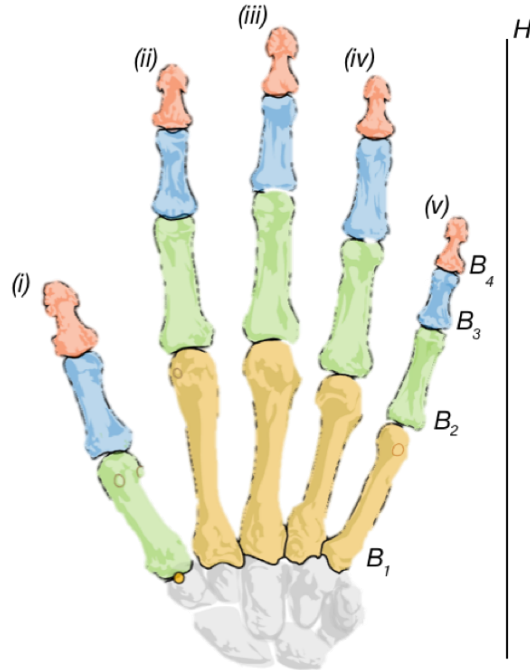


Figure. 3.6 LMC presented hand objects during extraction

In Figure 3.6, it is relevant to present the corresponding information relating to the objects. With the guidance of the API documentation provided by Leap Motion, it is possible to classify all the necessary information into a model that is easier to understand during the development process.

With the use of Table 3.1, it was evident what the class hierarchy would have to be in order to successfully implement the extraction of hand geometry measurements. The information would then be further classified using a Unified Modelling Language to visualise the object structure to be used in the extraction algorithm. Figure 3.7 represents the proposed object structure.

³<https://developer-archive.leapmotion.com/documentation/csharp/devguide/Leap-Overview.html>

Table 3.1 LMC hand object mapping according to infrared scan

Object	Symbol	Name
Hand	H	Hand Class
Finger	(i) (ii) (iii) (iv) (v)	Thumb Index Middle Ring Pinkie
Bone	B_1 B_2 B_3 B_4	Metacarpal Proximal phalanges Intermediate phalanges Distal phalanges

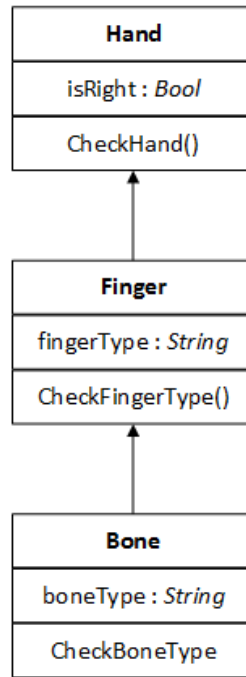


Figure. 3.7 UML object structure

Once the model has been set out and the measurements have been extracted from the presented user hand one can then prepare the extracted biometric for transformation. However, prior to transformation, factors such as where the biometric will be stored and what the template will be, must be considered. In this study the biometric storage preparation is done

using steganographic techniques. In the following section, the stego-images and how they were generated will be discussed.

To aid the development process, Leap Motion has presumed the thumb metacarpal to have a length of 0. It is important to note that the following processes (explained in Algorithm 3.1) all occur at the time of initiating the scan via the LMC. To further illustrate the function used in the development of the extraction process, the following Algorithm can be consulted.

Algorithm 3.1: Leap motion controller algorithm to extract hand geometry

```

1 function ExtractHandGeometry (hand);
   Input :Hand object
   Output :Hand Measurements (fingerLength, boneLength)
2 for hand in hands do
3   if hand=RightHand then
4     for finger in Fingers do
5       fingerType = ClassifyFinger(finger); // Thumb, Index, Middle,
        Ring & pinkie
6       switch fingerType do
7         for bone in finger do
8           boneType = ClassifyBoneType(finger);
9           switch boneType do
10            // Metacarpal, Proximal, Intermediate & Distal
11            AddMeasurements(boneType);
12   else
13     return CloseConnectionError;
```

To explain Algorithm 3.1, the first check that has to be done is one to determine which hand it is. Once the hand is confirmed to be the right hand, the algorithm can then proceed to check the fingers of that hand. Upon classification of the finger, the bones of that finger are then checked. Upon classification of the bone type, within the finger, within the hand, the measurement can be stored in a list. This process occurs for each hand upon enrolment of the finger (prior to storage) and upon authentication to match the measurements.

This research includes the use of the technique of creating cancelable biometrics. The first transformation of the hand geometry occurs in the scan of the hand, whether it be during enrolment or authentication. What is done to the original measurement initiates the cancelability. During the initial ten second enrolment scan, the measurements are extracted as previously discussed in Algorithm 3.1. However, before storage, all the measurements that have temporarily been stored in a list are then aggregated for each of the nineteen bones. This total is then divided by the number of measurements that were taken by the LMC during the scan. The average measurement for each bone is then stored in an array of nineteen unique measurements that are rounded off to the nearest integer. This array of nineteen measurements is then transformed for the first time into a vector of five unique values (one for each finger). This vector is five values and is the first line of defence in protecting the user's biometric. The manner in which Algorithm 3.7 protects the user's biometrics has to do with the transformation that takes place to form this new five value vector. For this example, the values are mathematically transformed by simply aggregating the bone measurements in each finger. It should be noted that any mathematical function can be applied at this point, however, for simplicity, the values are merely aggregated.

Another technique can be applied at this point to practice cancelability, namely by simply discarding particular bone measurements ensures that the cancelability is reusable (as mentioned in Chapter 2). By simply changing the way in which the measurements are transformed, value can be added mathematically to ensure cancelability.

An illustrative example will clarify this process towards the end of this section.

Algorithm 3.1 adds every user's hand geometry measurements to a list. This list consists of $\pm 10\,000$ readings.

Once these readings have been recorded and stored during the initial scan, Algorithm 3.2 is used to drill-down into meaningful hand geometry measurements. Algorithm 3.2 is depicted below.

For each of the bones, in each of the fingers, on each of the hands, the measurements are aggregated. Once the measurements for each finger and it's bones are extracted, this Algorithm 3.2 iterates through the stored readings, aggregates the values, calculates the average (aggregated readings/number of readings), rounded off to the nearest integer. Once this vector is created, the vector is then further transformed.

Algorithm 3.2: Create user hand geometry vector during enrolment

```

1 function EnrolUser (HandGeometryMeasurements);
   Input : All of the different hand geometry measurements (Finger and Bone Lengths)
   Output : HandGeometry vector
2 counter;
3 measurementAverages;
4 for value in measurements do
5   | measurementAverage += value;
6 measurementAverage = RoundToNearestInteger(measurementAverage/counter);
7 for measurementAverage in HandGeometryMeasurements do
8   | vector = ArrayOfMeasurements(measurementAverage);
   // Transformed vector from the array of measurements, passed
   // through the final transformVector function
9 transformedVector = transformVector(vector);
10 return transformedVector

```

3.5.2 Steganographic development

First and foremost to note was how pixels store information. The main concept behind working with pixels was the manner in which the data would be stored in the image in order to accurately represent a user's hand geometry, while maintaining the privacy thereof.

In order for this particular system to work, it had to be thoroughly planned and mathematically accurate to avoid any complications. With the original plan being to use multifactor

Algorithm 3.3: Create stego-image for PINs

```

1 function CreatePINStegoImage ();
   Output : randomImage
2 Array allPins = CreateUserPins(9 000);
3 for pin in allPins do
4   | GenerateHash(pin);
5 int length = allPins.Length;
6 height = 90;
7 width = 800;
8 Bitmap randomImage = new Bitmap(width, height);
9 for (int y = 0; y < height; y++) do
10  | for (int x = 0; x < width; x++) do
11  | | for int i = 0; i < length; i += 4 do
12  | | | a = allPins[i];
13  | | | r = allPins[i + 1];
14  | | | g = allPins[i + 2];
15  | | | b = allPins[i + 3];
16  | | | randomImage.SetPixel(x, y, ARGB(a, r, g, b));
17 return randomImage.Save();

```

authentication with the use of four-digit PINs, the manner in which these PINs are stored had to remain consistent and secure. Not only would the PINs have to be stored using steganography, but all of the users' hand geometry that corresponded to each of those PINs as well.

It was decided to incorporate a type of mapping technique that would have two separate stego-images. By mapping out the user PINs for both stego-images, it provided an easy way to map and keep track of the users and where their information was stored in the image.

Initially, the random four-digit PINs needed to be generated and mapped to the corresponding pixels. The way this was done involved calculations that had to be tested and verified various times before the stego-images were successfully generated (refer to Algorithm 3.3).

Firstly, stego-image 1 would contain the random four-digit PINs after they had been hashed using the SHA-256 algorithm that was discussed in Chapter 2. The calculations went as follows: The SHA-256 algorithm, as the name implies, produces a hash value consisting

of 256bits. By using this algorithm for each of the PINs, one would have to specify what the bits per pixel (bpp) would have to be for each of the pixels in the stego-image. It was decided that 32bpp would be acceptable to use. This is due to the fact that the hashed values would suit this image format in terms of storage capacity.

Typically, what the bpp does is determine the number of colours that can be stored in an image. This number of colours in an image depends on the bpp value. This value grows exponentially. An example of this would be:

If 1bpp is equal to two colours and 2bpp is equal to four colours, then 32bpp is equal to 4,294,967,296 colours. This is due to the stego-images using the format of 32bpp to store the hashed values in the A, R, G and B values (eight bits each).

Furthermore, as seen in Algorithm 3.4, the values for the stego-images are generated at 90 X 800, providing a resolution of 7 200. This is simply because of the number of users who can have a unique four-digit PIN given to them of 9 000. This means that each user's information will be mapped and stored to eight specific pixels in the stego-images.

Algorithm 3.4: Create four-digit user PINs

```

1 function CreateUserPINs (numberOfUsers);
   Input :numberOfUsers
   Output :userPins
2 List userPins ;
3 while numberOfUsers <= 9 000 && !userPins.Contains() do
4   | userPins.Add(Random(1 000, 10 000));
5   | numberOfUsers++;
6 return userPins;
```

The importance of generating the four-digit PINs randomly and assigning the users with these PINs is to provide better suited mapping capabilities. If this system was to be scaled, it could easily be done by simply generating five-digit PINs which would take the total number of users that the system could handle from 9 000 to 90 000. When generating the four-digit PINs that will be allocated to the users it is imperative that the following criteria are met:

- i. No repeating PINs;
- ii. 9 000 unique PINs are generated;
- iii. Unordered sequence (pseudo-random); and
- iv. PINs are only generated once.

Due to the above-mentioned criteria, the PINs carry larger weight when applying them as multifactor authentication to the user along with his/her biometric.

As described above, to meet the criteria for the PINs, it was decided to use PINs that start with 1. By doing so the number of PINs decreases from a possible 10000 to 9 000.

The number of unique PINs can be verified using the following formula:

$$N = x^n \quad (3.1)$$

where x is the number relating to the range of possible values that are considered. In this instance it would be 0 – 9, therefore $x = 10$. However, because this study is only considering values that start with 1 and upward, the formula can be rewritten as follows:

$$N = a^n . b^n . c^n . d^n \quad (3.2)$$

where N is the number of possible unique values and a , b , c and d are the positions in the four-digit PIN. In this particular example, a only has 9 possible values ranging from 1 to 9, whereas b , c and d can range from 0 to 9. This produces the equation:

$$N = 9^1 . 10^1 . 10^1 . 10^1 = 9000 \quad (3.3)$$

To calculate the probability of another user being able to guess your PIN, one would need to look at the statistical formula:

$$P(A) = \frac{\text{NumberOfFavourableOutcomes}}{\text{TotalNumberOfPossibleOutcomes}} \quad (3.4)$$

where the probability of event A in this instance is

$$\frac{1}{9000} = 0,000111111. \quad (3.5)$$

With the probability as low as this enhanced by the biometric feature transformation added to it, the likelihood of guessing a PIN and matching the biometric is very close to zero.

Algorithm 3.5: Create stego-image for users

```

1 function CreateUserStegoImage (bitmap, bytes);
   Input : bitmap
   Output : userAddedBitmap
   // Depending on the x, y coordinates associated to pin
2 if bitmap.GetPixels(x,y) == populated then
3   | return Error;
4 else
5   | for (int i = 0; i < 32; i += 4) do
6   |   | userAddedBitmap = bitmap.SetPixel(x, y, ARGB(bytes[i], bytes[i + 1],
6   |   |   bytes[i + 2], bytes[i + 3]));
7 return userAddedBitmap

```

Initially, stego-image 2 is generated as a blank image with zero values for each pixel. The resolution of stego-image 2 is required to stay consistent with that of stego-image 1 in order to ensure uniformity during the enrolment and authentication phases. Algorithm 3.5 executes during the enrolment phase where administration rights should be displayed in order to add a user to the system. Upon enrolment, the system will allocate a PIN to the user. Once the PIN has been allocated to the user, the system will then attempt to populate the transformed geometry into the eight pixels that are mapped in the same position of the PIN in

stego-image 1. General error checking is shown in Algorithm 3.5, but due to the transformed hand geometry being hashed using SHA-256, the bytes will be set accordingly into the specified pixels. When the user attempts to authenticate using the system, another scan will occur, the hand geometry will be transformed once more and then matched according to the new hash value.

3.5.3 Stego-image contextualisation


To abstract what an image is, consider the following:

A two-dimensional matrix that is made up of pixels containing information about the colours in each particular pixel.

This pixel information can be used to store sensitive biometric information. In order to use steganography techniques to store the transformed biometric models in an image, each model's bit data would have to be processed. All electronic information is essentially made up of 1's and 0's (or bits). This means that the models that are generated need to be manipulated in such a manner that each user model's bit data can be extracted for processing thereof. Once this bit data is processed, it can then be stored in an image to correspond to a particular user.

With two-factor authentication being applied, both the PIN and the hand geometry need to be stored. Using one image to store the PIN, the system can then use the stored PIN to enrol/locate a user in a second image. This can be likened to a one-to-one relational database model. To illustrate this concept, Table 3.2 shows how PIN information in the first image can be used to correspond to the hand geometry stored in the second image. For instance, in the first block of Table 3.2, the bold number (1) represents the user ID slot number while 3648 is the user PIN. The corresponding slot in the second stego-image is then used as the storage location for the user hand geometry data.

Table 3.2 Stego-image 1: User IDs vs their pixel correlation (10 IDs x 8 pixels per ID x 5 rows

									
1, 3648	2, 7896	3, 5091	4, 4948	5, 3102	6, 7500	7, 1651	8, 6765	9, 6865	10, 7677
11, 5153	12, 1782	13, 2922	14, 2183	15, 1817	16, 6372	17, 1621	18, 8283	19, 2845	20, 6931
21, 2608	22, 3587	23, 6231	24, 5373	25, 3594	26, 1877	27, 3867	28, 1080	29, 2807	30, 6143
31, 7362	32, 4162	33, 8075	34, 8742	35, 7851	36, 3653	37, 8431	38, 4352	39, 1238	40, 2128
41, 7673	42, 2513	43, 8825	44, 5110	45, 5701	46, 6623	47, 5963	48, 1703	49, 3697	50, 2073

In order to standardise the amount of data that can be used to store information in the pixels, the system uses 32bpp (bits per pixel) image formatting. This ensures that in each pixel of the image, 32 bits of information can be held. These 32 bits are made up of A (eight bits), R (eight bits), G (eight bits), and B (eight bits) values. Due to the fact that the number of bits used to store a four-digit PIN would vary depending on the value, it was decided to also standardise the number of bits used during PIN storage per user. To do so, a hash-function is used (Kashyap and Sharma, 2016). The hash-function ensures that regardless of what the PIN is, the length of the hash representation will be similar. A SHA-256 (Secure Hashing Algorithm 256-bit) function was chosen. This is because it is the successor of SHA1, which was compromised (Brandom, 2017), and addresses the issues prevalent in SHA1. Each PIN is made up of 256-bits (eight pixels, if one pixel = 32bpp), leading to eight pixels to store user their information in both images. Referring back to the earlier statement of using two images with a one-to-one relationship, a user PIN can be mapped and correlated directly to the hand geometry in the second image using the hash function prior to enrolling the user.

Table 3.2 is an example illustration of user ID slots in correlation to the image pixels with an image resolution of 80 X 5. The first image is used to store hashed user PINs. To generate the stego-image, the PINs are shuffled to ensure that the PIN-ID combination is not sorted in such a manner that PIN 1 000 is stored in the first eight pixels using the ID slot 1, etc.

3.5.4 Random PIN generation

To counter the threat of reverse engineering the generated PINs, 9 000 (unsorted) unique four-digit PINs were generated and each PIN mapped to an ID that ranged from 1-9 000. An example of such a mapping is demonstrated using Table 3.2 to illustrate that PIN 3648 correlates to the user ID of 1. With this information generated and stored locally, using a conversion to bit data, stego-image 1 was generated so that all of the hashed PINs were stored and mapped. Stego-image 1 will thus remain unaltered after it has been generated. Stego-image 2 can then be altered during the enrolment phase. This is further explained below.

3.5.5 Stego-image generation

Stego-image 2 is a randomly generated image that will be altered as users enrol into the system. During the enrolment phase, users will be issued a PIN. Depending on the PIN he/she receives, a user ID correlating to that PIN is known by the system. Once the system has calculated the user ID based on the PIN that was entered by the user, the pixels in stego-image 2 can be altered using the hashed hand geometry of the enrolling user. By altering stego-image 2 in this way using stego-image 1, the authentication phase becomes more efficient because the pixels containing the biometric information can be directly read due to the mapping. The authentication process would be inefficient if the system had to search through the entire image each time a user presented his/her hand. Since an image

can be seen as a matrix with 9 000 users, the complexity to compare and authenticate the presented hand geometry to the image would be $O(n^2)$ each time.

In order to gain a better understanding of how the system operates, the pseudocode for the system is subsequently discussed.

3.5.6 Cancelable biometric development

The SHA-256 algorithm was discussed in detail in Chapter 2. However, it has been revisited here in Algorithm 3.6 for completeness in order to provide context for how the bytes will be stored in the stego-images.

What Algorithm 3.6 does is prepare the transformed vector for storage in stego-image 2 by returning bytes of data that are irreversible and safely secured.

Algorithm 3.6: Generate hash algorithm

```

1 function GenerateHash (transformedVector);
   Input :transformedVector
   Output :vectorHash
2 using SHA-256 hash = ComputeHash(transformedVector);
3 for byte in hash do
4   | vectorHash.add(byte);
5 return vectorHash;

```

The transformed vector that is passed into this function comes in the form of a text representation subsequent to the extraction scan that takes place from the LMC device. This will be further demonstrated in the following section that discusses the illustrative example. However, Algorithm 3.7 revisits the simple transformation that occurs after the hand has successfully been scanned by the LMC and the measurements have been extracted.

3.5.7 Pseudocode for system algorithm

Keeping the above-mentioned information flow, as well as the mapping and stego-image generation in mind, this pseudocode should verify the exact functioning of the authentication

Algorithm 3.7: Transform algorithm

```

1 function TransformVector(ArrayOfMeasurements);
   Input :ArrayOfMeasurements
   Output :transformedvector
2 for measurementAverage in ArrayOfMeasurements do
3   | transformedVector += measurementAverage;
   | // Aggregated measurements for this example
4 return transformedVector;

```

system. The pseudocode below (Algorithm 3.8) aims to provide an overview of what input is retrieved in the system and to clarify how the two phases of biometric systems are applied based on the input retrieved from the user. As seen above, if the user is enrolled, the system merely transforms the presented hand geometry and authenticates the user by comparing the transformed information to that stored in stego-image 2.

Algorithm 3.8: Pseudocode for system algorithm

```

1 function cancelableTransform(PIN, array[] fingerBoneInfo);
   Input :PIN, BiometricFeatures handID (hID), array[boneType (bT), boneWidth (bW), boneLength (bL)]
   Output :User-specific HashID for Steganography
2 if (PIN == hID) && (enrolled == true) then
3   | handGeo = Transform(fingerBoneInfo);
4   | Authenticate(getPixels(map),handGeo);
5 else
6   | newUser = Transform(fingerBoneInfo);
7   | EnrolUser(PIN, newUser);
8 return HashID;

```

The pseudocode for the entire system algorithm attempts to summarise the process that the authentication system follows, from the initial scan during enrolment to the matching the transformed biometric that is presented by the user during authentication.

Algorithm 3.8 describes the logic behind the system in a simplified manner to portray the main functionality.

However, if the user has not been enrolled, he/she is then issued a PIN and the presented hand geometry is transformed and stored in stego-image 2, correlating to the issued PIN location.

Next, the advantages and disadvantages of the system will be discussed.

3.5.8 Discussion

The use of the current implementation of this authentication system has its advantages and disadvantages.

Advantages of the proposed system include:

- i. The low-cost factor;
- ii. Ease of use and convenience;
- iii. The security aspects are superior when compared to passwords because authentication is based on a combination of PIN and hand information that cannot be stolen or guessed; and
- iv. Auditability in terms of being able to connect users to a specific event or activity.

The disadvantages include:

- i. The technology is still in its infancy and is not mature;
- ii. While system performance for authentication is expected to be high for small organisations, it may pose a problem should more users need to be enrolled; and
- iii. Error incidence due to changes in a person's hands due to injury, old age, or illness.

The following section will provide an illustrative example of the system.

3.6 Illustrative example

In this section, a simplified example of a user being authenticated is presented in order to provide a holistic view of the combination of the topics discussed in previous sections. With each hand that is presented to the LMC a model is created that is either used for enrolment or for authentication. Assuming that the user hand that is presented has already undergone enrolment, the LMC will create a model using a particular transform parameter to compare this model to the binary representation of the hand already stored in stego-image 2. By using the PIN that is entered prior to hand scanning, the system ensures that the user's transformed biometric representation can efficiently be compared to the newly transformed model. This is efficient because the system has mapped the PINs to pixel IDs, rather than having to search the entire image for the corresponding biometric representation.

Consider the explanation of the illustrative example shown in Figure 3.8.

- i. Assume the user was presented with the PIN 6283 during enrolment. The user would then have a dedicated storage section with the ID of 86 in both stego-image 1 and in stego-image 2. During the authentication phase the user will have his/her hand geometry scanned to compare the presented hand to the binary representation stored in stego-image 2.
- ii. During the above-mentioned scan, the hand geometry of the user is mathematically generated by using various combinations from the thousands of readings gathered to form one vector (readings for each of the 19 individual bones in his/her hand).
- iii. By using the vector created in (ii), the system then transforms the biometric vector once more in order to implement CB (as discussed in Chapter 2). In this particular example, the vector was simply transformed by adding each finger's bone readings together (three readings for the thumb and four readings for all the other fingers). It

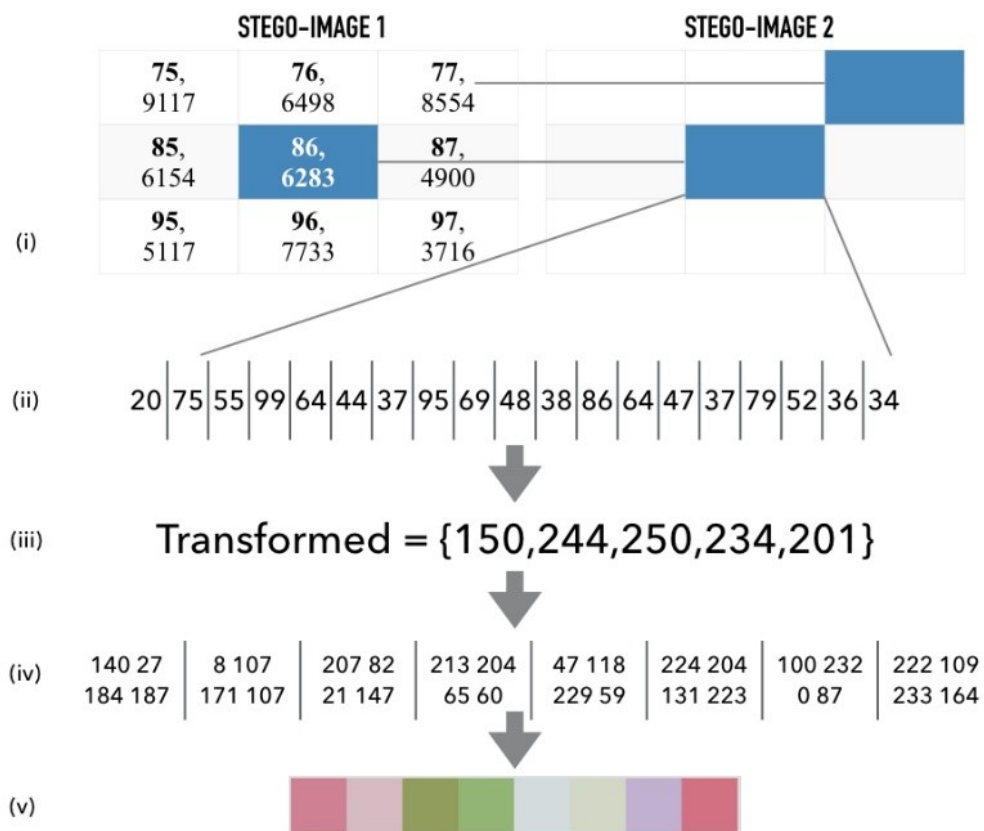


Figure. 3.8 Example of biometric vector reading and transformation

should be noted that more complex mathematical transformations are recommended for the actual implementation.

- iv. The system further protects the biometric information by applying a SHA-256 hash function to the vector. This vector is then represented as a byte array consisting of 32 values from the 256-bit hash function. Ultimately, this ensures that each user only uses eight pixels in both the stego-images.
- v. Once the byte array has been generated, it can then be compared to the stored biometric representation in ID 86 consisting of eight pixels. Upon completion of the above-mentioned process, the system will either accept the user as successfully authenticated, or the system will reject the user and ask for the hand to be re-scanned.

By using steganography techniques, the system ensures imperceptibility and cancelability.

Figure 3.9 provides a comparative view of two generated images for their use in this context.

The image on the left was randomly generated, while the image on the right contains sensitive biometric information. To the human eye one cannot easily infer that these two images differ, however, upon closer inspection one may realise differing colour mappings but cannot differentiate between sensitive data and just another randomly generated image.

Ultimately, cancelability of the biometric can be confirmed due to the biometric information being transformed and obscured prior to storage. This means that should an attacker find these two images in a compromised system, he/she will not know what information was used to generate these images, nor how the information was transformed prior to storage. In fact, without prior knowledge he/she will not even know to expect hidden data in said images.

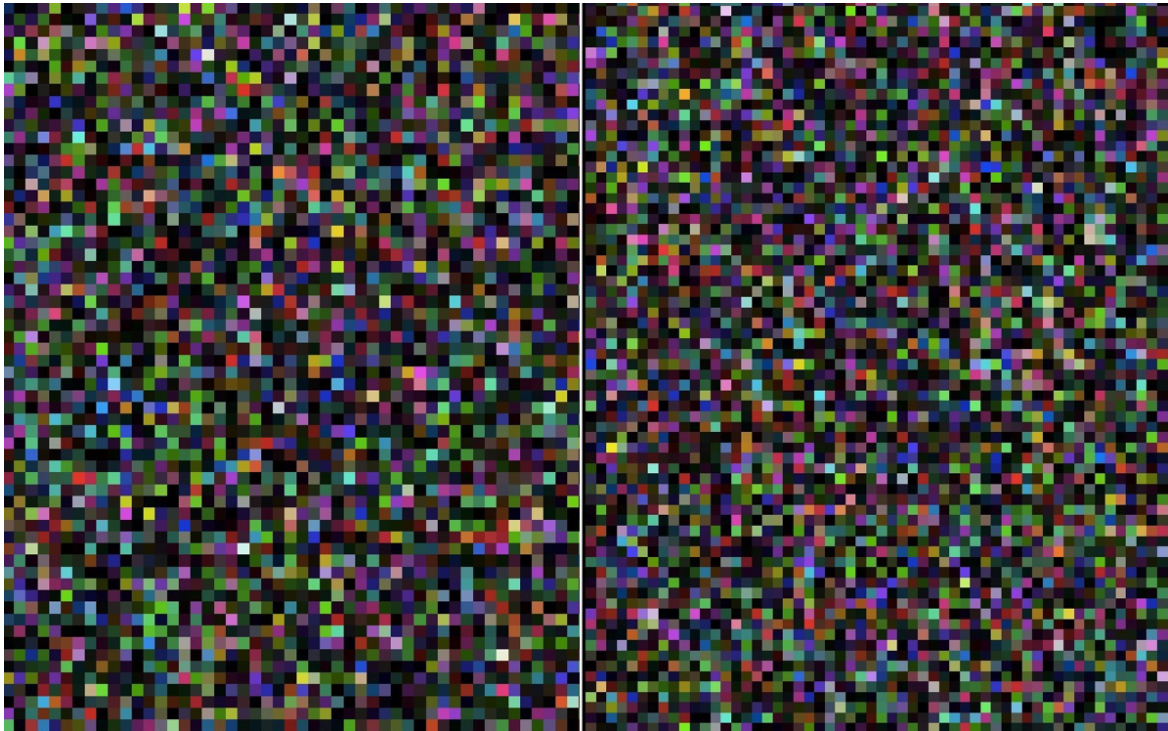


Figure. 3.9 Randomly generated image versus stego-image

3.7 Chapter summary

The purpose of this chapter was to demonstrate the approach used throughout the system design and implementation thereof. Due to the process implemented in the system consisting of various iterations, the development of the system involved a considerable amount of integration. With the use of algorithms and an illustrative example, the functionality of the system (with reference to the increments described in Chapter 2) was thoroughly and explicitly explained in order to provide greater context.

In Chapter 4, the results produced by the authentication system will be analysed, and the algorithmic performance and evaluation will be discussed.

Chapter 4

Evaluation and data analysis

4.1 Introduction

In an attempt to quantify the performance of the proposed system, a three-fold evaluation was instantiated and conducted. This is presented in terms of the consistency of the LMC, followed by a comparative vector tolerance analysis, and finally, the overall system accuracy. Thereafter a discussion is presented. The following evaluation and discussion are based on sample data that was collected through the scanning (enrolment and authentication) of forty unique candidates.

4.2 Testing methodology

In testing the system, it was decided that a simulation should be initiated in order to determine the reliability and efficiency of the system by eliminating the LMC. This was done due to the device's lack of customisability. The simulation attempts to exclude the aspects of the system that cannot be altered or changed. The LMC, as a peripheral device is bound by the hardware and software capabilities that are controlled by external sources. For this reason, the simulation would eliminate the LMC component of the proposed authentication system

and use only the extracted data to test the algorithm efficiency. As the system stored the transformed biometric data of the forty users in stego-image 2, the simulation would attempt to authenticate only the user data that was extracted during enrolment and authentication phases.

In order to successfully simulate the authentication process, the following steps would need to be conducted:

- i. Both stego-images will be stored to read information from within the test program;
- ii. A list will be created correlating with the users' PINs;
- iii. A list will be created correlating with the transformed hand geometry extracted during the authentication scans;
- iv. These lists will be iterated accordingly, having each PIN in the list hashed and matched to the data corresponding to that PIN in stego-image 1;
- v. Once the PIN is successfully matched, the corresponding authentication transformation will be hashed and matched to the data within stego-image 2;
- vi. Each of the aforementioned steps will be timed in order to gauge the efficiency of the matching algorithm.

With the core functionality of the proposed system being to successfully transform and authenticate users, the efficiency is perceived to be slightly lacking. As Figure 4.1 shows, the algorithm used to find the authentication match within the threshold tolerance range (explained further in Section 4.2.2) of 5 affects the speed at which a user can be authenticated. A simple and effective solution to this drawback of obtaining a successful match may be to place an upper limit on the time that the algorithm is allowed to scan for a match. This upper limit can be deduced from the average time of 6.65s to authenticate all forty users.

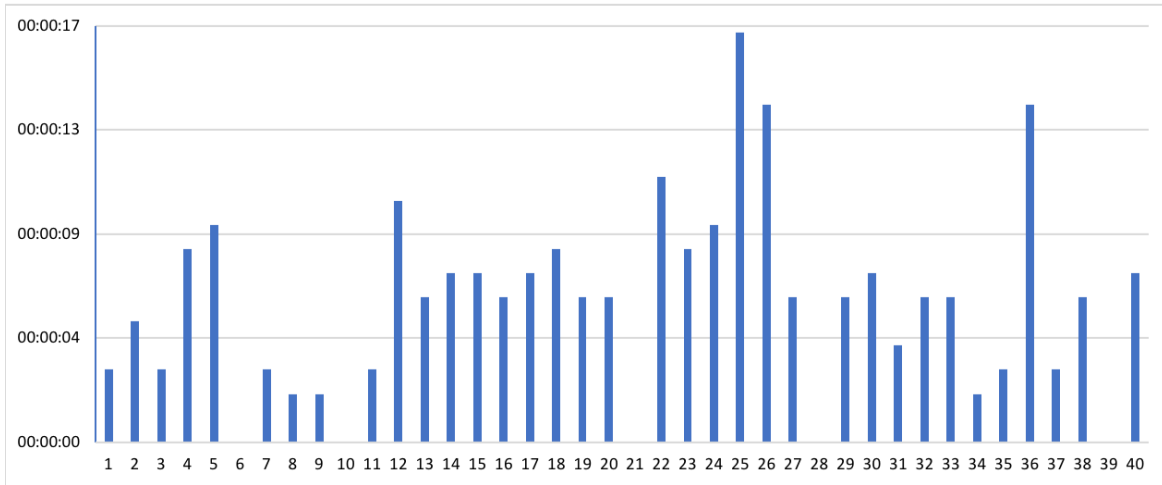


Figure. 4.1 Simulation for time taken to authenticate users

4.2.1 Leap motion controller performance evaluation

To illustrate the efficiency and reliability of the LMC, the data that was collected from one randomly-selected, five-second hand geometry scan is presented in both Table 4.1 and Figure 4.2. In order to present a visualisation with a high enough resolution to be able to see the variance in the scan readings, only the three fingers most similar in length are shown in Figure 4.2 (i.e., the index, middle, and ring fingers).

Table 4.1 Randomly-selected data from five-second scan

Thumb	Index	Middle	Ring	Pinkie
0.197203783	0.424346553	0.464246258	0.438259197	0.35738522

The significance of this data is prevalent when taking into consideration the distribution throughout the scan. It is of the utmost importance to consistently extract concise data readings throughout the length of the scan. Thus, the standard deviation of the raw data correlating to the plotted data was calculated in an attempt to demonstrate the accuracy that the LMC provides (see Table 4.1).

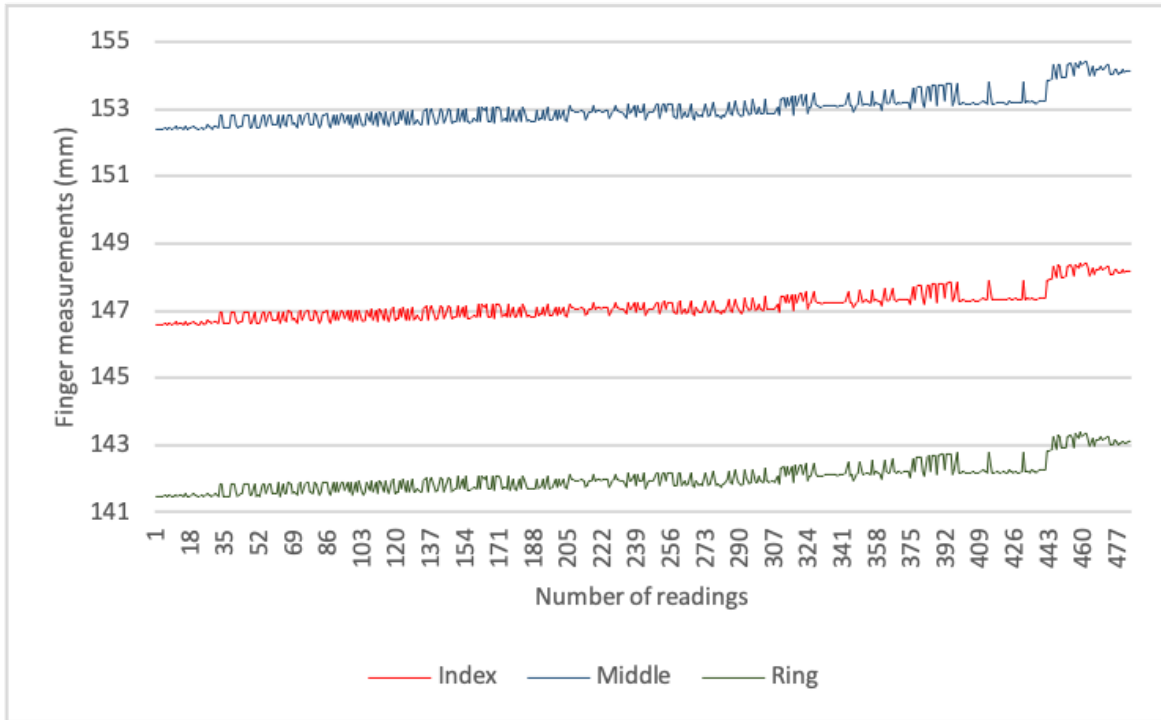


Figure. 4.2 LMC readings for a five-second hand scan

It is interesting to note that the longer the scan has progressed, the more varied the readings become. This is attributed to the instability that is associated with an unsupported hand being held in mid-air for any given period of time.

4.2.2 Comparative vector tolerance

Despite the above-mentioned LMC accuracy, the system shows slight deviation from one scan to the next. To provide an explicit limit regarding the deviation of the readings during a scan, it was decided to measure a tolerance range.

The manner in which this tolerance range was calculated involves comparing test data from user enrolment scan to that of the associated authentication scan. This data includes all the users and their transformed vector combinations. With this data, the maximum tolerance range was extrapolated based on the variations produced by the system. As seen in Figure 4.3 below, it was concluded that the maximum tolerance range for this data set is 5mm.

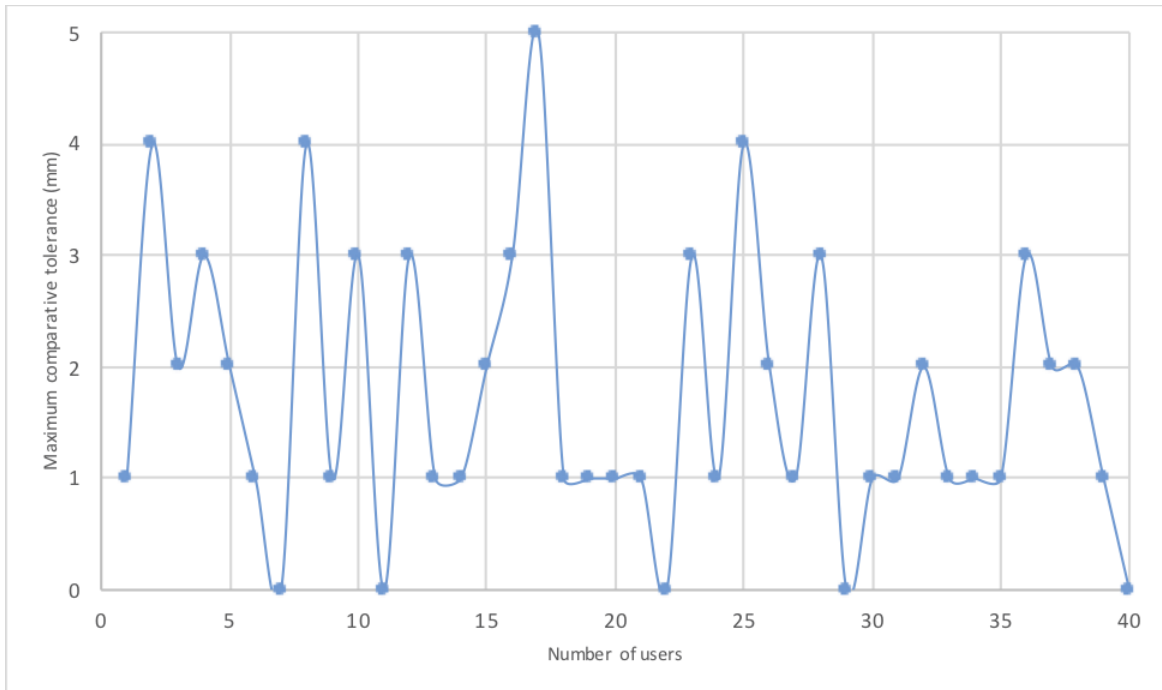


Figure. 4.3 Comparative vector tolerance

Upon further evaluation, with the tolerance range at a maximum of 5mm, the acceptance rates exponentially improved. This, however, increased the processing time to find a positive match within the tolerance range of the transformed vector.

4.3 Algorithm evaluation

As with any authentication system, one needs to take human error or inconsistency during the scanning process into consideration. To better illustrate the thought process prior to the formulation of the Algorithm 4.1, consider the following example:

- i. User A enrolls with the transformed hand geometry vector of *50, 60, 70, 80, 90*;
- ii. When user A attempts to authenticate thereafter, his/her hand is not scanned identically due to various factors and the transformed hand geometry vector produced this time is *52, 59, 74, 81, 90*

- iii. Due to the SHA-256 hashing applied to the transformed geometry prior to storage, the match to the value stored within stego-image 2 fails, even though user A has provided the correct PIN.
- iv. In order to provide greater match accuracy, an algorithm was formulated in order to compensate for fault tolerance during scans.
- v. As seen in Figure 4.3, the fault tolerance was variable for a range of 5 for each vector value.

With a fault tolerance of 5mm, the probability of finding an exact match of the stored biometric increases exponentially. Algorithm 4.1 attempts to find a match as efficiently as possible while reducing the number of false positive matches produced by the system.

Once the scanned vector is passed into this algorithm, the calculations proceed as follows:

- i. The original transformed vector is copied and the 1st value is decremented by 1;
- ii. This alteration creates a new vector;
- iii. The new vector is then hashed and compared to what is stored in stego-image 2.
- iv. The process repeats itself for each value until the last value in the original vector is decremented by 1;
- v. The 1st value is then incremented by 1, hashed and compared to what is stored in stego-image 2;
- vi. The process then repeats itself and increases the increment to 2, 3, 4 and 5 respectively;
- vii. If a match is found during this process, the algorithm is halted. If no match is found, the algorithm continues to recursively search for a match until the possible vector combinations are exhausted.

Algorithm 4.1: Recursive algorithm to find possible vector combinations

```

1 function VectorCombinationsCheck ( transformedVector, count);
   Input : transformedVector
   Output : result
   // transformedVector, low and high are vectors
2 low; high;
3 increment = 0;
4 if count = transformedVector.Length then
5   | return;
6 for (value in transformedVector) do
7   | increment++;
8   | Array.Copy(transformedVector, low);
9   | low[count] = transformedVector[count] - increment;
10  | checkLowMatch = GenerateHash(low);
11  | Array.Copy(transformedVector, high);
12  | high[count] = transformedVector[count] + increment;
13  | checkHighMatch = GenerateHash(high); // Recurse
14  | VectorCombinationsCheck(low, count + 1);
15  | VectorCombinationsCheck(high, count + 1);
16 return result = VectorCombinationsCheck(transformedVector)

```

The above-mentioned process is illustrated in Algorithm 4.1.

This approach attempts to decrease the false-positive match rates.

4.4 Overall system evaluation

As deduced from Figure 4.4, a 0mm tolerance resulted in only a 12.5% true acceptance rate. If this tolerance is then increased, the true acceptance rate also increases (e.g. 97.5% with a 4mm tolerance) until a 100% true acceptance rate is obtained at 5mm tolerance. When considering implementing this particular system approach, one needs to determine what risk factor is suitable within the authentication scenario. If the users who need to be authenticated are to be granted access to sensitive data/areas, then the tolerance range should be adjusted accordingly. The acceptance rate is drastically affected when using the maximum tolerance range. With such a high tolerance range, the false acceptance rate is

also dramatically increased, but because of the two-factor authentication provided with the allocated PIN, the users are authenticated correctly and no inter-user error is observed where one user is authenticated as another.

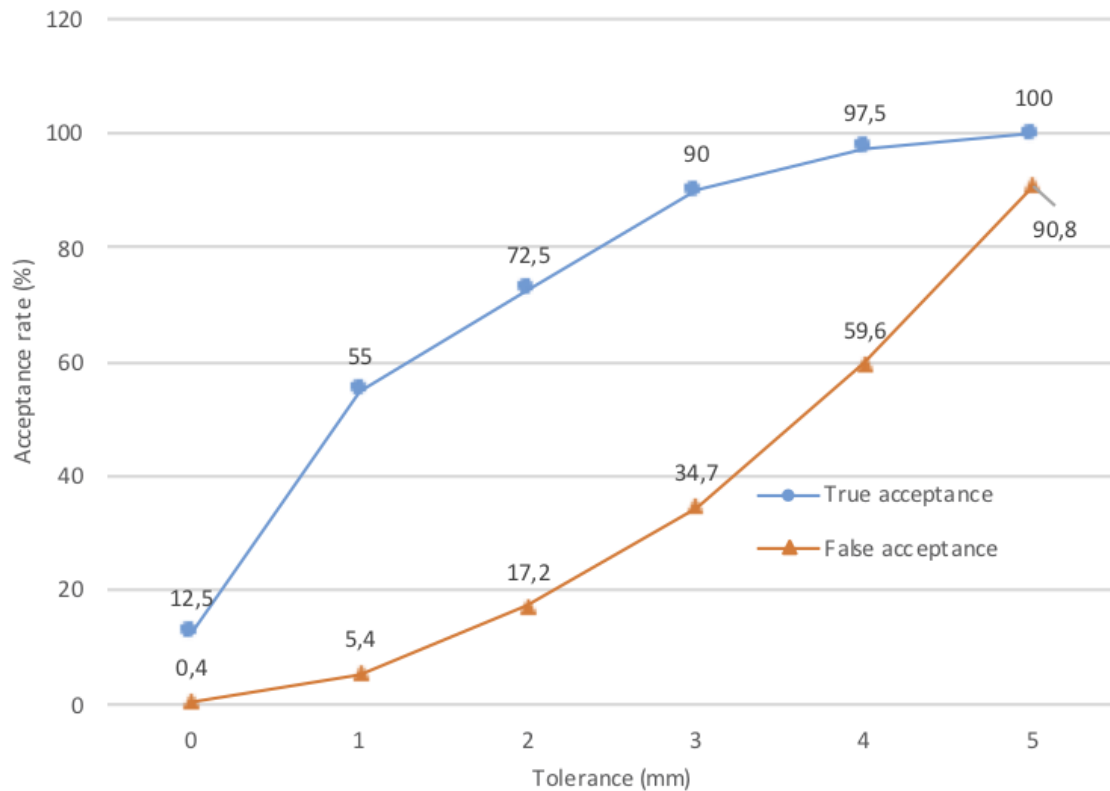


Figure. 4.4 System tolerance versus acceptance rates

4.5 Discussion

The proposed technique has revealed several promising advantages by using a combination of the techniques specified in Chapter 2. The LMC was found to be a stable and efficient hand geometry scanner. In addition, the steganography techniques used in this paper were relatively easy to implement for use in this particular instance. By using PINs (to implement two-factor authentication) the security is enhanced and aids in achieving cancelability for

storing biometrics. The proposed framework ensured that the system provided results that were reliable and efficiently obtained.

Bearing in mind the above-mentioned advantages, some disadvantages are present when using this approach. The algorithm implemented to find positive matches slowed down the system. It may be of value to consider the possibility of removing the algorithm in future and alternatively producing a false match, followed by a re-scan. This system was only exposed to limited testing and the authentication accuracy and robustness will need to be measured using a formal evaluation. In order to fully explore the system's functionality, extensive tests should be conducted upon this framework on a larger scale. This will form part of the ongoing research.

4.6 Chapter summary

The aim of this chapter was to evaluate the overall system design, performance, accuracy and efficiency. This was done by analysing data extracted during the testing process. Once analysis of that data was complete, the system performance, accuracy and efficiency were measured using simulation tests by removing certain system components. The algorithmic complexity was analysed for optimisation possibilities.

In Chapter 5, the objectives of the study will be revisited and discussed. Any problems experienced throughout the study will also be addressed and opportunities that may have come to fruition throughout the research will be discussed for future studies.

Chapter 5

Conclusion

5.1 Introduction

In Chapter 5, this study is concluded by presenting definitive remarks and comments. The aforementioned will be based on the research objectives that were presented during the initial stages and whether or not these objectives were realised. The limitations that emerged will also be discussed, as well as new opportunities that have become apparent upon completion.

5.2 Research objectives

In Chapter 1, it was stated that in order to achieve the primary aim of this study, various secondary objectives would first need to be met. Subsequently, these objectives and how they were achieved are discussed below, followed by the main aim.

Objective 1: *By means of a literature review, discuss the use and implementation of cancelable biometrics, steganography, hand geometry authentication and the leap motion controller*

Addressing this objective involved a thorough investigation into a multitude of seemingly disparate techniques and an attempt to unify them to provide a holistic approach for an

authentication system. This was carried out in Chapter 2. The discussions regarding these techniques focused on their individual characteristics and what the best practices were for implementing each of those techniques independently. In the discussions that accompany the literature review it was shown that these techniques could collectively produce a framework that is implementable as an authentication system.

Objective 2: *Design and implement an authentication system that utilises the techniques from literature*

It was shown that if the collective techniques could produce an authentication system, the design and implementation of this proposed system would have to be laid out systematically. In Chapter 3, the system design process was mapped out using the iterative and incremental approach which allowed the materialisation of smaller objectives or increments that needed to be implemented in order to successfully create the proposed authentication system. The aforementioned increments guided the development process and ensured that the primary objective of this study was well aligned with the those increments.

The implementation process presented various challenges that were overcome due to the knowledge that was gained in the literature review and was well managed through the use of the iterative and incremental model. In Chapter 3, the development of the system was discussed, highlighting the crucial algorithmic functions that were needed in order to meet the incremental authentication system capabilities. By meeting this secondary objective, the only objective remaining would be to thoroughly test the functionality of the system.

Objective 3: *Evaluate the resulting authentication system using error-based metrics and iterative validation testing*

In order to conclusively state that the proposed authentication system is fully functional, an evaluation of the system using error-based metrics and iterative validation testing was performed. The testing was conducted by means of the testing methodology as described in Chapter 4. The authentication system was evaluated in terms of the LMC performance, comparative vector tolerances, matching algorithm performance, and finally, a holistic evaluation of the authentication system performance. The results of the evaluation showed that even though the system lacked efficiency and could be optimised to authenticate users faster, it did so with a high success rate and a high accuracy rate.

The above-mentioned objectives were successfully met and allowed for the main research aim to be addressed. The research aim is reiterated below:

Aim: *Develop a technique that ensures cancelability of biometrics (1) based on hand geometry information from an LMC (2) and utilises steganographic storage techniques (3).*

An authentication system was developed that implements the techniques that were expressed in the research aim. The steps that the authentication system performs, and that relates to the requirements of the research aim, are presented below:

- *Extract biometric information based on hand geometry measurements from users (2)*

The LMC performs an infrared scan and determines measurements relating to hand geometry. These measurements are used to create a model of the hand that can be used as a biometric template for enrolment and authentication.

- *Ensure that these biometrics are made cancelable using various techniques to transform the biometric information prior to storage (1)*

In order to ensure the cancelability of the biometric template, the measurements from the LMC are aggregated by taking the average measurements for each scanned finger and combining them in a vector. Thereafter, the vector is used to create an irreversible hash that is used in the following step.

- *Finally, the biometrics are stored using steganographic techniques (3).*

Steganography techniques were employed to create a storage mechanism that provides an extra layer of security to the system. By replacing a traditional user database with the stego-images, the fidelity of user biometrics is enhanced. This is due to the novel way in which the biometric templates are stored. In the event that one user's biometric template is compromised, the rest of the templates remain secure.

Thus, the aim and all of the objectives, as described in Chapter 1 and reiterated here, have been successfully addressed and achieved, while simultaneously supporting the research statement, also from Chapter 1:

Research statement: *Biometric cancelability can be enhanced using user-based transform parameters (obtained from an LMC) for a steganography algorithm that stores biometric information.*

5.3 Contribution to field

The use of biometric authentication has become ubiquitous to manage access to physical and digital resources, such as buildings, rooms and computing devices. By proposing a framework for a novel biometric system that not only improves the security of user's biometrics, but also provides ease of use and is cost-effective, ultimately, a broader contribution is made

within the information security field.

A novel application of hand-geometry for creating cancelable biometrics from LMC readings

An LMC was employed in this research as a way to extract latent biometric measurements that the device uses for motion control. The use of measurements from an LMC for biometric authentication builds on the work of Chan *et al.* (2015). The manner in which these measurements are used in this research for the construction of the hand-geometry model extends the work of Chan *et al.* (2015) and includes the following:

- The hand-geometry measurements are combined mathematically by creating a novel hand-geometry model;
- LMC measurements are used to determine user-specific transforms that are applied during the cancelability phase; and
- The performance of the LMC is experimentally evaluated.

Ensuring cancelability for novel biometrics

The importance of the cancelability of biometrics is discussed in Chapter 2. Cancelable biometric templates are created by employing the following techniques:

- Ensure the cancelability of the biometric template by including user-specific transforms, obtained from LMC scans; and
- By applying uni-directional hashing with the SHA-2 algorithm.

The use of steganography for the storage of biometric templates

This research presented the novel application of steganography techniques to store the hand-geometry templates in a secure manner. Image steganography is used to store the biometric templates rather than a regular user database. This contributes to the overall security of the authentication system as follows:

- User biometrics are hidden in plain sight within an image. When a server is compromised, it is not necessarily obvious to attackers where to look for sensitive information, and if the images are found, an attacker would not know that the images contain any hidden information;
- User-specific biometric information, along with PIN information, are used to determine storage locations in the images. In the event that one user's biometrics are located within the image, the storage locations of the biometric templates remain uncompromised.
- The implementation of two-factor authentication, by means of issuing users with PINs, contributes to lower false acceptance rates for the authentication system.

5.4 Limitations

With regard to the setup of the proposed framework, there were few limitations in terms of the actual development of the system due to the wide range of supported development platforms, languages and firmware. However, a limitation to the system remains that the LMC is a peripheral device and therefore requires a host on which to run. The minimum system requirements for the system can be seen in Appendix C. Upon testing, another limitation in terms of the number of willing participants for testing was observed. Due to the number of willing and available members, the total number of participants was limited to forty. Even though the LMC proved to be an effective and efficient biometric sensor, the use of hand geometry for the source of user biometric revealed the lack of uniqueness of a human hand found in this approach. It may be useful to use a more distinctive biometric in the future (such as fingerprints). However, with the reduced cost of using a peripheral device like the LMC, the limitations posed by this approach may also be regarded as advantageous due to the ease of use and affordability.

5.5 Future work

The research that was presented in this study provides opportunities for future research. Some of the possibilities are highlighted in this section. The combination of techniques presented in this study are merely one approach that can be taken, and various other approaches may be followed to create an authentication system. Another possible approach that could be implemented for future research may be to use fingerprints as the biometric source, along with an alternative CB approach, as well as, using steganography in a different way. The proposed system could open up many possibilities into the manner in which cancelable biometrics are used in authentication systems. Further studies may also include the use of a larger data set to provide more detailed analysis regarding the cancelability and accuracy of the proposed framework.

To improve the proposed framework, one could look at the vast number of opportunities that were revealed throughout the research process. Some of these opportunities include:

- i. Improving the system performance by using more efficient search algorithms to match users faster;
- ii. Increasing the level of security provided through the steganographic techniques by applying a greater level of dynamic randomness during the enrolment and storage process;
- iii. Using mathematically complex approaches to apply cancelability prior to the biometric storage and matching processes; and
- iv. Upgrading the system to use cloud services for storing the stego-images rather than storing the information locally.

5.6 Chapter summary

Chapter 5 is the final chapter of this study in which the aim was to present a summary of the objectives that were presented in Chapter 1, how these objectives were approached and achieved, and the limitations that were realised throughout the study and the possibilities that arose upon completion thereof.

References

- Anderson, R. (2001), Why information security is hard - an economic perspective, *in Proceedings of the '17th annual Computer security applications conference'*, IEEE, pp. 358–365.
- Anonymous (2017), 'SDLC iterative incremental model, [online], available: <http://tiny.cc/bl922y>, [Date of access: 2017-06-13]'.
- Brandom, R. (2017), 'Google just cracked one of the building blocks of web encryption (but don't worry) - the verge, [online], available: <https://www.theverge.com/2017/2/23/14712118/google-sha1-collision-broken-web-encryption-shattered>, [Date of access: 2017-08-27]'.
- Chan, A., Halevi, T. and Memon, N. (2015), Leap Motion Controller for authentication via hand geometry and gestures, *in Proceedings of the 'International Conference on Human Aspects of Information Security, Privacy, and Trust'*, Springer International Publishing, pp. 13–22.
- De Villiers, M. R. (2005), Three approaches as pillars for interpretive Information Systems research: development research, action research and grounded theory, *in Proceedings of the '2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries'*, pp. 142–151.
- Dictionary, B. (2016), 'What is positivism?'.
URL: <http://www.businessdictionary.com/definition/positivism.html>

- Dlamini, M., Eloff, M., Eloff, J., Venter, H., Chetty, K. and Blackledge, J. (2016), Securing cloud computing's blind -spots using strong and risk-based MFA, *in Proceedings of the 'International Conference on Information Resource Management'*, pp. 58: 1–28.
- Jain, R. and Boaddh, J. (2016), Advances in digital image steganography, *in Proceedings of the '2016 International Conference of Innovation and Challenges in Cyber Security (ICICCS-INBUSH)'*, IEEE, pp. 163–171.
- Jakobsen, T. G. (2013), 'Theory of science - what is positivism, [online], available: <http://www.popularsocialscience.com/2013/02/15/theory-of-science-what-is-positivism> [Date of access: 2016-03-26]'.
- Karimovich, G. S. and Turakulovich, K. Z. (2016), Biometric cryptosystems: Open issues and challenges, *in Proceedings of the 'International Conference on Information Science and Communications Technologies (ICISCT)'*, IEEE, pp. 1–3.
- Kashyap, Y. and Sharma, R. (2016), 'A survey on various authentication attacks and database secure authentication techniques', *International Journal of Multidisciplinary Educational Research* **5**(15), pp. 67–81.
- Kishor, S., Ramaiah, G. and Jilani, S. (2016), A review on steganography through multimedia., *in Proceedings of the 'International Conference on Research Advances in Integrated Navigation Systems (RAINS)'*, IEEE, pp. 1–6.
- Laskar, S. A. and Hemachandran, K. (2013), 'Steganography based on random pixel selection for efficient data hiding', *International Journal of Computer Engineering & Technology* **4**(2), pp. 31–44.
- Liu, S. and Silverman, M. (2001), 'Practical guide to biometric security technology', *IT Professional* **3**(1), pp. 27–32.
- Nagar, A. and Jain, A. K. (2009), On the security of non-invertible fingerprint template transforms, *in Proceedings of the 'First IEEE International Workshop on Information Forensics and Security (WIFS)'*, IEEE, pp. 81–85.

- National Institute of Standards and Technology (2015), *FIPS PUB 180-4: Secure Hash Standard*, NIST.
- Oates, B. J. (2006), *Researching Information Systems and Computing*, Sage Publications Ltd.
- Owen, C. L. (1998), 'Design research: Building the knowledge base', *Design Studies* **19**(1), pp. 9–20.
- Pandit, A. S. and Khope, S. R. (2016), 'Review on image steganography', *International Journal of Engineering Science* **6**(5), pp. 6115–6117.
- Patel, V. M., Ratha, N. K. and Chellappa, R. (2015), 'Cancelable Biometrics: A review', *IEEE Signal Processing Magazine* **32**(5), pp. 54–65.
- Paul, P. P. and Gavrilova, M. (2012), Multimodal cancelable biometrics, in *Proceedings of the '2012 IEEE 11th International Conference on Cognitive Informatics and Cognitive Computing'*, IEEE, pp. 43–49.
- Paul, P. P., Gavrilova, M. and Klimenko, S. (2014), 'Situation awareness of cancelable biometric system', *Visual Computer* **30**(9), pp. 1059–1067.
- Pfleeger, C., Pfleeger, S. and Margulies, J. (2015), *Security in Computing*, 5th edn, Prentice Hall.
- Piciuccio, E., Maiorana, E., Kauba, C., Uhl, A. and Campisi, P. (2016), Cancelable biometrics for finger vein recognition, in *Proceedings of the 'First International Workshop on Sensing, Processing and Learning for Intelligent Machines (SPLINE)'*, IEEE, pp. 1–5.
- Pradhan, A., Sahu, A. K., Swain, G. and Sekhar, K. R. (2016), Performance evaluation parameters of image steganography techniques, in *Proceedings of the 'Research Advances in Integrated Navigation Systems (RAINS)'*, IEEE, pp. 1–8.
- Radha, N. and Karthikeyan, S. (2011), 'An evaluation of fingerprint security using noninvertible biohash', *International Journal of Network Security & Its Applications (IJNSA)* **3**(4), pp. 1–11.

- Ratha, N. K., Connell, J. H. and Bolle, R. M. (2001), An Analysis of Minutiae Matching Strength, in *Proceedings of the 'International Conference on Audio-and Video-Based Biometric Person Authentication'*, pp. 223–228.
- Rathgeb, C. and Uhl, A. (2011), 'A survey on biometric cryptosystems and cancelable biometrics', *EURASIP Journal on Information Security* **2011**(1), pp. 1–25.
- Roy, R. and Changder, S. (2016), 'Quality Evaluation of Image Steganography Techniques: A Heuristics based Approach', *International Journal of Security and Its Applications* **10**(4), pp. 179–196.
- Sadkhan, E. S. B., Al-Shukur, B. K. and Mattar, A. K. (2016), 'Survey of biometric based key generation to enhance security of cryptosystems', pp. 1–6.
- Schrag, F. (1992), 'In defense of positivist research paradigms', *Educational researcher* **21**(5), pp. 5–8.
- Shahim, L. P., Snyman, D. P., Du Toit, J. V. and Kruger, H. A. (2016), 'Cost-Effective Biometric Authentication using Leap Motion and IoT Devices', *Securware* pp. 10–13.
- Stevens, M., Bursztein, E., Karpman, P., Albertini, A. and Markov, Y. (2017), The first collision for full SHA-1, in *Proceedings of the 'Annual International Cryptology Conference'*, pp. 570–596.
- Syed Ahmad, S., Mohd Ali, B. and Wan Adnan, W. A. (2012), 'Applications as access control tools of information security', *International Journal of Innovative Computing, Information and Control* **8**(11), pp. 7983–7999.
- Teoh, A. B., Kuan, Y. W. and Lee, S. (2008), 'Cancellable biometrics and annotations on biohash', *Pattern recognition* **41**(6), pp. 2034–2044.
- Uludag, U., Pankanti, S., Prabhakar, S. and Jain, A. (2004), 'Biometric cryptosystems: issues and challenges', *Proceedings of the IEEE* **92**(6), pp. 948–960.

- Vaishnavi, V. K. and Kuechler, W. (2015), *Design Science Research Methods and Patterns*, 2nd edn, CRC Press.
- Varchol, P. and Levick, D. (2007), 'Using of hand geometry in biometric security systems', *Radioengineering* **16**(4), pp. 82–87.
- Verma, G. and Sinha, A. (2016), 'Digital holographic-based cancellable biometric for personal authentication', *Journal of Optics (Online)* **18**(5).
- Wieringa, R. J. (2014), *Design science methodology for information systems and software engineering*, 1st edn, Springer.

Appendix A

SECURWARE2016

Conference paper published in the proceedings of The Tenth International Conference on Emerging Security Information, Systems and Technologies

During the design and proposal phases of this research, this conference paper was accepted for oral presentation at SECURWARE2016 under the category of idea paper (work in progress). The conference was held in Nice, France. The work that was presented, outlines the initial research directions that were envisioned. The paper was published in the proceedings of the conference after rigorous double-blind peer review. The feedback from the reviewers and comments from the delegates at the conference provided invaluable insight to establish the scope and the direction that the research in this dissertation ultimately addressed.

Contributions of authors:

- Shahim, Louis-Philip - Principle investigator and lead author
- Snyman, Dirk - Supervisor and presenting author
- Du Toit, Tiny - Co-supervisor and critical reader (technical)
- Kruger, Hennie - Co-supervisor and critical reader (conceptual)

Bibliographic reference: Shahim, L.P.; Snyman, D.P.; Du Toit, J.V.; Kruger, H.A. *Cost-effective biometric authentication using Leap Motion and IoT devices*. In Proceedings of Tenth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2016), eds. Carla Merkle Westphall, Hans-Joachim Hof, Geir Kjøien, Lukáš Králík, Martin Hromada, and Dora Lapkova. ISBN: 978-1-61208-493-0.; pp. 10-13.

Cost-Effective Biometric Authentication using Leap Motion and IoT Devices

Louis-Philip Shahim, Dirk Snyman, Tiny du Toit, Hennie Kruger

School of Computer-, Statistical- and Mathematical Sciences

North West University,

Potchefstroom, South Africa.

e-mail:lp.shahim6@gmail.com; {dirk.snyman, hennie.kruger, tiny.dutoit}@nwu.ac.za

Abstract — Biometric authentication is a popular method for information security defense and access control. With the availability of small computing Internet of Things (IoT) devices in conjunction with a hardware peripheral that is able to track hand geometry, multifactor authentication becomes cost-effective and mobile. The proposed system would attempt to authenticate system users by combining both a user's hand geometry scan, along with a series of gestures while simultaneously using machine learning classification techniques for user classification. Cancelability will be insured with a novel steganography implementation for user biometric information.

Keywords – *biometrics; information security; internet of things (IoT); leap motion; multifactor authentication.*

I. INTRODUCTION

Biometrics have long been used as an accepted user authentication method and have been implemented as a security measure in many real world systems including personal computers, mobile devices (cell phones and tablets), and also physical access control systems [1][2][3]. Biometrics are the digitalization and analysis of a person's innate physical or biological characteristics and the use thereof to distinguish between persons that are to be afforded access to specific systems, information or physical areas [1][3]. By encoding a person's physical attributes the disadvantages of traditional password based security, like passwords being lost or stolen, can be overcome [1][3]. One of the factors that hampers the acceptance of biometric authentication systems is that the cost of the development and implementation has traditionally been high due to factors such as biometric hardware, computational processing power, infrastructure integration, user training, and research and testing [1][3]. Cost still remains an ever present consideration for organizations when deciding to implement novel approaches over existing traditional methods. This factor raises the question whether traditional biometrics can be accomplished at a lower cost by using non-traditional methods and/or hardware.

With the current influx of new augmented computer interaction possibilities (i.e., new and non-traditional ways to control computers), a wide range of technological facets such as voice-, image- and movement control are receiving a lot of attention [3][4]. This leads to advancements in hardware capability and a definitive decrease in the cost of related hardware. Hardware peripherals (like the Leap Motion Controller (LMC)) that extend the basic functionality of computers to include support for the aforementioned facets are becoming more commonplace [2]. In order to facilitate these interactions, the hardware is implicitly working with information that can be harnessed for biometric identification. Chan *et al.* [2] mentions the possibility of partial sign language gesture

recognition using the LMC. The recognition of simple gesture interactions could be implemented as a form of biometric identification due to the latent biometric information it conveys.

The advent of the IoT movement [5][6] presents a myriad of small computing systems that display reasonable processing power and connectivity capabilities at a cost point far lower than traditional computer systems. The IoT is the interaction of everyday objects over the internet or similar networks by embedding computer systems that add smart functionality or an implied "intelligence" to these objects [5][6].

By combining the two above mentioned paradigms, this paper proposes a system that would implement the required hardware and software in an environment that uses augmented user interaction techniques in order to authenticate system users. Using a LMC for advanced hand scanning, a user would be able to gain access to a system or physical area (interfacing with electronic components of traditional security systems to be controlled by the RPi) by having their hand geometry scanned, combined with a series of gestures to incorporate a technique called multifactor authentication [2] in an inexpensive way. Because the LMC requires no direct touch (compared to traditional fingerprint scanners), an applicable scenario for such a system could be to allow medical surgeons access to an operating theatre once they have disinfected their hands and would not like to touch any surfaces before entering. By simply gesturing towards the authentication system, access will be granted if the surgeon is duly authorized thereto.

The rest of this paper is structured as follows: Section II presents system design in terms of security, hardware, interpretation of biometric information, and advantages and disadvantages. The conclusion and future direction for this research is presented in Section III.

II. SYSTEM DESIGN

A. Security considerations

Literature [1][3] mentions a series of considerations (other than cost) that should be central to decision making relating to biometric systems and the biometric traits on which the system functions. Among others, these include:

1) *Reliability* – The system needs to be always operational and available and therefore hardware should be able to handle many interactions without fail.

2) *Error incidence and accuracy* – Errors may be introduced to the system by external factors like user aging or environmental changes. The accuracy of the system (false-acceptance vs. false-rejection rates) should be balanced to ensure security while promoting usability.

3) *User acceptance* – Users need to embrace the technology in order for the biometric authentication method to be successful. Unobtrusive technologies get accepted more easily.

4) *Ease of use* – The biometric technology should be easy to use, preferably without extensive training.

5) *Security application* – The choice of biometric authentication method should fit the level of security expected for the specific application.

6) *Cancelability* – Cancelable biometrics (CB) refer to the obfuscation of stored personal biometric information in such a manner that prohibits the reconstruction of said information by third parties using computational techniques [9]. This ensures the anonymity of users who submit their data to biometric authentication systems by ensuring that their specific information is difficult to decipher by any party other than the intended system. One the main categories of CB is that of biometric salting [9]. This entails the transform of biometric information using transform parameters native to the user in question. E.g., using hand information retrieved from the LMC as transform parameters.

7) *Maturity of technology* – Traditionally the maturity of the technology, i.e., the technology is often implemented and how well it is supported, determines its longevity. This is also based on prevailing standards that are expected of a proven technology. The LMC, when implemented as a biometrics device, should conform well to these factors mentioned above except for the maturity of the technology. Due to the novel nature of the application it is to be expected that the maturity level is to be quite low.

B. Hardware

With the LMC's advanced hand and finger tracking capabilities, the position, velocity and orientation, supplemented by hand geometry information, are reported upon with accuracy and reduced latency [8]. Chan *et al.* [2] present the implementation of an LMC to assume the role of a biometric authentication device by harnessing the abovementioned information. The low cost factor of this device makes this implementation even more favorable in situations where cost is of substantial concern. One drawback of this approach is that the LMC is a peripheral device that still requires a computer system to connect it to as the device cannot function in a stand-alone way. This disadvantage will add to the associated cost of implementation. However, because the IoT is such a phenomenon presently, many low cost alternatives to traditional computer systems have become commonplace. One of the most widely known computer systems for IoT development is the Raspberry Pi (RPi) platform [6][7]. The RPi presents a balance between size, connectivity, processing power and cost making it an ideal IoT device to serve as an electronic interface (e.g., for interaction with existing physical security systems) alongside traditional computers that drive peripheral devices like the LMC. The information from the LMC can be analyzed locally using methods such as those described by Chan *et al.* [2] but augmenting the result of the analysis by transmitting instructions to the RPi to effect remote digital electronics based tasks, for instance the arming or disarming

of alarm systems across interconnected networks (like the Internet) where the RPi serves as an intelligent node for electronic systems interaction. The RPi can further be used for the communication with remote sensors such as movement- or sound sensors.

C. Interpreting biometric information

In order to interpret the implicit biometric information that is conveyed by the LMC and harness it in order to do biometric authentication, [2] proposes the use of machine learning techniques (see [8] for more examples on machine learning in biometrics). The readings obtained from the LMC (or other biometric devices) can be presented to a machine learning algorithm as features. The machine learning algorithms (each to their own internal structure) represent data that was gathered from users as a model against which to assess biometric access attempts at runtime. These models for biometric classification are usually biased to have a high precision, but low recall rate (i.e., to favor low false-acceptance rate at the expense of high false-rejection rates). The following algorithms are often implemented for biometric classification [2][8][11][12]: Naïve Bayes classifiers, Random Forest classifiers, Support Vector Machines, Gaussian Mixture Models, and Artificial Neural Networks.

D. Advantages/Disadvantages

Advantages of the proposed approach to biometric authentication include: *a)* Ease of use and convenience. *b)* The low cost factor. *c)* Security aspects should be good when compared to passwords because authentication is based on gestures and hand information that cannot be stolen or guessed. *d)* Auditability in terms of being able to connect users to a specific event or activity. *e)* Well suited for environments where typing is difficult or unwanted (e.g., surgeon in theatre).

Disadvantages include: *a)* The technology is still in its infancy and is not mature. *b)* While accuracy of authentication is expected to be high for small organizations, it may pose a problem with many users. *c)* Error incidence due to changes in a person's hands due to injury, old age, or illness.

E. Comparison with literature

Table 1 presents a cursory summary of a selection of systems from literature in comparison to the idea proposed in this paper. The proposed novelty of this idea is the combination of the resulting LMC biometric authentication system with an environment where IoT devices interact with existing security infrastructure. The idea further proposes the inclusion of novel cancelability by employing a new steganography approach for the storage and retrieval of biometric user information. The steganography algorithm will include biometric information of each user as transform parameters. To further illustrate the approach, Fig. 1 presents a graphical representation of the proposed algorithmic framework.

TABLE 1: COMPARISON OF SYSTEMS FROM LITERATURE.

Biometric device	Biometric task	Cancelability	Algorithm	IoT	
LMC	3D signature recognition	None specified	Naïve Bayes/Support vector machine	No	[11]
LMC	Gesture based biometrics	None specified	k -nearest neighbor classifier	No	[12]
LMC	Hand geometry and gestures	None specified	Random forest classifier	No	[2]
LMC	Hand geometry and gestures	Stenographical encryption based on biometric information	Machine learning classification and novel steganography	Yes	[this paper]

III. CONCLUSION AND FUTURE WORK

This paper presented the proposed idea of a LMC as a low cost biometric authentication device by its combination with an RPi as an IoT device. The next stage in this research will be to investigate different implementation possibilities. Further investigation into the underlying hardware and software topics is warranted to gauge the feasibility of these technological aspects before experimental implementation can commence. Issues in terms of information security that need to be investigated are: Classification methods need to be researched to ensure the highest possible accuracy of implemented classifiers. The implementation of secure cancelable biometrics to ensure user anonymity. Dlamini *et al.* [10] present the encryption of user credentials in transit and rest by using steganography to “hide” user information in images rather than commonly used user databases. If a common user database is breached, all of the users’ information contained therein may be exposed. Future work may include the incorporation of biometrics (read from the LMC) as parameters for use in such a steganography engine as implemented by Dlamini *et al.* [10]. This results in a steganography algorithm that encodes the user information in a picture based on their own unique traits rather than arbitrary encryption keys which may be computationally deduced. The premise is that even when one user’s information is identified from the image, the fidelity of other users’ information remains intact because the encryption parameters are unique to each user. Finally, extensive real world experimentation is planned with the resulting system to identify any inherent security flaws.

REFERENCES

- [1] S. Liu and S. Silverman, “A practical guide to biometric security technology,” *IT Professional*, vol. 3, no. 1, 2002, pp. 27-32.
- [2] A. Chan, T. Halevi, and N. Memon, “Leap Motion Controller for Authentication via Hand Geometry and Gestures,” In *Human Aspects of Information Security, Privacy, and Trust*, 2015, pp. 13-22.
- [3] A. K. Jain, K. Nandakumar, and A. Ross, “50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities,” *Pattern Recognition Letters*, 2016. [Online]. Available from: <http://www.sciencedirect.com/science/article/pii/S0167865515004365>. 2016.06.10.
- [4] X. Wang, S. K. Ong, and A. Y. C. Nee, “A comprehensive survey of augmented reality assembly research,” *Advances in Manufacturing*, vol. 4, no. 1, 2016, pp. 1-22.
- [5] F. Xia, L. T. Yang, L. Wang, and A. Vinel, “Internet of things,” *International Journal of Communication Systems*, vol. 25, no. 9, 2012, p. 1101.
- [6] M. Maksimović, V. Vujović, N. Davidović, V. Milošević, and B. Perišić, “Raspberry Pi as Internet of things hardware: performances and constraints,” *Design issues*, vol. 3, 2014, p. 8.
- [7] MagPi, “Raspberry Pi 3 is out now! Specs, Benchmarks & More,” 1 March 2016. [Online]. Available from: <https://www.raspberrypi.org/magpi/raspberry-pi-3-specs-benchmarks/>. 2016.03.01.

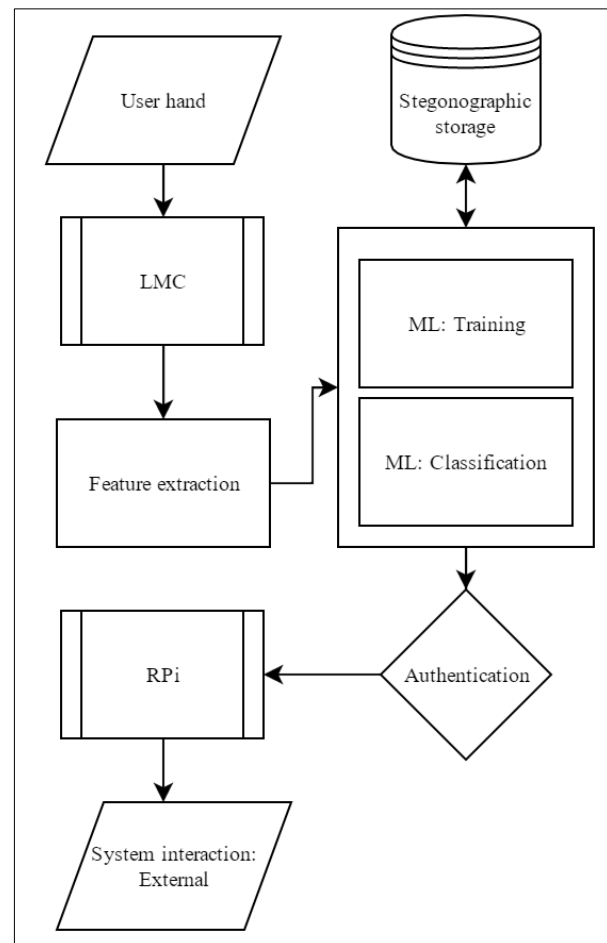


Figure 1. Graphic representation of the algorithm.

-
- [8] G. Damousis and S. Argyropoulos, "Four Machine Learning Algorithms for Biometrics Fusion: A Comparative Study," *Applied Computational Intelligence and Soft Computing*, vol. 2012, 2012, p. 6.
 - [9] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security* 2011.1, 2011, pp. 1-25.
 - [10] M.T. Dlamini, J. Eloff, H.S. Venter, M. Eloff, K. Chetty, and J. Blackledge, "Securing cloud computing's blind-spots using strong and risk-based MFA," In *International Conference on Information Resource Management*, 2016, pp. 58:1-28.
 - [11] I. Nigam, M. Vatsa, and R. Singh, "Leap signature recognition using hoof and hot features," In *2014 IEEE International Conference on Image Processing (ICIP)*, 2014, pp. 5012-5016.
 - [12] M. Piekarczyk and M.R. Ogiela, "On using palm and finger movements as a gesture-based biometrics," In *2015 International Conference on Intelligent Networking and Collaborative Systems (INCOS)*, 2015, pp. 211-216.

Appendix B

IARIA

Journal paper published in The International Journal of Advances in Security

The International Journal of Advances in Security publishes special issues, from time to time, that draws contributions from its sister conferences. Such contributions are selected by the editors of the journal based on the publications in the proceedings of the conferences. Based on the the relevance and recommendations from the peer review process, selected papers are invited to be extended for inclusion in the special issues of the journal.

The conference paper in Appendix A was selected for publication in the International Journal of Advances in Security and is subsequently presented here in Appendix B. The main results of the study were presented in this paper. Before publication, the paper subjected to a double-blind peer review.

Contributions of authors:

- Shahim, Louis-Philip - Principle investigator and lead author
- Snyman, Dirk - Supervisor and experimental design
- Du Toit, Tiny - Co-supervisor and critical reader (technical)

- Kruger, Hennie - Co-supervisor and critical reader (conceptual)

Bibliographic reference: Shahim, L.P.; Snyman, D.P.; Du Toit, J.V.; Kruger, H.A. Cancelable hand geometry-based biometric authentication system using steganography techniques. *International Journal of Advances in Security*, 2017, 10, pp. 134-144.

Cancelable hand geometry-based biometric authentication system using steganography techniques

Louis-Philip Shahim, Dirk Snyman, Tiny du Toit, Hennie Kruger

School of Computer-, Statistical- and Mathematical Sciences

North-West University,

Potchefstroom, South Africa.

e-mail: LP.Shahim6@gmail.com; {Dirk.Snyman, Tiny.DuToit, Hennie.Kruger}@nwu.ac.za

Abstract – Complex methods are often used in an attempt to rectify basic security aspects that should be prevalent in all authentication systems, but are lacking. Biometric information remains unique to each individual and it is for that reason that it should be protected, and yet many developers neglect the importance of securing biometrics effectively. This research presents a novel approach for authentication systems to protect biometric information using a combination of transformation techniques and steganography encryption methods. A leap motion controller captures user-specific biometric information. Once this information is retrieved, it is transformed or made “cancelable.” This ultimately prevents a third party from reconstructing the information to its original state. The concept of obfuscating biometric information seems inadequate without storing this information so that users may be authenticated. The shortcomings of storing this information become apparent should an attack occur on the database that holds the biometric information. One can breach a database and expose all the users’ personal information by simply gaining access to a username and password. To counter this threat, the use of image steganography to store user-biometric information in various pixels throughout an image is presented. By using cancelable biometrics combined with image steganography, biometric information can be safeguarded against reconstruction and possible identity theft prevented. The resulting framework presented in this paper shows promise to a novel cancelable biometrics approach using steganography.

Keywords- cancelable biometrics; information security; leap motion controller; multifactor authentication; steganography.

I. INTRODUCTION

Biometrics have long been used as an accepted user authentication method and have been implemented as a security measure in many real-world systems including personal computers, mobile devices (cell phones and tablets), and also physical access control systems [1]. Biometrics are the digitalization and analysis of a person’s innate physical or biological characteristics and the use thereof to distinguish between persons that are to be afforded access to specific systems, information or physical areas [1][2]. By encoding a person’s physical attributes the disadvantages of traditional password based security, like passwords being lost or stolen, can be overcome [1][3]. One of the factors that hampers the acceptance of biometric authentication systems is that the cost of the development and implementation has traditionally been high due to factors such as biometric hardware, computational processing power, infrastructure integration, user training, and

research and testing [1][3]. Furthermore, biometric systems present a unique challenge in terms of user privacy due to the personal nature of the biometric information that is stored in and used by the system [4].

The cost factor is one that decreases as continued development in the related hardware takes place. Alongside this development of dedicated biometric hardware there is an influx of new augmented computer interaction possibilities (i.e., new and non-traditional ways to control computers), a wide range of technological facets such as voice-, imaging- and movement control are receiving a lot of attention [3][4]. Image-control typically refers to facial recognition implementations, retina scanners and/or eye-tracking software that implement infrared imaging. In order to facilitate these interactions, the hardware is implicitly working with information that can be harnessed for biometric authentication. Hardware peripherals (like the leap motion controller (LMC)) that extend the basic functionality of computers to include support for voice and imaging facets are becoming more commonplace [2]. These peripherals are even used in biometrics research. For instance, Chan *et al.* [5] used an LMC for hand scanning and biometric authentication whereby a user would be able to gain access to a system, physical area or information by having their hand geometry scanned and analysed. They also posit the use of an LMC in multifactor authentication systems in combination with traditional passwords and PIN approaches.

Typically, this type of biometric authentication process follows the protocol of matching prior biometric templates (i.e., digitally formatted biometric features) that are stored within a database to the biometrics that are presented to the system during the biometric scanning process. This study proposes a system that expands on the existing techniques for biometric authentication with an LMC. This expansion uses techniques from steganography to store binary representations of the biometrics within an image as a biometric template alternative. The system does not merely store the raw biometric data within the image, but rather applies transform parameters to it. Only once the transform parameters have been added to the original biometrics are they stored/matched to authenticate and authorize the user. This ensures that each user’s biometric information is neither compromised, nor exposed. Cancelable biometrics refers to protecting the biometric information from third party scrutiny by

obfuscating this information (see Section II-A). This addresses the challenge of privacy of biometric information as mentioned above.

The objective of this research is to present the planning and development of a framework for a novel LMC hand-geometry authentication system that ensures the cancelability of biometric information by employing steganography techniques. Furthermore, this research also aims to present an illustrative example of the implementation of the steganography techniques for a cancelable biometric authentication system.

The remainder of this paper will be organized as follows: in Section II, background literature on the various related topics to this particular system will be discussed. Within Section III the proposed framework will be discussed, followed by an illustrative example in Section IV. In Section V, conclusions will be drawn and possible future work will be discussed. The final conclusion to the paper will be presented in Section VI.

II. LITERATURE STUDY

Within this section, the topics of *cancelability*, *steganography* and the use of an *LMC* for biometric authentication will be discussed in more detail. This section attempts to provide the reader with a better understanding of the individual topics and techniques before they are combined to create the proposed authentication system.

A. Cancelability

With the use of authentication systems becoming more prevalent, a primary concern becomes real-time processing of transmitted information as to verify a user's identity. The authentication process itself within traditional systems has evolved and often resorts to biometric information rather than passwords, tokens and/or secret keys [3]. This is primarily due to the inability of these traditional schemes to differentiate between an authentic user and an impostor. By authenticating users using biometric information the privacy of biometric data becomes important. Should attackers manage to gain access to the recognition system and its underlying data, the user-specific biometric information becomes readily available for identity theft. The biometric information should be protected. A possible solution would be to use multifactor biometric authentication with two or more biometric traits being employed. However, by adding more biometric features it will only add to the possible losses (should the system be compromised). Within the information security industry, one of the long acclaimed benefits of using biometric authentication has been that with post-enrolment biometric templates, user-specific biometric information (matching the stored template) could not be reconstructed. The benefit was refuted and once biometric templates become compromised, the biometric template is rendered useless [2]. This is because unlike passwords, biometric templates cannot simply be re-assigned due to their personal unique nature. Considering the susceptibility of such biometric authentication systems an approach to enhance the robustness can be used that is known

as cancelable biometrics (CB). This approach improves upon standard encryption algorithms that expose biometric templates during the authentication attempt by not supporting the comparison of templates within the encrypted domain [2]. Simply put, the encrypted domain referred to by CB ensures that data will remain secure in transit and in storage. Furthermore, CB allows for re-issuing and/or regenerating biometric information with a unique and independent identity. The process of transforming or repeatedly distorting the biometric feature using transform parameters that are predetermined rather than using the original biometric achieves this [1]. As to meet some of the major requirements regarding biometric information protection, biometric cryptosystems (BCS) and CB are designed so that biometric features are [2][3]:

- *Diverse* – Unable to be applied in multiple applications;
- *Reusable* – Reused/replaced in the event of compromise; and
- *Irreversible* – Computationally challenging to reconstruct the original biometric template, but simultaneously rudimentary to generate the protected biometric template.

Various approaches may be adopted when considering an implementation schema for biometric systems. However, one must consider the alternatives to an approach as to ensure that the chosen method is feasible. Thus, both BCS and CB are presented in order to gain an objective understanding.

BCSs are systems designed so that digital keys can be directly bound to a particular biometric [2]. One BCS approach is relevant to this particular study, namely biohashing, which implements a biometric key-generation. However, Rathgeb and Uhl [2] state that an implementation should not exist that directly generates keys from biometric templates. They elaborate that biometric features cannot provide sufficient information to reliably obtain lengthy and renewable keys without relying on helper data. Helper data is public information that is used within the key generation/retrieval process in a BCS [2]. This is useful to the study because helper data can be used to transform and obscure biometric information. Another approach to BCS is a biometric key-bind cryptosystem. This involves a secret key that relates to a biometric model by using helper data. To successfully implement this approach, facts regarding both the biometric model and the secret key may not be disclosed [6]. According to [2][7], implementation of key-binding cryptosystems can occur through a fuzzy commitment and a fuzzy vault. The concept of fuzzy incorporates the generation of helper data extracted from biometric features using a secrecy key. The abovementioned helper data, combined with the secrecy key are then both encrypted and stored in the database. In order to authenticate a user, the helper data then uses the model and biometric features to rebuild the key and match the generated template to the secure template [6]. Finally, if the templates match then the result will be positive and the user will gain access.

Having considered a BCS, one needs to weigh up the options regarding the possible approaches to cancelability and implementations thereof. Cancelability, too, has the sole purpose of ensuring computational challenges when attempting to retrieve/recover the original biometric data by a third party [2]. The focal point regarding cancelability remains that biometric characteristics should remain innately robust so that even when transform parameters are applied the biometric features do not lose value/individuality. Among individuality, by transforming biometrics one should ensure tolerance to intra-class variance so that the false rejection rate is not too high. Another important feature that cancelability has to offer is unlinkability [2]. This ensures that multiple transformed templates do not reveal any information relating to the original biometrics. In the unlikely event (assuming successful implementation) of data compromise, the transform parameters are simply altered, which simultaneously implies biometric template updates.

With regards to transforms within a CB implementation, two categories remain forthcoming, namely [2]:

- Non-invertible transforms; and
- Biometric salting.

The abovementioned approaches differ in performance, accuracy and security. Depending on the system that is to be implemented, a weighted feasibility analysis should be conducted on those particular factors in order to select the most suitable approach. These approaches are briefly discussed below.

1. Non-invertible transforms

This approach involves the use of a non-invertible function that is applied to the biometric template. By applying this function, stored templates can be updated when transform parameters are modified [2][8]. Therefore, security is increased due to the inability to reconstruct the biometric data even though transforms may have been compromised. With this advantage comes an equal and opposite disadvantage. A loss of accuracy and a performance decrease is the disadvantageous result thereof. This is due to transformed biometric templates becoming laborious in comparison processing, which ultimately provides fewer biometric results to process during matching (thus, influencing the accuracy thereof).

2. Biometric salting

Biometric salting commonly involves biometric template transforms that are preferred invertible as opposed to the non-invertible approach (abovementioned). The term “*salting*” refers to the act of merging specific data (such as passwords) with unique random values (“salt”) in order to make all of the original data distinct [9]. In this particular context, this technique may be applicable when a 4-digit PIN is used as the salt to be combined with the hand geometry vector prior to hashing the combination of data. This means that regardless of what biometric feature vector is chosen, the biometric template extraction

cannot be reconstructed to the original biometric template [2][7]. This commands that transform parameters have to remain private. Variations of the approach may appear if user-specific transforms are applied. However, this demands that each authentication attempt requires transform parameters, which may result in discrepancies if attackers successfully attain transform parameters. Ultimately, a decrease in performance is likely if the system implementation does not contain efficient biometric algorithms with high accuracy regarding private transform parameters. In contrast to non-invertible transforms, this approach maintains high recognition performance, however, the latter excels in terms of security [2][10].

According to Rathgeb and Uhl [2], even though it seems to be common to adopt non-invertible approaches to system implementation schemes, biometric salting seems superior. Not only does biometric salting increase performance, but in user-specific transform applications by incorporating two-factor authentication one can improve both security and accuracy.

To conclude this subsection, the aim is to combine the key-binding capabilities of a BCS with the biometric salting of CB. Once the user-specific biometric information has been transformed and is secure, it is ready for storage. In order to store this sensitive biometric information, rather than using a conventional database (due to its vulnerabilities, i.e., username/password exploits) a technique known as *steganography* was utilized.

B. Steganography

According to Kishor *et al.* [11], secret information is hidden using a type of communication, known as steganography. This is done through the use of multimedia files in cohesion with secret keys to embed information within these multimedia files. Steganography came about when it was realised that cryptography itself was incapable to securely transmit various forms of information across the Internet [12]. The word steganography can be translated from Greek into “covered writing” [13]. When hiding sensitive information, the information in question is typically concealed using an alternative format to that of its original. This is done through regeneration of data using multimedia formats. Some of these formats include text, image, audio and even video. For the purposes of this particular study, focus will be maintained upon image steganography and the shrouding of sensitive biometric information by means of bit encryption within the cover object (image). While cryptography disguises only the meaning of a message using code, steganography aims to hide the entire message from possible attackers [11][14].

The conventional flow of image steganography (as seen in Figure 1) follows a combination of encryption and decryption (just as cryptography does), but aims to use a confidential communication channel while secretly storing data and protecting the alteration of that data. Other applications that also make use of similar techniques, which are crucial to this particular study, include steganography as a conventional

database alternative [13], and encryption method for user authentication data [15].

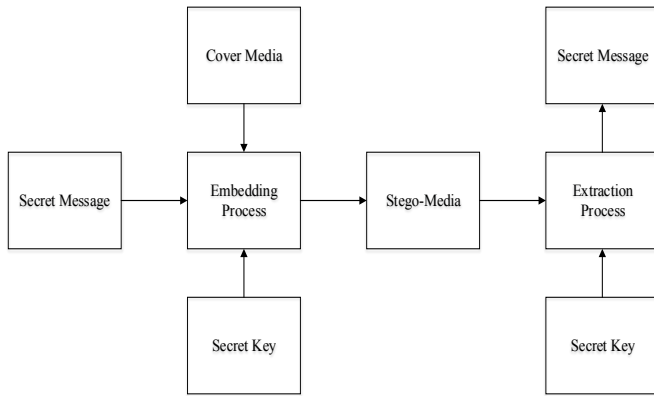


Figure 1. Conventional image steganography flow

In image steganography, both the encryption process and the decryption process involve the use of a cover image and a stego-image. In short, the difference between the two is merely that the stego-image contains the sensitive information, while the cover image can be seen as an empty data storage location for the sensitive information. In Figure 1, the steganography process requires sensitive information that is to be stored within the cover media (in this case, the image). This sensitive information is embedded into the image during the embedding process with the use of a secret key and a cover image to hide the information in. With the embedded information, the image is then referred to as the “*stego-image*.” The sensitive information can then only be extracted if the secret key is known.

Steganography can be implemented in various ways. However, the two major techniques that will be discussed regarding image steganography involve the following [4][14]:

- Spatial domain technique; and
- Transform domain technique.

The main difference between the two techniques is that when implementing a spatial domain steganography, the pixels within the image are directly manipulated. This is juxtaposed to the transform domain steganography that uses distinct transformations to allow image transformation in the transform domain and then only is the sensitive information stored with the image [14][16].

The purpose of modern steganography is to allow the host image protection so that the image itself, as well as the sensitive data it holds may not be recovered from the stego-image. By achieving this, the technique implemented is classified as irreversible steganography. The aforementioned objective is typically partnered with the ability to conceal sensitive information in a natural image in such a way that distortion of that image is minimal.

It is important to maintain that this particular study focusses on cancelable biometrics being stored using steganography techniques. This implies that the image may be distorted because even if an attacker manages to access the stego-image, he/she should not know what type of information is being stored, nor how to recover to biometrics after the transforms.

According to [12][14], steganography techniques are evaluated using various criteria. However, evaluation criteria that is relevant to this particular study are the following:

- *Hiding capacity* – This is the maximum amount of data that can be stored within an image with reference to bits per pixel (bpp). Comparatively speaking, a larger hiding capacity means the steganography technique is better.
- *Security Analysis* – The technique should be able to withstand attacks to the image that include any attempt to alter the image.
- *Robustness* – By being robust against attempts to attack the image statistically, as well as image manipulation attacks, the technique alone provides protection to the sensitive information hidden within the image.
- *Computational complexity* – With an algorithmic implementation, it is always important to take into consideration the time and space complexity.

An image can be seen as a two-dimensional function, where the $F(x, y)$ is the image pixels that can be represented as a grid. Each pixel contains ARGB (Alpha-Red-Green-Blue) values. Alpha values represent the pixel’s opacity and RGB values represent a particular colour within the colour system. These ARGB values range from (0, 0, 0, 0) to (255, 255, 255, 255). To embed data, one can either store information sequentially or randomly among various image pixels using the $F(x, y)$ grid layout. By using sequential embedding of data one makes the data more susceptible to steganalysis detection by clustering the sensitive information within the image grid [17]. Randomly embedding data complicates the detection process by scattering the data using a random number sequence. The proposed system aims to use steganography techniques in the storage and obscuring of sensitive biometric information within (an) image(s) once the biometric information has been transformed using CB techniques. In the next subsection, the means by which biometric information will be extracted using an LMC as the biometric scanner will be discussed.

C. The leap motion controller

With the LMC’s advanced hand and finger tracking capabilities, the position, velocity and orientation of all ten fingers, supplemented by hand geometry information, are reported upon with accuracy and reduced latency [8]. Chan *et al.* [5] presented the implementation of an LMC to assume the role of a biometric authentication device by harnessing the abovementioned information. The low-cost factor of this

device makes this implementation even more favorable in situations where cost is of substantial concern. One drawback of this approach is that the LMC is a peripheral device that still requires a computer system to connect it to as the device cannot function in a stand-alone way. This disadvantage will add to the associated cost of implementation.

The LMC is able to scan a human hand at approximately 100 frames per second (FPS). With the use of an LMC it is possible to extract all finger/bone measurements of any given hand during a scan. Any given combination of these measurements should be unique to every person [5]. The infrared scanner is then able to capture metrics relating to the hand and/or bones within the hand. As seen in Figure II, a model of the hand is then created based on the readings taken by the LMC.

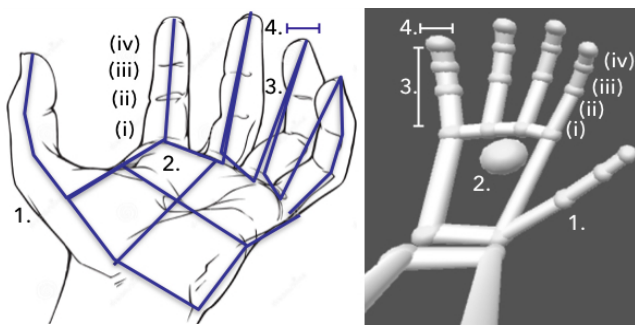


Figure II. Example of LMC generated hand model

Information retrieved from the hand scans can be seen in Table I. The LMC is capable of acquiring numerous metrics relating to any presented hand. A combination of Figure II and Table I provides an overview of the metrics that are relevant to the proposed system. It must be stated that i-iv can be further explained as the acquired lengths and widths of each of these bones.

Table I. Relevant LMC readings

	Readings		Bone
1.	Left/Right (Hand)	(i)	Metacarpal
2.	Palm Width (Hand)	(ii)	Proximal
3.	Length (Fingers)	(iii)	Intermediate
4.	Width (Fingers)	(iv)	Distal

All of the above information becomes relevant when attempting to authenticate users based on their hand-geometry. Although the LMC maintains great accuracy when gathering information regarding to the presented hand, the readings tend to differ depending on the position of the hand in relation to the LMC device itself. The readings show minimal discrepancy; however, this could become an issue when statistically analysing the false acceptance rate and false rejection rate of the final authentication system [18].

While scanning the hand using an LMC one can vary the length of the scans to acquire a larger data set for each user reading during the enrolment and storage phase. This allows for the system to iterate through the hand and its 19 bones (four bones per finger, except for the intermediate bone, which is non-existent in the thumb) within the fingers and retrieve the lengths of each of those bones.

With the use of an LMC, features can be extracted from presented hands, transformed to implement CB and stored using steganography techniques. A proposed framework to implement such a system is discussed in the following section.

III. PROPOSED FRAMEWORK

The prevailing architectures of biometric authentication systems consist of two main phases. These phases involve *enrolment* and *authentication*. The reason these two phases are required is so that during the authentication phase, the system has a biometric to compare to the biometric currently being presented to the system. This comparative biometric is typically referred to as a *biometric template*. During the enrolment phase, the biometric template is created for the user and then stored in a database. The manner within which the biometric template is created consists of several images being taken of the hand and then algorithmically extracting features from those images to create a final model for the specified user [19]. This entire enrolment phase can be simplified through the use of an LMC due to its ability to extract hand features from the internal LMC hand model that is created upon presentation of the hand. In order to comply with CB practices, this hand model has its features transformed mathematically, such that the original biometric information is not used in the transit/storage processes. The authentication phase simply compares the presented hands' extracted features to those of the models within the database. This authentication process would, therefore, also need to transform the presented biometrics in order to match it to the stored model.

Figure III represents the information (system structure) flow within the authentication system. The LMC initiates the information flow for the system when the hand is presented and immediately extracts features therefrom. Once the features are extracted, they can be transformed mathematically allowing for the enrolment phase to commence. In an attempt to further secure the biometric information, the decision was made to implement two-factor authentication. This is done by issuing a 4-digit PIN to each new user that is enrolled into the system. For implementation purposes, the use of 4-digit PINs allows for a maximum unique user capacity of nine thousand users (randomly generated and numbered from 1000 to 9999). The issued user PIN will determine where in the stego-image the biometric information is stored. By taking this approach, the system is then able to use two different images for storage (one for PINs and one for the biometrics).

In order to generate stego-images for sensitive information storage, one needs to specify exactly what images are made

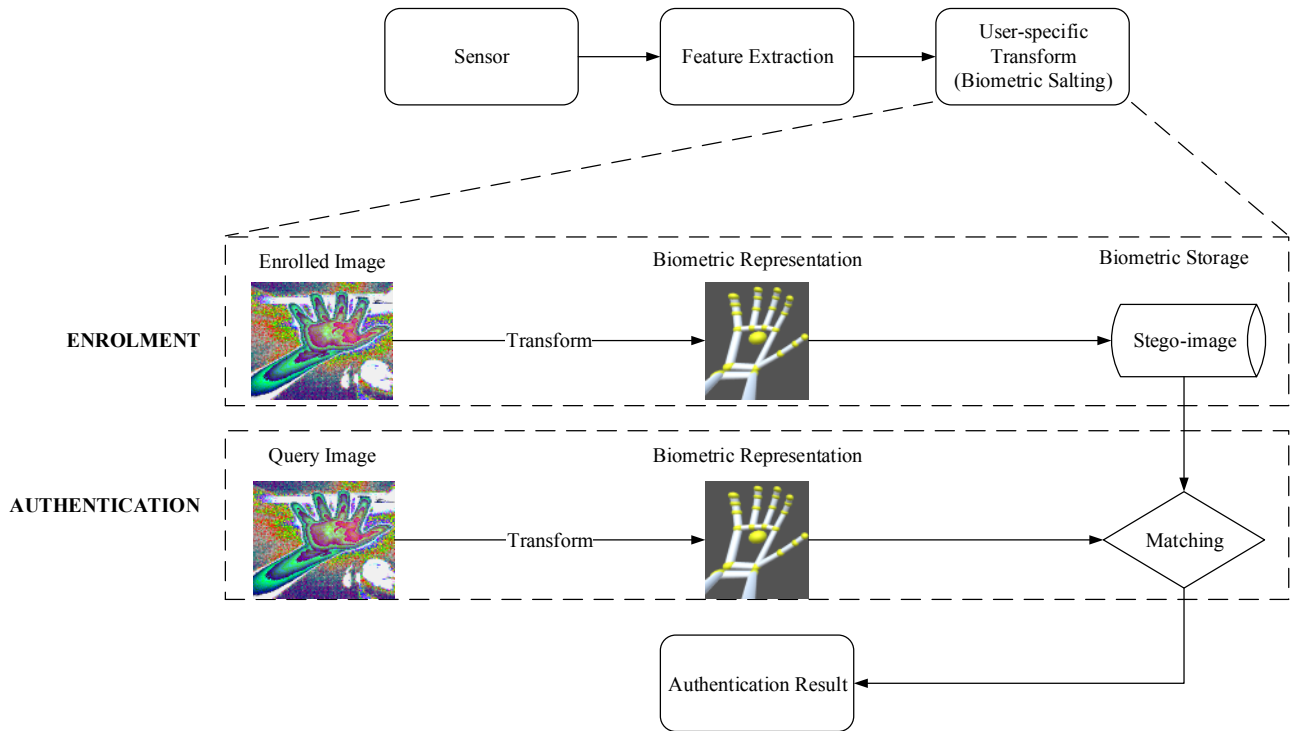


Figure III. System structure flow diagram

up of, how they are processed and how to programmatically generate them.

A. Stego-image contextualisation

An image can be seen as a two-dimensional matrix that is made up of pixels containing information about the colours within each particular pixel. This pixel information can be used to store sensitive biometric information. Using steganography techniques to store the transformed biometric models in an image involves that in order to store these models, each models' bit-data would have to be processed. All electronic information is essentially made up of 1's and 0's (or bits). This means that the models that are generated need to be manipulated in such a manner that each user model's bit data can be extracted for processing thereof. Once this bit data is processed, it can then be stored within an image to correspond to a particular user.

With two-factor authentication being applied, both the PIN and the hand geometry need to be stored. Using one image to store the PIN, the system can then use the stored PIN to enrol/locate a user in a second image. This can be likened to a one-to-one relational database model. To illustrate this concept, Table II shows how PIN information in the first image can be used to correspond to the hand geometry stored in the second image. For instance, in the first block of Table II, the bold number (1) represents the user ID slot number while 3648 is the user PIN. The corresponding slot in the second stego-image is then used as the storage location for the user hand geometry data.

In order to standardize the amount of data that can be used to store information within the pixels, the system uses 32bpp (bits per pixel) image formatting. This ensures that within each pixel of the image, 32 bits of information can be held. These 32 bits are made up of A (8 bits), R (8 bits), G (8 bits), and B (8 bits) values. Due to the fact that the number of bits used to store a 4-digit PIN would vary depending on the value, it was decided to also standardize the number of bits used during PIN storage per user. To do so, a hash-function is used [20].

The hash-function ensures that regardless of what the PIN is, the length of the hash representation will be similar. A SHA256 (Secure Hashing Algorithm 256-bit) function was chosen. This is because it is the successor of SHA1, which was compromised [21], and addresses the issues prevalent in SHA1.

Each PIN is made up of 256-bits (8 pixels, if one pixel = 32bpp), leading to 8 pixels to store user their information within both images. Referring back to the earlier statement of using two images with a one-to-one relationship, a user PIN can be mapped and correlated directly to the hand geometry in the second image using the hash function prior to enrolling the user.

Table II is an example illustration of user ID slots in correlation to the image pixels with an image resolution of 80 X 5. The first image is used to store hashed user PINs.

To generate the stego-image, the PINs are shuffled to ensure that the PIN-ID combination is not sorted such that PIN 1000 is stored in the first 8 pixels using the ID slot 1 etc.

B. Random PIN generation

To counter the threat of reverse-engineering the generated PINs, a program was written that generated 9 000 (unsorted) unique 4-digit PINs and mapped each PIN to an ID that ranged from 1-9000. An example of such a mapping is demonstrated using Table II to illustrate that PIN 3648 correlates to the user ID of 1. With this information generated and stored locally, using a conversion to bit data, stego-image 1 was generated so that all of the hashed PINs were stored and mapped. Stego-image 1 will, thus, remain unaltered after it has been generated. Stego-image 2 can then be altered during the enrolment phase. This is further explained below.

C. Stego-image generation

Stego-image 2 is a randomly generated image that will be altered as users enrol into the system. During the enrolment phase, users will be issued a PIN. Depending on the PIN he/she receives, a user ID correlating to that PIN is known by the system. Once the system has calculated the user ID based on the PIN that was entered by the user, the pixels within stego-image 2 can be altered using the hashed hand geometry of the enrolling user. By altering stego-image 2 in this way using stego-image 1, the authentication phase become more efficient because the pixels containing the biometric information can be directly read due to the mapping. The authentication process would be inefficient if the system had to search through the entire image each time a user presented their hand. Since an image can be seen as a matrix with 9 000 users, the complexity to compare and authenticate the presented hand geometry to the image would be $O(n^2)$ each time.

In order to gain a better understanding of how the system operates, the pseudo-code for the system is discussed.

D. Pseudocode for system algorithm

Keeping in mind the abovementioned information flow, as well as the mapping and stego-image generation, this pseudo-code should verify the exact functioning of the authentication system.

The pseudo-code below (Algorithm 1) aims to provide an overview of what input is retrieved within the system and to clarify how the two phases of biometric systems are applied based on the input retrieved from the user. As seen above, if the user is enrolled, the system merely transforms the presented hand geometry and authenticates the user by comparing the transformed information to that stored in stego-image 2.

Algorithm 1: Pseudocode for system algorithm


Input: PIN, Biometric Features {handID (hID), array[boneType (bT), boneWidth (bW), boneLength (bL)]}

Output: User-specific HashID for Steganography

```
function cancelableTransform(PIN, array[]
fingerBoneInfo) returns HashID;

    If (PIN == hID) && (enrolled == true)
    Then
        handGeo = Transform(fingerBoneInfo);
        Authenticate(getPixels(map), handGeo);
    Else
        newUser = Transform(fingerBoneInfo);
        EnrolUser(PIN, newUser);
    return HashID;
```

Table II. Stego-image 1: User IDs vs. their pixel correlation (10 IDs x 8 pixels per ID x 5 rows)

									
1, 3648	2, 7896	3, 5091	4, 4948	5, 3102	6, 7500	7, 1651	8, 6765	9, 6865	10, 7677
11, 5153	12, 1782	13, 2922	14, 2183	15, 1817	16, 6372	17, 1621	18, 8283	19, 2845	20, 6931
21, 2608	22, 3587	23, 6231	24, 5373	25, 3594	26, 1877	27, 3867	28, 1080	29, 2807	30, 6143
31, 7362	32, 4162	33, 8075	34, 8742	35, 7851	36, 3653	37, 8431	38, 4352	39, 1238	40, 2128
41, 7673	42, 2513	43, 8825	44, 5110	45, 5701	46, 6623	47, 5963	48, 1703	49, 3697	50, 2073

However, if the user has not been enrolled, he/she then is issued a PIN and the presented hand geometry is transformed and stored within stego-image 2, correlating to the issued PIN location.

Next, the advantages and disadvantages of the system will now be discussed.

E. Advantages/Disadvantages

The use of the current implementation of this authentication system has its advantages and disadvantages.

Advantages of the proposed system include:

- The low-cost factor;
- Ease of use and convenience;
- The security aspects are superior when compared to passwords because authentication is based on a combination of PIN and hand information that cannot be stolen or guessed; and
- Auditability in terms of being able to connect users to a specific event or activity.

The disadvantages include:

- The technology is still in its infancy and is not mature;
- While system performance for authentication is expected to be high for small organizations, it may pose a problem should more users need to be enrolled; and finally
- Error incidence due to changes in a person's hands due to injury, old age, or illness.

The following section will provide an illustrative example of the system.

IV. ILLUSTRATIVE EXAMPLE

In this section, a simplified example of a user being authenticated is presented in order to provide a holistic view to the combination of the topics discussed in previous sections.

With each hand that is presented to the LMC a model is created that is either used for enrolment or for authentication. Assuming that the user-hand that is presented has already undergone enrolment, the LMC will create a model using a particular transform parameter to compare this model to the binary representation of the hand already stored within stego-image 2. By using the PIN that is entered prior to hand scanning, the system ensures that the users' transformed biometric representation can efficiently be compared to the newly transformed model. This is efficient because the system has mapped the PINs to pixel IDs, rather than having to search the entire image for the corresponding biometric representation.

Consider the explanation on the next page of the illustrative example shown in Figure IV.

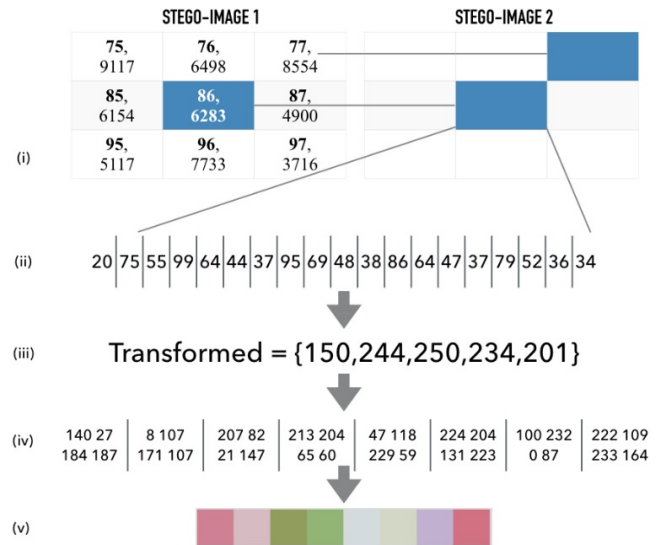


Figure IV. Example of biometric vector reading and transformation

- (i) Assume the user was presented with the PIN **6283** during enrolment. The user would then have a dedicated storage section with the ID of **86** in both stego-image 1 and in stego-image 2. During the authentication phase the user will have his/her hand geometry scanned to compare the presented hand to the binary representation stored within stego-image 2.
- (ii) During the abovementioned scan, the hand geometry of the user is mathematically generated by using various combinations from the thousands of readings gathered to form one vector (readings for each of the 19 individual bones in his/her hand).
- (iii) By using the vector created in (ii), the system then transforms the biometric vector once more in order to implement CB (as discussed in Section II-A). In this particular example, the vector was simply transformed by adding each finger's bone readings together (3 readings for the thumb and 4 readings for all the other fingers). It should be noted that more complex mathematical transformations are recommended for the actual implementation.
- (iv) The system further protects the biometric information by applying a SHA256 hash function to the vector. This vector is then represented as a byte array consisting of 32 values from the 256-bit hash function. Ultimately, this ensures that each user only uses 8 pixels within both the stego-images.
- (v) Once the byte array has been generated, it can then be compared to the stored biometric representation within ID **86** consisting of 8 pixels.

Upon completion of the abovementioned process, the system will either accept the user as successfully authenticated, or the system will reject the user and ask for the hand to be re-scanned.

By using steganography techniques, the system ensures imperceptibility and cancelability. Figure V provides a comparative view of two generated images for their use in this context.

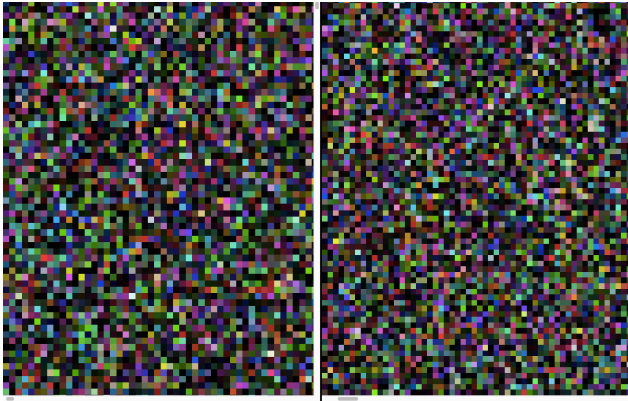


Figure V. Randomly generated image versus stego-image

The image on the left was randomly generated, while the image on the right contains sensitive biometric information. To the human eye one cannot easily infer that these two images differ, however, upon closer inspection one may realize differing colour mappings but cannot differentiate between sensitive data and just another randomly generated image.

Ultimately, cancelability can be concluded due to the biometric information being transformed and obscured prior to storage. This means that should an attacker find these two images in a compromised system, he/she will not know what information was used to generate these images, nor how the information was transformed prior to storage. In fact, without prior knowledge he/she will not even know to expect hidden data in said images.

V. EVALUATION AND DISCUSSION

In an attempt to quantify the performance of the proposed system, a threefold evaluation was instantiated and conducted. This is presented in terms of the consistency of the LMC, followed by a comparative vector tolerance analysis and finally, the overall system accuracy. Thereafter a discussion is presented. The following evaluation and discussion are based on sample data that was collected through the scanning (enrolment and authentication) of forty candidates.

A. LMC performance evaluation

To illustrate the efficiency and reliability of the LMC, the data that was collected from one randomly selected, five second hand geometry scan is presented in both Table III and Figure VI below.

In order to present a visualisation with a high enough resolution to be able to see the variance in the scan readings, only the three fingers most similar in length are shown (i.e., the index, middle, and ring fingers).

Table III. Standard deviation of finger readings (mm)

Thumb	Index	Middle	Ring	Pinkie
0.197203783	0.424346553	0.464246258	0.438259197	0.35738522

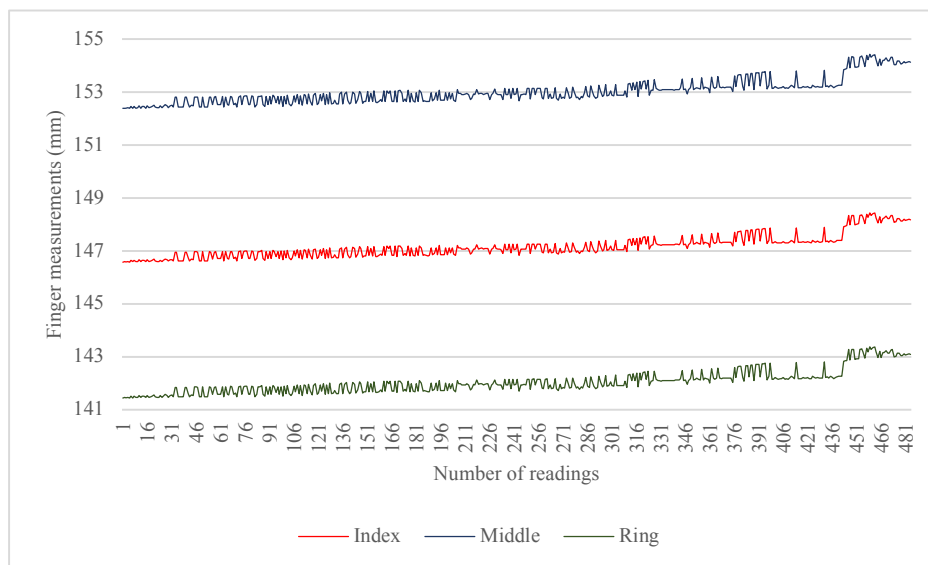


Figure VI. Measurement consistency for LMC

The significance of this data is prevalent when taking into consideration the distribution throughout the scan. It is of utmost importance to consistently extract concise data readings throughout the length of the scan. Thus, the standard deviation of the raw data correlating to the plotted data was calculated in an attempt to demonstrate the accuracy that the LMC provides (see Table III).

It is interesting to note that the longer the scan has progressed, the more varied the readings become. This is attributed to the instability that is associated with an unsupported hand being held in mid-air for any given period of time.

B. Comparative vector tolerance

Despite the abovementioned LMC accuracy, the system shows slight deviation from one scan to the next. To provide an explicit limit regarding the deviation of the readings during a scan, it was decided to measure a tolerance range.

The manner within which this tolerance range was calculated involves comparing test data from user enrolment scan to that of the associated authentication scan. This data includes all of the users and their transformed vector combinations. With this data, the maximum tolerance range was extrapolated based on the variations produced by the system. As seen in Figure VII below, it was concluded that the maximum tolerance range for this data set is 5mm.

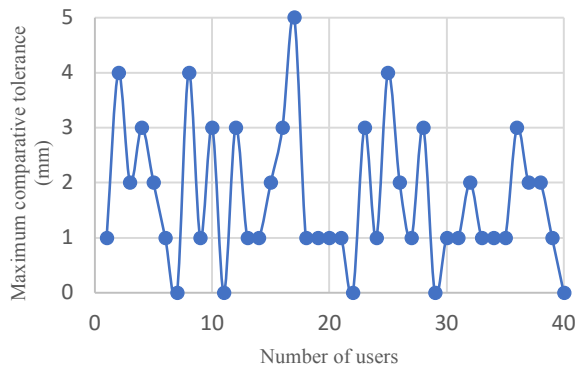


Figure VII. Maximum comparative tolerance levels

Upon further evaluation, with the tolerance range at a maximum of 5mm, the acceptance rates exponentially improved. This, however, increased the processing time to find a positive match within the tolerance range of the transformed vector.

C. Overall system evaluation

As deduced from Figure VIII, a zero-tolerance rate resulted in only a 12.5% true acceptance rate. If this tolerance is then increased, the true acceptance rate also increases (e.g. 97.5% with a 4mm tolerance) until a 100% true acceptance rate is obtained at 5mm tolerance.

When considering implementing this particular system approach, one needs to determine what risk factor is suitable within the authentication scenario. If the users that need to be authenticated are to be granted access to sensitive data/areas, then the tolerance range should be adjusted accordingly. The acceptance rate is drastically affected when using the maximum tolerance range. With such a high tolerance range,

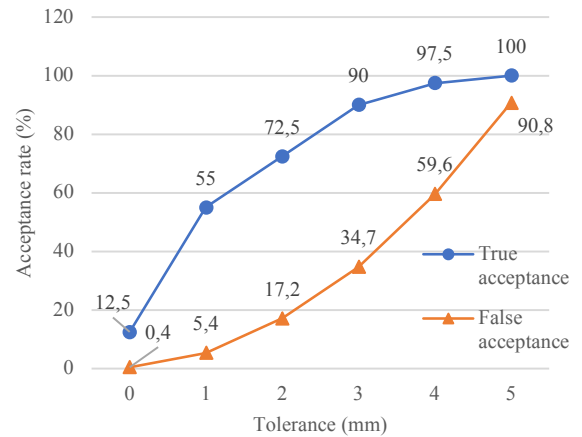


Figure VIII. Acceptance rates based on dynamic tolerance range

the false acceptance rate is also dramatically increased, but because of the two-factor authentication provided with the allocated PIN, the users are authenticated correctly.

D. Discussion

The proposed technique has revealed several promising advantages by using a combination of the techniques specified in Section II. The LMC was found to be a stable and efficient hand geometry scanner. Also, the steganography techniques used in this paper were relatively easy to implement for use in this particular instance. By using PINs (to implement two-factor authentication) the security is enhanced and aids in achieving cancelability for storing biometrics. The proposed framework ensured that the system provided results that were reliable and efficiently obtained.

Bearing in mind the abovementioned advantages, one must acknowledge some disadvantages are present when using this approach. This system was only exposed to limited testing and the authentication accuracy and robustness will need to be measured using a formal evaluation. In order to fully explore the system's functionality, one would have to extensively test the use of this framework on a larger scale. This will form part of the ongoing research.

VI. CONCLUSION

This paper presented the planning and development of a framework for a novel LMC hand-geometry authentication system that ensures the cancelability of biometric information by employing steganography techniques. The research presented favours authentication using intrinsic and

distinctive traits of each system user's biometric information with multiple advantages over conventional password-based authentication systems. With the use of this novel approach the privacy concerns mentioned earlier are addressed by implementing CB techniques; paired with steganography techniques that have consistently been used to conceal sensitive information. The resulting stego-image generation and biometric storage process shows promising results in achieving biometric cancelability.

REFERENCES

- [1] L. Shahim, D. P. Snyman, J. V. Du Toit, and H. A. Kruger, "Cost-Effective Biometric Authentication using Leap Motion and IoT Devices," *Secureware2016*, pp. 10–13, 2016.
- [2] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Secur.*, vol. 2011, no. 1, pp. 1–25, 2011.
- [3] G. Verma and A. Sinha, "Digital holographic-based cancellable biometric for personal authentication," *J. Opt.*, vol. 18, no. 5, 2016.
- [4] P. P. Paul and M. Gavrilova, "Multimodal Cancelable Biometrics," in *2012 IEEE 11th International Conference on Cognitive Informatics and Cognitive Computing*, 2012, pp. 43–49.
- [5] A. Chan, T. Halevi, and N. Memon, "Leap Motion Controller for Authentication via Hand Geometry and Gestures," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, Springer International Publishing, 2015, pp. 13–22.
- [6] P. Eng and S. B. Sadkhan, "Enhance Security of Cryptosystems," 2016.
- [7] P. P. Paul, M. Gavrilova, and S. Klimenko, "Situation awareness of cancelable biometric system," *Vis. Comput.*, vol. 30, no. 9, pp. 1059–1067, 2014.
- [8] E. Piciucco, E. Maiorana, C. Kauba, A. Uhl, and P. Campisi, "Cancelable biometrics for finger vein recognition," in *2016 First International Workshop on Sensing, Processing and Learning for Intelligent Machines (SPLINE)*, 2016, pp. 1–5.
- [9] S. Syed Ahmad, B. Mohd Ali, and W. A. Wan Adnan, "Applications As Access Control Tools of Information Security," *Int. J. Innov. Comput. Inf. Control*, vol. 8, no. 11, pp. 7983–7999, 2012.
- [10] N. Radha and S. Karthikeyan, "An evaluation of fingerprint security using noninvertible biohash," *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 4, 2011.
- [11] S. N. Kishor, G. K. Ramaiah, and S. A. K. Jilani, "A review on steganography through multimedia," in *Research Advances in Integrated Navigation Systems (RAINS), International Conference on*, 2016, pp. 1–6.
- [12] R. Jain and J. Boaddh, "Advances in Digital Image Steganography," *Int. Conf. Innov. Challenges Cyber Secur.*, no. Iccics, pp. 163–171, 2016.
- [13] A. S. Pandit and S. R. Khope, "Review on Image Steganography," vol. 6, no. 5, pp. 6115–6117, 2016.
- [14] A. Pradhan, A. K. Sahu, G. Swain, and K. R. Sekhar, "Performance Evaluation Parameters of Image Steganography Techniques," in *International Conference on Research Advances in Integrated Navigation Systems*, 2016.
- [15] M. Dlamini, M. Eloff, J. Eloff, H. Venter, K. Chetty, and J. Blackledge, "Securing Cloud Computing 's Blind -spots using Strong and Risk-based MFA," in *International Conference on Information Resource Management*, 2016, p. 58: 1-28.
- [16] R. Roy and S. Changder, "Quality Evaluation of Image Steganography Techniques : A Heuristics based Approach," *Int. J. Secur. Its Appl.*, vol. 10, no. 4, pp. 179–196, 2016.
- [17] S. A. Laskar and K. Hemachandran, "Steganography based on random pixel selection for efficient data hiding," *Int. J. Comput. Eng. Technol.*, vol. 4, no. 2, pp. 31–44, 2013.
- [18] A. Nagar and A. K. Jain, "On the security of non-invertible fingerprint template transforms," in *Information Forensics and Security, 2009. WIFS 2009. First IEEE International Workshop.*, 2009, pp. 81–85.
- [19] P. Varchol and D. Levický, "Using of hand geometry in biometric security systems," *Radioengineering*, vol. 16, no. 4, pp. 82–87, 2007.
- [20] Y. Kashyap and R. Sharma, "A survey on various authentication attacks and database secure authentication techniques," *Int. J. Multidiscip. Educ. Res.*, vol. 5, no. 15, pp. 67–81, 2016.
- [21] R. Brandom, "Google just cracked one of the building blocks of web encryption (but don't worry) - The Verge." [Online]. Available: <https://www.theverge.com/2017/2/23/14712118/google-sha1-collision-broken-web-encryption-shattered>. [Accessed: 27-Aug-2017].

Appendix C

Minimum system requirements

To successfully use the proposed authentication system that supports the Leap Motion Controller peripheral device, the following minimum system requirements need to be met.

- i. Windows 7+ and/or Mac OS X 10.7 +;
- ii. AMD Phenom II or Intel Core i3/i5/i7 processor;
- iii. 2GB RAM; and a
- iv. USB 2.0 port