Cancelable biometrics using hand geometry-based steganographic techniques

Louis-Philip Shahim

Supervisor: D.P. Snyman

Department of Natural Sciences
North West University, Potchefstroom

This dissertation is submitted for the degree of
Master of Computer Science and Information Systems

NWU September 2017

I would like to dedicate this thesis to my loving parents …

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. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements. This dissertation contains fewer than 65,000 words including appendices, bibliography, footnotes, tables and equations and has fewer than 150 figures.

Louis-Philip Shahim
September 2017

Acknowledgements

And I would like to acknowledge ...

Abstract

This is where you write your abstract ...

Table of contents

List of figures

List of tables

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 perverse 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 ourselves, 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 Silverman, 2001:27–32). Biometric information remains the most personal of possessions. 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 below.

The use of basic authentication systems can almost be classified as defunct, due to the fraudulent attacks becoming more commonplace. It is because of this that researchers are continuously looking for more secure forms of information protection. One of the main downfalls of basic authentication systems is the vulnerability that occurs within storage and in transit of attackers being able to intercept sensitive authentication information. Thus,

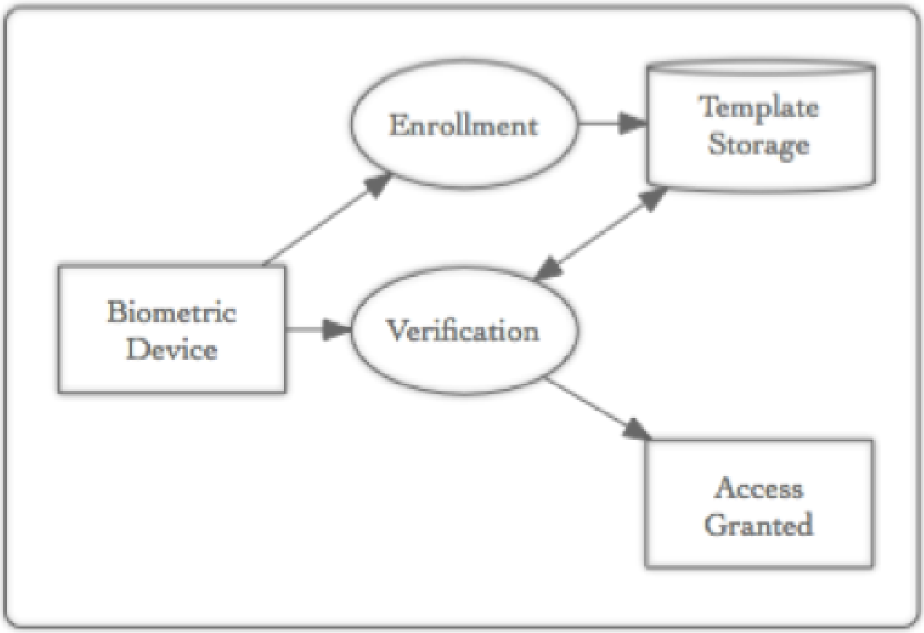


Fig. 1.1 Basic authentication process model

cryptosystems were initiated. A biometric cryptosystem is an implementation technique for authenticating users by incorporating template protection (Uludag et al., 2004:948–960). 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., 2016:1–6). This brings about the concept of combining cancelable biometrics with steganography. To summarize, 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.

The most famous equation in the world: $E^2 = (m_0c^2)^2 + (pc)^2$, which is known as the **energy-mass-momentum** relation as an in-line equation.

A *LaTeX class file* is a file, which holds style information for a particular LaTeX.

$$CIF: \quad F_0^j(a) = \frac{1}{2\pi\imath}\oint_\gamma \frac{F_0^j(z)}{z-a}dz \tag{1.1}$$

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 Silverman, 2001). By encoding a person's physical attributes the disadvantages of traditional password based security, like passwords being lost or stolen, can be overcome (Jain et al., 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 Uhl, 2011).

The concept of Cancelable Biometrics (CB) has to do with 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 anonymity of users within 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 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 the original data can be obtained for use in a biometric system. This approach usually relies on a static salting algorithm which can be 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 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 within 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 within security systems.

To capture biometric information, Chan et al. (2015) presents 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.

Thus, 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 question

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

1.4 Aims 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. In figure 1.2 To achieve the primary objective, the following secondary objectives need to be met:

i. With the use of a literature review, 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.

1.5 Research method

1.5.1 Introduction

For the sake of transparency, this section intends to discuss various research paradigms that were considered for this study, 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

1.5.2.1 Introduction to interpretivism

According to Oates, interpretivism refers to the researcher's ability to analyse an information system by means of comprehending the processes within its development in terms of social factors (Oates, 2006, p. 292). These social factors involve the people that created the systems and the dependencies from a social standpoint within 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 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, thus, 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. This particular researcher should ensure that he/she possesses a non-neutral perspective in order to interpret the topic in a manner that is influence by the various social factors.

1.5.2.3 Characteristics of interpretivistic approach

Because 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 within the setting are associated and unified. Interpretivistic research paradigms have the following characteristics (Oates, 2006, p.292):

i. Realities that are subjective. This means that the concept of ‘truth’ is based on perspectives and that one researchers’ perception is likely to differ from another researcher’s, simply because of the construction of knowledge that takes place within each of our own minds.

ii. Volatile construction to meaning based on social factors. This means that the researcher is 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. This research is dependent on the researcher’s personal opinions.

iv. Analysis of research subjects within their social settings. This means that the researcher attempts to comprehend people within their natural settings 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. This means that 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. This means that 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 amounts of information and finally concluding the study.

1.5.2.4 Interpretivistic critique

Interpretivism involves studying social factors relating to specific social settings and behaviors within 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 as a positivistic approach would.

1.5.2.5 Interpretivistic methods

The methods used within interpretivism are ethnography and case studies. Within 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 setting.

ii. Case studies have the focal point that ensures one specific ‘target’ is examined. This target can be analyzed 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 generation techniques are crucial in providing evidence for the conclusions that are drawn by the researcher. This evidence can be regarded as valid if they are generated using the following techniques (Oates, 2006, p.295):

i. Interviews;

ii. Observation;

iii. Document analysis; and

iv. Field notes.

1.5.3 Positivistic paradigm

1.5.3.1 Introduction to positivism

According to Jokobsen, positivism refers to the positions within philosophy that accentuate both scientific methods, as well as, data that is empirical (Jokobsen, 2013). Within the Business Dictionary, positivism is a concept that perceives true knowledge to be that that is directly linked to scientific knowledge based on what is observed. It is then stated that empiricism is extended within positivism (Business Dictionary, 1999). 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 epistemology

The ontology of positivism is 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 stand-point and is objective in his/her approach. With regards to epistemology in positivism, is 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 positivistic approach

Because positivism is based on a 'scientific approach' to research, the researcher is expected to share a worldview with that of either positivistic researchers. Various assumptions can be made by these researchers that include common characteristics. According to Oates, these characteristics include the following (Oates, 2006, p. 286):

i. Measuring and creation of models. This means that the researcher is able to observe the world according to the positivistic ontology and using this view is able to create models of this perceived world according to the 'facts' obtained through scientific methods.

ii. The objective approach. This means that 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 means the use of empiricism within the testing of various theories or the refuting of these theories.

iv. Data analysis using quantitative methods. This means that within the positivistic approach, the preferred data analysis technique is that of a quantitative nature. This involves creation of mathematical models to logically and objectively analyse the given results and observations.

1.5.3.4 Positivism critique

Because the positivism involves studying aspects relating to the natural world, researchers who prefer other methods are likely to impose on this technique. Positivism is a very general approach to research and it cannot always be used to generalize the ontology of things. This shows that there are not always predictable patterns and that research can evolve around various natural interpretations.

1.5.3.5 Positivistic methods

The method used within positivism is a scientific method. Within this method, it can be assumed that objectivity is crucial within our investigation, and that the world could be viewed as an orderly entity that does not operate in a random fashion (Oates, 2006, p. 283). With the use of the scientific method, it can be stated that various characteristics of positivism are used. Such characteristics include reducing problems, repeatability of processes and finally refuting theories. The scientific method runs through 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 methods used within positivism are structured and involves a set process by stating the research assumption and then either accepting or rejecting the assumption based on objective observation and analysis.

1.5.3.6 Data gathering techniques and analysis

Various data gathering techniques may be used within positivistic research. Such techniques mainly involve experiments. However, other methods such as the sending out of surveys and questionnaires. 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 (DSR)

1.5.4.1 Overview

A general definition for research would be an activity that aids in the detailed comprehension of a specific phenomenon (Vaishnavi Kuechler, 2015). In contrast to the aforementioned definition, DSR allows for 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 (1997) proposes that through action, knowledge can be generated. Critics occasionally consider this approach to lack in rigor. 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 within a research community (Vaishnavi Kuechler, 2015).

1.5.4.2 DSR process model

The DSR process model can be seen below in Figure 2 (Vaishnavi Kuechler, 2015). This precedes the descriptions of each of the phases in the next section.

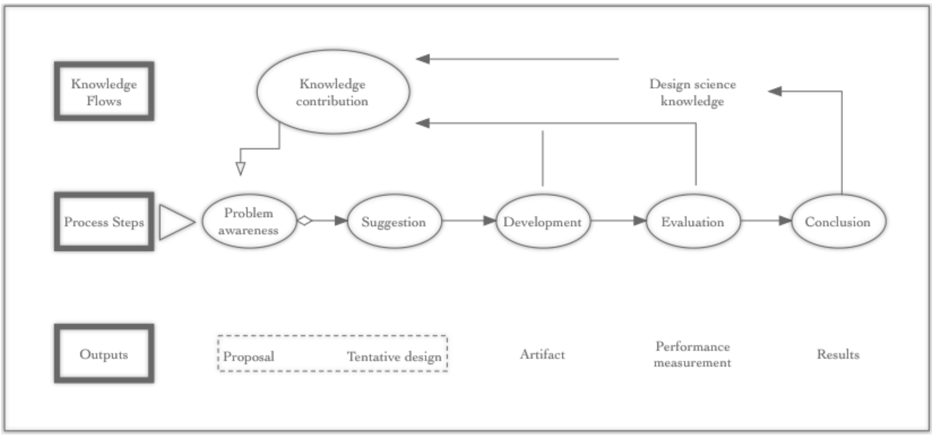


Fig. 1.2 DSR Process Model

1.5.4.3 Phases

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 within allied disciplines). In this way, the researcher may come across new developments to propose improved approaches. As seen in the above figure, 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 into 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 extend upon 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 the problem exploration may be confirmed or acquitted.

v. Conclusion

By concluding the study, the researcher typically states whether the results sufficed the hypothesis or 'problem exploration' 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.

1.5.5 Conclusion

Upon completing a full 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 due to 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.

1.6 Deployment

Within chapter 2, further research will be conducted on related topics to the explored problem. This research will take an in-depth look at 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, the expansion upon these subsections will include what each element consists of, how they work, how they suit this study and finally how they will be implemented. In chapter 3, the system design will be described with regards to its various elements and the chosen approach for each element will be discussed at length. In chapter 4, experimentation will commence by analyzing data extraction techniques, as well as testing algorithm efficiency based on extraction, processing and storing biometric information within the suggested system. Chapter 5 will involve evaluation of the system based on implicit criteria set out within the proposal and design of the suggested model. Finally, chapter 6 will conclude the study by justifying the problem exploration based on results attained.

1.7 Chapter summary

Within this chapter the basics concepts relating to this study were explained. This chapter is introductory to the purpose of the study, what the preliminary aims and objectives are and what research method will be followed. Finally, a brief over regarding the layout for the remainder of the study is given.

Chapter 2

Related research

2.1 Introduction

2.2 Biometrics

2.3 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 [2]. The benefit was refuted and once biometric templates become compromised, the biometric template is rendered useless. 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 cancelable biometrics (CB) are designed so that biometric features are [2][3]:

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 as to ensure that the chosen method is feasible. Thus, both BCS and CB are presented in order to gain an objective viewpoint. 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 [5]. According to [2][6], 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 [5]. A structural representation of this method can be seen below in Figure 1.

Figure 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' hand, the current information within the system is then matched to that of the template that is stored within 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 abovementioned 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 3rd 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 (FRR) is not too high. The most important feature that cancelability has to offer is unlinkability. 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]:

i. Non-invertible transforms; and

ii. 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.

i. 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][7]. 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).

ii. 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 [8]. 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][6]. 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][9].

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.

2.4 Steganography

According to Kishor et al. [10], 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 realized that cryptography itself was incapable to securely transmit various forms of information across the internet [11]. The word steganography can be translated from Greek into "covered writing" [12]. 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 [10][13]. The conventional flow of image steganography (as seen in Figure 2) 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 [12].

Figure 2 : 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 2, 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 [13] [4]:

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 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[13][14]. To broaden the scope of steganography even more, literature states that spatial and transform domain techniques branch out into subcategories of implementation [3][8][9]. A few examples of these methods can be seen in the Table 1.

Table 2.1 Steganography methods

Spatial Domain	**Transform Domain**
Least Significant Bit (LSB) substitution	Discrete Cosine Transform (DCT)
Pixel Value Differencing (PVD)	Discrete Wavelet Transform (DWT)
Random pixel selection	Discrete Fourier Transform (DFT)

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 [11][13], steganography techniques are evaluated using various criteria. However, evaluation criteria that is relevant to this particular study are the following:

i. 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.

ii. Security Analysis – The technique should be able to withstand attacks to 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 within the image.

iv. 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 [15]. 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 a(n) 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.

2.5 Leap motion controller (LMC)

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. [2] 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 [16]. The infrared scanner is then able to capture metrics relating to the hand and/or bones within the hand. As seen in Figure 3, a model of the hand is then created based on the readings taken by the LMC.

Figure 3 : Example of LMC generated hand model

Information retrieved from the hand scans can be seen in Table 2. The LMC is capable of acquiring numerous metrics relating to any presented hand. A combination of Figure 3 and Table 2 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 2.2 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 FAR/FRR (False-Acceptance-Rate/False-Rejection-Rate) of the final authentication system [17]. 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) 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.

2.6 Conclusion

2.7 Chapter summary

I'm going to randomly include a picture Figure 2.1.

If you have trouble viewing this document contact Krishna at: kks32@cam.ac.uk or raise an issue at https://github.com/kks32/phd-thesis-template/

Enumeration

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed vitae laoreet lectus. Donec lacus quam, malesuada ut erat vel, consectetur eleifend tellus. Aliquam non feugiat lacus. Interdum et malesuada fames ac ante ipsum primis in faucibus. Quisque a dolor sit amet

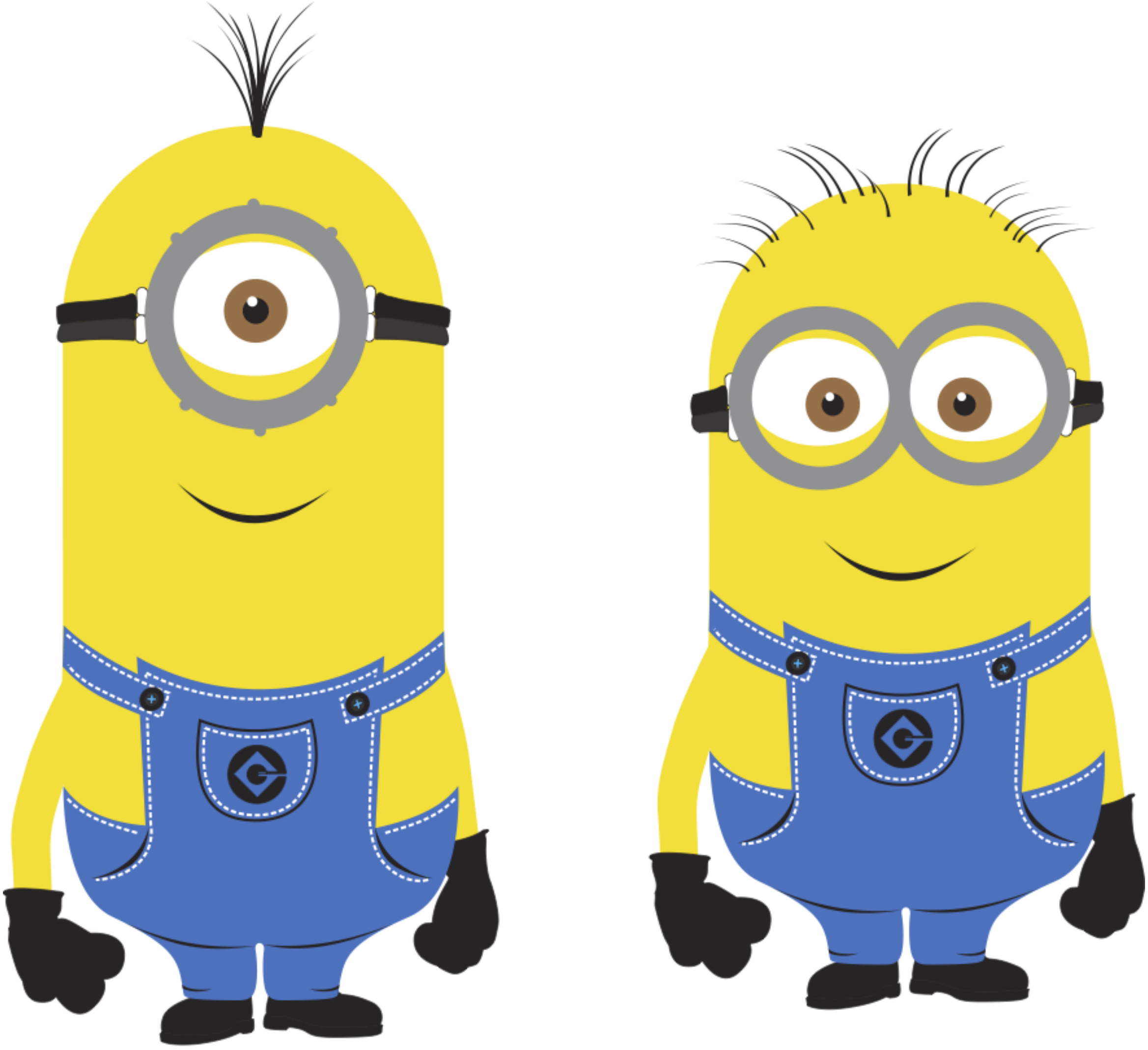


Fig. 2.1 This is just a long figure caption for the minion in Despicable Me from Pixar

dui malesuada malesuada id ac metus. Phasellus posuere egestas mauris, sed porta arcu vulputate ut. Donec arcu erat, ultrices et nisl ut, ultricies facilisis urna. Quisque iaculis, lorem non maximus pretium, dui eros auctor quam, sed sodales libero felis vel orci. Aliquam neque nunc, elementum id accumsan eu, varius eu enim. Aliquam blandit ante et ligula tempor pharetra. Donec molestie porttitor commodo. Integer rutrum turpis ac erat tristique cursus. Sed venenatis urna vel tempus venenatis. Nam eu rhoncus eros, et condimentum elit. Quisque risus turpis, aliquam eget euismod id, gravida in odio. Nunc elementum nibh risus, ut faucibus mauris molestie eu. Vivamus quis nunc nec nisl vulputate fringilla. Duis tempus libero ac justo laoreet tincidunt. Fusce sagittis gravida magna, pharetra venenatis mauris semper at. Nullam eleifend felis a elementum sagittis. In vel turpis eu metus euismod tempus eget sit amet tortor. Donec eu rhoncus libero, quis iaculis lectus. Aliquam erat volutpat. Proin id ullamcorper tortor. Fusce vestibulum a enim non volutpat. Nam ut interdum nulla. Proin lacinia felis malesuada arcu aliquet fringilla. Aliquam condimentum, tellus eget maximus porttitor, quam sem luctus massa, eu fermentum arcu diam ac massa. Praesent ut quam id leo molestie rhoncus. Praesent nec odio eget turpis bibendum eleifend non sit amet mi. Curabitur placerat finibus velit, eu ultricies risus imperdiet ut. Suspendisse lorem orci, luctus porta eros a, commodo maximus nisi.

Nunc et dolor diam. Phasellus eu justo vitae diam vehicula tristique. Vestibulum vulputate cursus turpis nec commodo. Etiam elementum sit amet erat et pellentesque. In eu augue sed tortor mollis tincidunt. Mauris eros dui, sagittis vestibulum vestibulum vitae, molestie a velit. Donec non felis ut velit aliquam convallis sit amet sit amet velit. Aliquam vulputate, elit in lacinia lacinia, odio lacus consectetur quam, sit amet facilisis mi justo id magna. Curabitur aliquet pulvinar eros. Cras metus enim, tristique ut magna a, interdum egestas nibh. Aenean lorem odio, varius a sollicitudin non, cursus a odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae;

1. The first topic is dull
2. The second topic is duller
   (a) The first subtopic is silly
   (b) The second subtopic is stupid
3. The third topic is the dullest

Morbi bibendum est aliquam, hendrerit dolor ac, pretium sem. Nunc molestie, dui in euismod finibus, nunc enim viverra enim, eu mattis mi metus id libero. Cras sed accumsan justo, ut volutpat ipsum. Nam faucibus auctor molestie. Morbi sit amet eros a justo pretium aliquet.

Maecenas tempor risus sit amet tincidunt tincidunt. Curabitur dapibus gravida gravida. Vivamus porta ullamcorper nisi eu molestie. Ut pretium nisl eu facilisis tempor. Nulla rutrum tincidunt justo, id placerat lacus laoreet et. Sed cursus lobortis vehicula. Donec sed tortor et est cursus pellentesque sit amet sed velit. Proin efficitur posuere felis, porta auctor nunc. Etiam non porta risus. Pellentesque lacinia eros at ante iaculis, sed aliquet ipsum volutpat. Suspendisse potenti.

Ut ultrices lectus sed sagittis varius. Nulla facilisi. Nullam tortor sem, placerat nec condimentum eu, tristique eget ex. Nullam pretium tellus ut nibh accumsan elementum. Aliquam posuere gravida tellus, id imperdiet nulla rutrum imperdiet. Nulla pretium ullamcorper quam, non iaculis orci consectetur eget. Curabitur non laoreet nisl. Maecenas lacinia, lorem vel tincidunt cursus, odio lorem aliquet est, gravida auctor arcu urna id enim. Morbi accumsan bibendum ipsum, ut maximus dui placerat vitae. Nullam pretium ac tortor nec venenatis. Nunc non aliquet neque.

Itemize

- The first topic is dull
- The second topic is duller
  - The first subtopic is silly
  - The second subtopic is stupid
- The third topic is the dullest

Description

The first topic is dull

The second topic is duller

> **The first subtopic** is silly
>
> **The second subtopic** is stupid

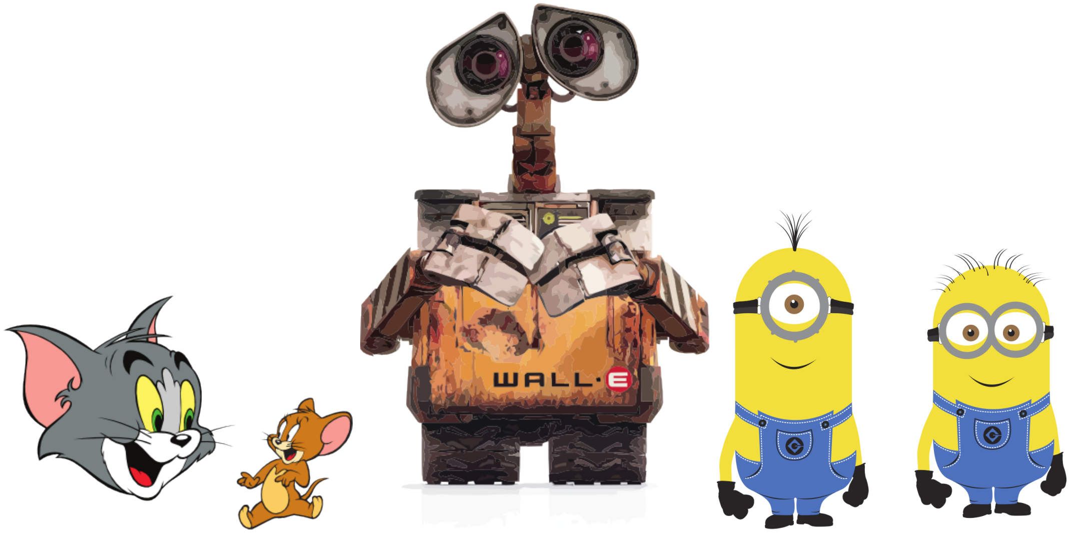
The third topic is the dullest

2.8 Hidden section

Lorem ipsum dolor sit amet, *consectetur adipiscing elit.* In magna nisi, aliquam id blandit id, congue ac est. Fusce porta consequat leo. Proin feugiat at felis vel consectetur. Ut tempus ipsum sit amet congue posuere. Nulla varius rutrum quam. Donec sed purus luctus, faucibus velit id, ultrices sapien. Cras diam purus, tincidunt eget tristique ut, egestas quis nulla. Curabitur vel iaculis lectus. Nunc nulla urna, ultrices et eleifend in, accumsan ut erat. In ut ante leo. Aenean a lacinia nisl, sit amet ullamcorper dolor. Maecenas blandit, tortor ut scelerisque congue, velit diam volutpat metus, sed vestibulum eros justo ut nulla. Etiam nec ipsum non enim luctus porta in in massa. Cras arcu urna, malesuada ut tellus ut, pellentesque mollis risus.Morbi vel tortor imperdiet arcu auctor mattis sit amet eu nisi. Nulla gravida urna vel nisl egestas varius. Aliquam posuere ante quis malesuada dignissim. Mauris ultrices tristique eros, a dignissim nisl iaculis nec. Praesent dapibus tincidunt mauris nec tempor. Curabitur et consequat nisi. Quisque viverra egestas risus, ut sodales enim blandit at. Mauris quis odio nulla. Cras euismod turpis magna, in facilisis diam congue non. Mauris faucibus nisl a orci dictum, et tempus mi cursus.

Etiam elementum tristique lacus, sit amet eleifend nibh eleifend sed [1]. Maecenas dapibu augue ut urna malesuada, non tempor nibh mollis. Donec sed sem sollicitudin, convallis velit aliquam, tincidunt diam. In eu venenatis lorem. Aliquam non augue porttitor tellus faucibus porta et nec ante. Proin sodales, libero vitae commodo sodales, dolor nisi cursus magna, non tincidunt ipsum nibh eget purus. Nam rutrum tincidunt arcu, tincidunt vulputate mi sagittis id. Proin et nisi nec orci tincidunt auctor et porta elit. Praesent eu dolor ac magna cursus euismod. Integer non dictum nunc.

[1] My footnote goes blah blah blah! . . .



(a) Tom and Jerry (b) Wall-E (c) Minions

Fig. 2.2 Best Animations

Subplots

I can cite Wall-E (see Fig. 2.2b) and Minions in despicable me (Fig. 2.2c) or I can cite the whole figure as Fig. 2.2

Chapter 3

My third chapter

3.1 First section of the third chapter

And now I begin my third chapter here . . .

And now to cite some more people **?** **?**]

3.1.1 First subsection in the first section

. . . and some more

3.1.2 Second subsection in the first section

. . . and some more . . .

3.1.2.1 First subsub section in the second subsection

. . . and some more in the first subsub section otherwise it all looks the same doesn't it? well we can add some text to it . . .

3.1.3 Third subsection in the first section

. . . and some more . . .

3.1.3.1 First subsub section in the third subsection

. . . and some more in the first subsub section otherwise it all looks the same doesn't it? well we can add some text to it and some more and some more and some more and some more and some more and some more and some more . . .

3.1.3.2 Second subsub section in the third subsection

. . . and some more in the first subsub section otherwise it all looks the same doesn't it? well we can add some text to it . . .

3.2 Second section of the third chapter

and here I write more . . .

3.3 The layout of formal tables

This section has been modified from "Publication quality tables in LaTeX*" by Simon Fear.

The layout of a table has been established over centuries of experience and should only be altered in extraordinary circumstances.

When formatting a table, remember two simple guidelines at all times:

1. Never, ever use vertical rules (lines).

2. Never use double rules.

These guidelines may seem extreme but I have never found a good argument in favour of breaking them. For example, if you feel that the information in the left half of a table is so different from that on the right that it needs to be separated by a vertical line, then you should use two tables instead. Not everyone follows the second guideline:

There are three further guidelines worth mentioning here as they are generally not known outside the circle of professional typesetters and subeditors:

3. Put the units in the column heading (not in the body of the table).

4. Always precede a decimal point by a digit; thus 0.1 *not* just .1.

5. Do not use 'ditto' signs or any other such convention to repeat a previous value. In many circumstances a blank will serve just as well. If it won't, then repeat the value.

A frequently seen mistake is to use '\begin{center}' . . . '\end{center}' inside a figure or table environment. This center environment can cause additional vertical space. If you want to avoid that just use '\centering'

Table 3.1 A badly formatted table

	Species I		Species II	
Dental measurement	mean	SD	mean	SD
I1MD	6.23	0.91	5.2	0.7
I1LL	7.48	0.56	8.7	0.71
I2MD	3.99	0.63	4.22	0.54
I2LL	6.81	0.02	6.66	0.01
CMD	13.47	0.09	10.55	0.05
CBL	11.88	0.05	13.11	0.04

Table 3.2 A nice looking table

Dental measurement	Species I		Species II	
	mean	SD	mean	SD
I1MD	6.23	0.91	5.2	0.7
I1LL	7.48	0.56	8.7	0.71
I2MD	3.99	0.63	4.22	0.54
I2LL	6.81	0.02	6.66	0.01
CMD	13.47	0.09	10.55	0.05
CBL	11.88	0.05	13.11	0.04

Table 3.3 Even better looking table using booktabs

Dental measurement	Species I		Species II	
	mean	SD	mean	SD
I1MD	6.23	0.91	5.2	0.7
I1LL	7.48	0.56	8.7	0.71
I2MD	3.99	0.63	4.22	0.54
I2LL	6.81	0.02	6.66	0.01
CMD	13.47	0.09	10.55	0.05
CBL	11.88	0.05	13.11	0.04

Appendix A

How to install LaTeX

Windows OS

TeXLive package - full version

1. Download the TeXLive ISO (2.2GB) from https://www.tug.org/texlive/

2. Download WinCDEmu (if you don't have a virtual drive) from http://wincdemu.sysprogs.org/download/

3. To install Windows CD Emulator follow the instructions at http://wincdemu.sysprogs.org/tutorials/install/

4. Right click the iso and mount it using the WinCDEmu as shown in http://wincdemu.sysprogs.org/tutorials/mount/

5. Open your virtual drive and run setup.pl

or

Basic MikTeX - TeX distribution

1. Download Basic-MiKTeX(32bit or 64bit) from http://miktex.org/download

2. Run the installer

3. To add a new package go to Start » All Programs » MikTex » Maintenance (Admin) and choose Package Manager

4. Select or search for packages to install

TexStudio - TeX editor

1. Download TexStudio from http://texstudio.sourceforge.net/#downloads
2. Run the installer

Mac OS X

MacTeX - TeX distribution

1. Download the file from https://www.tug.org/mactex/
2. Extract and double click to run the installer. It does the entire configuration, sit back and relax.

TexStudio - TeX editor

1. Download TexStudio from http://texstudio.sourceforge.net/#downloads
2. Extract and Start

Unix/Linux

TeXLive - TeX distribution

Getting the distribution:

1. TexLive can be downloaded from http://www.tug.org/texlive/acquire-netinstall.html.
2. TexLive is provided by most operating system you can use (rpm,apt-get or yum) to get TexLive distributions

Installation

1. Mount the ISO file in the mnt directory

   ```
   mount -t iso9660 -o ro,loop,noauto /your/texlive####.iso /mnt
   ```

2. Install wget on your OS (use rpm, apt-get or yum install)

3. Run the installer script install-tl.

   ```
   cd /your/download/directory
   ./install-tl
   ```

4. Enter command ‘i’ for installation

5. Post-Installation configuration:
   http://www.tug.org/texlive/doc/texlive-en/texlive-en.html#x1-320003.4.1

6. Set the path for the directory of TexLive binaries in your .bashrc file

For 32bit OS

For Bourne-compatible shells such as bash, and using Intel x86 GNU/Linux and a default directory setup as an example, the file to edit might be

```
edit $~/.bashrc file and add following lines
PATH=/usr/local/texlive/2011/bin/i386-linux:$PATH;
export PATH
MANPATH=/usr/local/texlive/2011/texmf/doc/man:$MANPATH;
export MANPATH
INFOPATH=/usr/local/texlive/2011/texmf/doc/info:$INFOPATH;
export INFOPATH
```

For 64bit OS

```
edit $~/.bashrc file and add following lines
PATH=/usr/local/texlive/2011/bin/x86_64-linux:$PATH;
export PATH
MANPATH=/usr/local/texlive/2011/texmf/doc/man:$MANPATH;
export MANPATH
INFOPATH=/usr/local/texlive/2011/texmf/doc/info:$INFOPATH;
export INFOPATH
```

Fedora/RedHat/CentOS:

```
sudo yum install texlive
sudo yum install psutils
```

SUSE:

```
sudo zypper install texlive
```

Debian/Ubuntu:

```
sudo apt-get install texlive texlive-latex-extra
sudo apt-get install psutils
```

Appendix B

Installing the CUED class file

LaTeX.cls files can be accessed system-wide when they are placed in the <texmf>/tex/latex directory, where <texmf> is the root directory of the user's TeXinstallation. On systems that have a local texmf tree (<texmflocal>), which may be named "texmf-local" or "localtexmf", it may be advisable to install packages in <texmflocal>, rather than <texmf> as the contents of the former, unlike that of the latter, are preserved after the LaTeXsystem is reinstalled and/or upgraded.

It is recommended that the user create a subdirectory <texmf>/tex/latex/CUED for all CUED related LaTeXclass and package files. On some LaTeXsystems, the directory look-up tables will need to be refreshed after making additions or deletions to the system files. For TeXLive systems this is accomplished via executing "texhash" as root. MIKTeXusers can run "initexmf -u" to accomplish the same thing.

Users not willing or able to install the files system-wide can install them in their personal directories, but will then have to provide the path (full or relative) in addition to the filename when referring to them in LaTeX.