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 s*teganography* 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 I) 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].
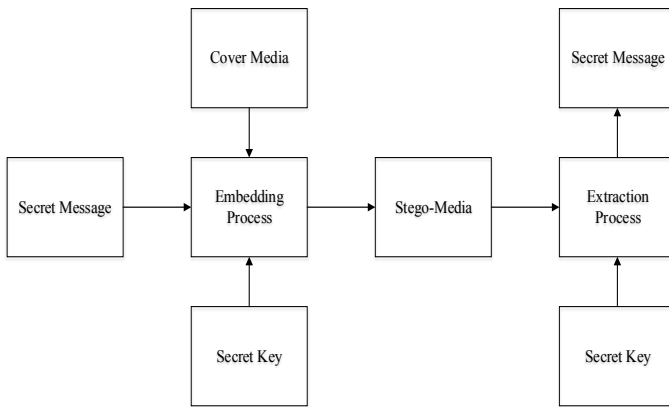

Figure I. Conventional image steganography flow

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 I, 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.
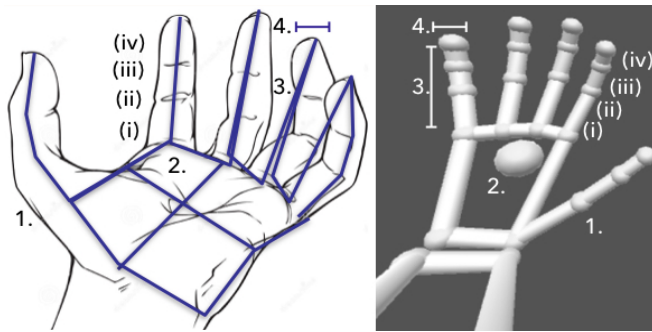

Figure II. Example of LMC generated hand model

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
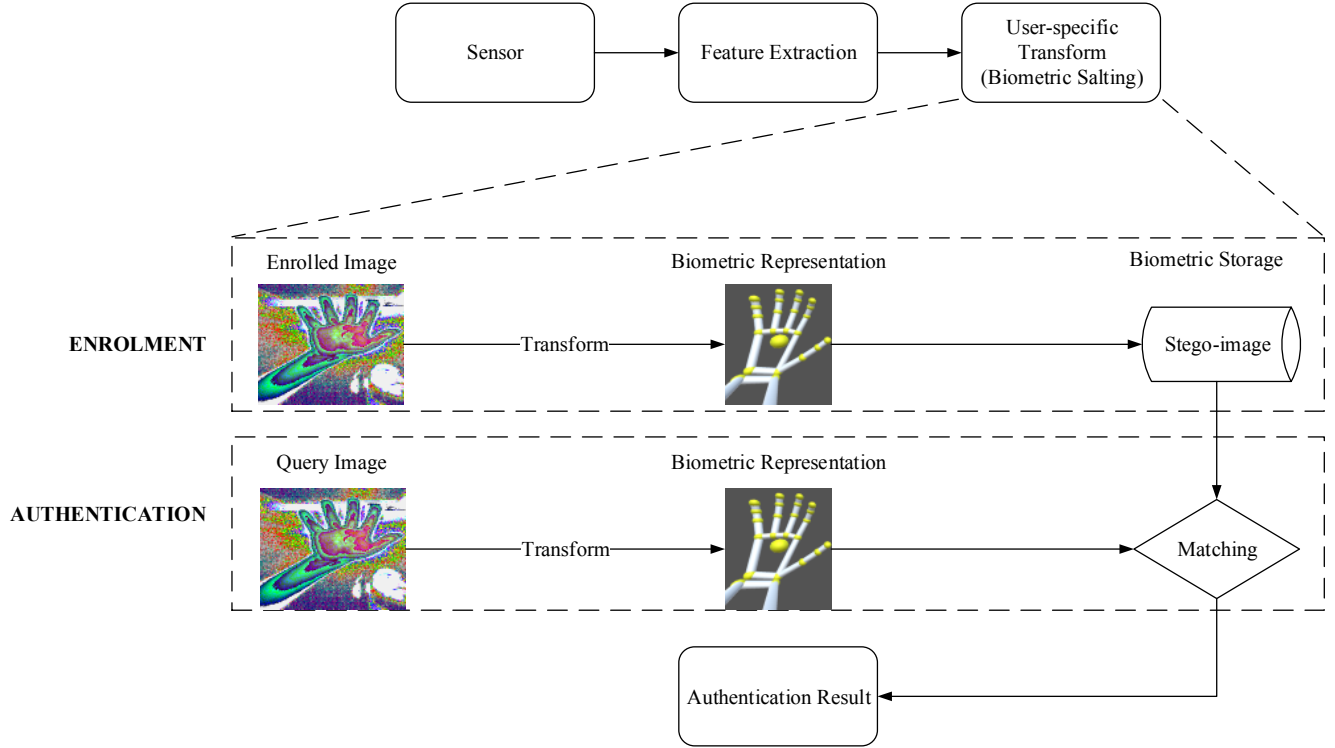
Figure III. System structure flow diagram

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.
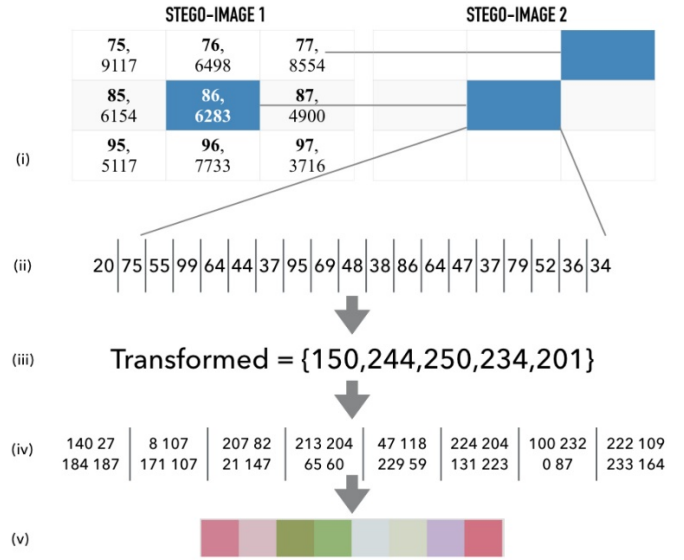

Figure IV. Example of biometric vector reading and transformation

(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.
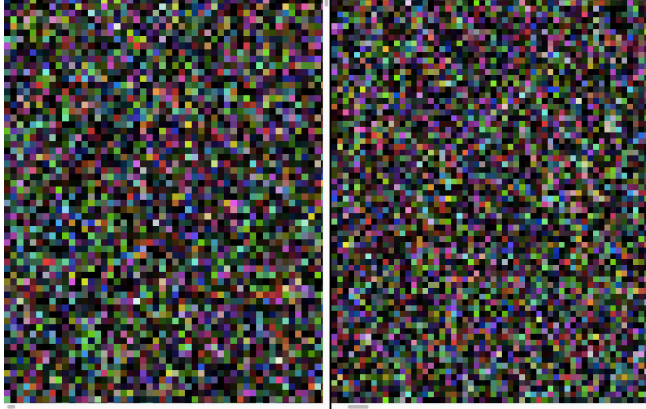

Figure V. Randomly generated image versus stego-image

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)

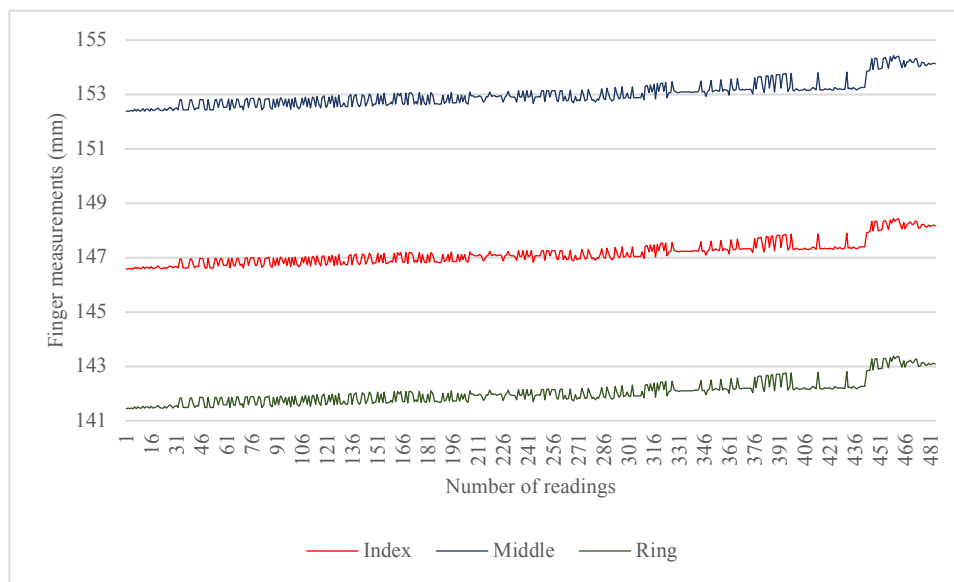| Thumb	Index	Middle	Ring	Pinkie
0.197203783	0.424346553	0.464246258	0.438259197	0.35738522

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 conistently 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.
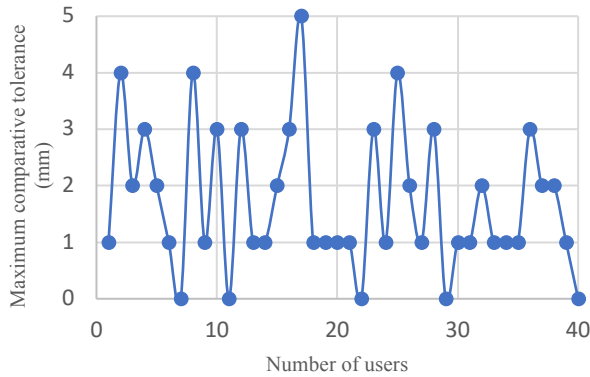

Figure VII. Maximum comparative tolerance levels

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,
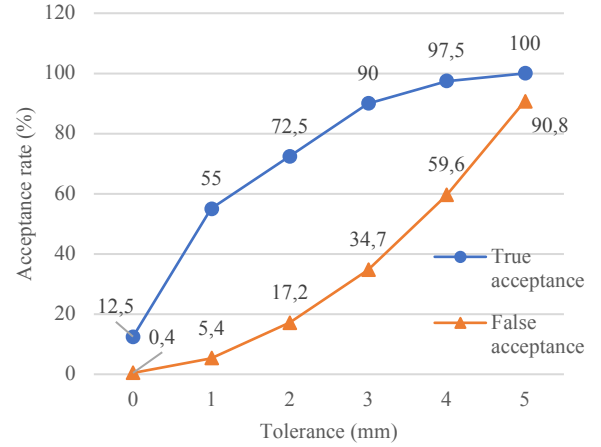

Figure VIII. Acceptance rates based on dynamic tolerance range

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 Internation 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. Iciccs, 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. Levickỳ, "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].