International Journal of Advanced Technology and Engineering Exploration, Vol 5(45)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2018.544003

Review Article

Assessment of vulnerabilities of the biometric template protection mechanism

Taban Habibu[1*] and Anael E. Sam[2]
Research Scholar, Department of Applied Mathematics and Computational Sciences, Nelson Mandela African Institution of Science and Technology, Arusha, Tanzania[1]
Senior Lecturer, Department of Communication Science and Engineering, Nelson Mandela African Institution of Science and Technology, Arusha, Tanzania[2]

Abstract
In the ever-changing world of global data transmission, the security of data and individual privacy are the growing fears in today's human life worldwide. The major concerns are the protection of the biometric templates in the biometric identification and authentication process. Storage of the biometric template in the database raises the chance of compromising it, hence lead to serious threats and abuse of the person's identity. When an individual's registered biometric data is disclosed, their security and privacy can be compromised. Therefore, public acceptance of biometrics will depend on the system designer's ability to demonstrate that the systems are robust, with low error rates, and tamper proof. If someone's biometric template inside the database is compromised, that consequently might imply identification robbery of that individual. In the recent past, a considerable number of methods for biometric template protection have been published. This article explains, a thorough valuation on numerous attacks and threats associated with the biometric system alongside the biometric template protection, elucidating the measures anticipated to address the threats, to the performance gap and establish the status quo of the current biometric template protection for public acceptance.

Keywords
Biometric mechanism, Biometric attacks, Privacy threats, Security threats, Biometric template protection.

1.Introduction
Every individual is exceptional in terms of biometric feature traits that make them distinct from all other individuals. Biometric system offers a reliable solution to the problem of user authentication in identity verification. It is a pattern of authenticating the character of an individual using their body or behavior traits such as facial, iris, fingerprint, voice, palm print among others[1].The growing demand for improved security and the increasing volume of electronic transactions across wired and wireless networks has created a strong need for more reliable identity supervision. The existing aspect of the traditional biometric authentication approaches such as a token based and knowledge based techniques (secret keys, PIN numbers, the smart cards) are not consistent, easy to be forgotten, shared, stolen and guessed in the authentication systems, perhaps causing an identity robbery or misuse.

The danger from identity thieves is more serious because, once a biometric sample is stolen or compromised, an individual identity is compromised forever.

For instance, the identity thieves may result into the forgery of personalities. For example, in a financial institution, identity robbery might result into account fraud, payment card tricking, forgery of checks and use of stolen credit card numbers. In the healthcare domain, it might result in access to medical records, unlawful consent to restricted areas, unauthorized use of medical treatment, or health-insurance fraud. In the government organization, it might result into forged or abused identity permits/passports. This can have serious penalties as governmental identities are regularly used to validate personalities for other applications[2].

In Uganda more than 15,277 million voter's fingerprints, were extracted from the National Identification Registration Authority (NIRA) database for voting in the 2016 presidential election in order to verify the person's identity[3]. Though some observers appreciated them as good practice for fraud prevention and identity verification mechanism, the concern about the security of the biometric system templates and the potential breaches of the privacy of the user's biometric data raised many questions. Like any other user authentication mechanism, a biometric system template can be

*Author for correspondence

circumvented by a skillful imposter given the right circumstances and plenty of time and resource because biometric data can't be cancelled or substituted if it's captured by an imposter. This paper consequently presents a thorough valuation on numerous attacks and threats of the biometric system associated with the biometric template protection on the security and abuse of the individual identity. Therefore, mitigating such concerns is essential to ensure the integrity, reliability for identity claim verification, public confidence and acceptance of the biometric systems [4−6].

1.1An overview of biometric operational mechanism

Biometric system operates in two modes, verification and identification mode [6−8]. In the verification mode, the system records a sample of a user's biometric trait using a sensor machine, for instance, a digitalized camera for the face or fingerprint sensor during enrolment. It extracts the relevant features, like thumbprints minutiae, from the biometric traits via algorithm software known as feature extractor. These extracted characters are stored as a template in a database with other attribute such as names or an identifying number, then an ATM card or passport is issued to the individual. To confirm the authentication of the person, additional biometric traits are presented to the sensor machine, and then matched against the stored template of the claimed identity via a matcher. It conducts a one-on-one similarity to find if the claim is factual. Then brings the match score signifying the degree of resemblance amongst the template and the query. The identity is confirmed only if the match score is overhead a predefined threshold. During the authentication, the system recognizes the person by searching the whole template database for a match. It conducts one-on-many similarities to acquire an individual's uniqueness (fails if the theme is not registered). The verification is very fundamental because it confirms whether the individual is who he/she claims or denies being [6].

1.2Various attacks on biometric systems

In 2015, Gowdhaman et at. [9], indicated that, the biometric system can be attacked by the outsider or unauthorized person at various points, there are eight stages that are very critical to be attached by an imposter [6], [9–11].

(i)*The attack at the scanner (sensor module):* According to Malhotra and Kant [2], the attacker destroys the recognition sensor scanner and cause denial of services. It creates a forged fingerprint characters like an artificial finger to bypass fingerprint recognition systems or insert a fingerprint image between the sensors to escape fingerprint recognition process [12]. (ii) *The attack at the passage amongst the scanner and the sample feature extractor:* When the sensor machine obtains raw biometric traits, it forwards the sample to the extractor module for pre-processing via communiqué route. The hacker seized the biometric traits, steal the sample and store it somewhere else [2]. (iii) *The attack on the extractor module:* When the sample of biometric traits is acquired from sensor machine, they are sent to feature extractor module. The intruder then forces the feature extractor module to generate the sample values chosen by the impostor instead of producing the feature values generated from the original data acquired from the sensor device, the invader then substitutes the feature extractor unit with a Trojan horse. The Trojan horse can harvest user's fingerprints extracted samples and send them to the attacker. (iv) *The attack at the passage amongst the feature extractor and matcher:* Here, an impostor intercepts the message channel amongst the feature extractor and matcher units and steals the feature values of the genuine person and later resends them to the matcher module [12]. (v) *The attack on the matcher:* The intruder substitutes the matcher with a Trojan horse. The invader sends instructions to the Trojan horse to yield high matching scores and direct a "yes" to the application to bypass the biometric authentication mechanism. (vi) *The attack on the system database:* This occurs when the impostor compromises with the database security by adding fresh fingerprint templates, modifies the current templates stored to gain unlawful access, and creates physical spoofing from the template. The stolen template can be rerun to matcher to obtain unlawful admittance [13, 14]. Compromised database is done by manipulating vulnerability using the software, database or cracking an account on the database. (vii) *Attack between the system database and matcher:* Here, the invader intercepts the message pathway amongst the database and matched to either steal and replay data or alter the data. It occurs when an attacker changes the subject of the transferred template. (viii) *The attack at the passage amongst the matcher and the application:* In this module, an impostor supersedes the outcome announced by the matcher unit. The attacker either steals replays or alters the data. It interferes the match score to change the original decision (accept or reject) of the matcher module [15].

In 2014, Gobi and Kannan [1] indicated that, most of the attacks are established in the template database system. The template can be tempered with by adding the fresh user template to the database, amending current templates in the record and removing or deleting existing templates [6]. According to Brindha and Natarajan [16], the most destructive occurrence of a biometric system arises at the biometric templates side. She defined how attacks on the templates can cause dangerous vulnerabilities in which the template can be substituted by an impostor's template to achieve unlawful access to a system. She additionally warned alongside biometric templates being kept in plain text form and asserted that fool proof procedures are very important in securing the biometric template protection and the individual's privacy. In a survey done by Mwema et al. [17], observed that spooling of the biometric templates database was the most persistent outbreak experienced in biometric systems. When a biometric system is compromised, it leads to the following effects :(i) *Denial of Service:* It is an attempt to make system resources unavailable to its intended users. (ii) *Circumvention:* The act of prevailing over another by arts, address, or fraud. The authorized user does not get access to resources. (iii) *Repudiation:* Act, deliberately or denial or refusal of the contract previously approved. (iv) *Covert acquisition:* Here the knowledge of authorized person has been stolen and used by the intruder. (v) *Collusion:* the act to cheat, a secret agreement between two parties, this helps the intruder to modify the system's parameter to permit incursion (vi) *Coercion:* The act of compelling by force of authority. An authorized user is compelled by intruder to give him access to the system[8, 10].

1.3Biometric system threats

In 2010, Xi and Hu [6] elaborated that, the privacy threats on biometric systems involves the cross-match data between dissimilar services or applications through biometric reference comparison. The persistence and uniqueness of biometric characteristics allow a malicious person to link users between different databases. For instance, an attacker could link different financial service records across different banks' databases to one specific customer to illegally obtain the customer's financial condition or investment plan. They further explained that, second threat to privacy is the possibility to extract sensitive information from the stored biometric data, like the subject's ethnic background or (the probability for) certain diseases. Such data can be abused by healthcare insurance providers (for instance biometric references that are planned for patient authentication in a hospital could be used to distinguish between insurance premiums). If the application scope of the biometric system is not well defined and restricted, its use might expand into other applications or services. For instance, an application primarily planned to prevent misuse of municipal services might slowly be extended to privileges to buy property, cross-border, or the right to elect. As a result, data samples that would be used for the biometrics initial application would be forced to be used in another biometrics application.

Applying DNA can expose genetic information. Such private information is not relevant for authentication purpose, but is saved in biometric systems. Central storage of biometric data is critical due to privacy issue. Moreover, databases are the common attack target. The stored data can be intercepted, copied or tampered. Sensitive information about a person's personality and health can be revealed [18]. It is worth pointing that automatic biometrics technologies are also prone to enrolment threats interrelated to individuality spoofing since fake ID cards might be used at the enrolment stage and the identifiers could be stolen. It's easy to substitute a stolen credit card, but good luck changing the patterns on your iris. It is argued that a name, photograph or birthday can give the criminal a beginning point to collect the data of any individual identity and start to track the passage and allow him/her to predict the travels and then use the information to create a new fake identity for him/herself. Therefore, soft biometrics have been determined as the perfect way to pinpoint, track and control people, by reason, to reveal gender, ethnicity, religion or other exceptional features like gait or the shape of their ears. The applied areas vary from town squares, or department stores and banks to airports where passengers allowed walking from checkpoints into the gate, while their movements are watched and identities confirmed automatically by cameras. Nevertheless, most technologies don't store biometric data as an image or record, instead, it keeps a binary scientific representation of the original traits which can be hashed, transformed by an algorithm, to create the authorization code.

In 2008, Jain et al. [8] explained that, the greatest security threat comes from the input interface that is used in presenting a fake biometric characteristic. This results in the forging and staging of the fake physical biometric characteristic by the imposter of the sensor machine. It is identified that some features

are harder to forge (such as the iris, a retinal scan, or a face thermogram) while others are simple to forge (voice, face, handwritten signature). Therefore, aliveness detection methods must be put in place to confirm that the required biometric sample come from the correct subject at the time of verification. The sensor spoofing attack can be deployed as a coercive or an impersonation attack depending on the number of attempts applied to the capture subsystem. For instance, the invader may physically force a genuine subject to present his/her biometric traits in a verification setting. System designers have to consider how to counter such attacks, for instance by installing security cameras at ATMs.

In addition, the biometric references can be retrieved illegally or could be substituted or altered. The unlawful access or, alteration of biometric references may not only lead to security threats, but may also extend to threats in the privacy domain, such as cross-matching of the database. Therefore, guard of the biometric template database is key for security and privacy reasons. Decision subsystem attacks are potentially vulnerable to hill climbing and threshold manipulation attacks. The attacker might present an initial biometric characteristic and observe the corresponding comparison score. Depending on the value of the score, the presented biometric characteristic is modified and the resulting scores are supervised. This allows attackers to iteratively change the biometric input until a successful verification is obtained. In a threshold manipulation attack, the invader can modify the comparison threshold to enforce a "correct" verification. The transmitted and stored data, for instance, the biometric samples, features extraction, even comparison scores, can be read, eavesdropped, manipulated or substituted. The imposter can use a Trojan horse to change important system parameters such as decision threshold or replay the data of an authorized subject. The invader can also generate a fake biometric sample to bypass facial or fingerprint enrolment systems using an artificial finger or inject an image for sensing element thus create the security threat such as, Identity fraud where the biometric features cannot be copied, stolen or handed over like a token or a password and in case the biometric data are compromised, they cannot easily be revoked or renewed. We own an inadequate quantity of biometric modalities, e.g. Ten fingers, thumbs, one fascia, two eyes, nevertheless, a modification is likely only with very complex approaches such as transplantation, cosmetic surgery. Furthermore, Jain et al. [19] explained that, the existing biometric technologies suffer from the false match and false non-match or dishonesty evils which are caused by the imposter at the sensor machine interface by exploiting susceptibilities in the hardware or firmware, and cold booting the machine itself. This has resulted into a compromise amongst a usable system and security because the biometric technology, performance depends highly on how they are deployed and where they are tested [8, 20–23]

2.Related literature survey

The major challenge in designing a biometric template protection scheme is the need to handle intruder variability in the acquired biometric identifiers [2, 4, 8]. An ideal template protection system should comprise of the following properties [24] (i) *Diversity:* The secure template must not allow a cross matching of the databases; this will help to ensure user's privacy. (ii) *Revocability:* It must be straight to revoke compromised template and re-release a fresh one based on the same biometric data. (iii) *Security:* It should be arithmetically complex to acquire a genuine biometric template from the secure template. (iv) *Performance:* The biometric system should not destroy the recognition performance of the false match and false non-matching of the biometric system [25]. In 2013, Tigga and Wanjari [26] discussed that, the protection of the biometric template is classified as hardware-based and software-based approach. The hardware-based approach includes the use of smart cards or standalone biometric system. They are known as match-on-card or system-on-card device. Their main benefit is that; the biometric information does not leak from the card. However, their solution was not suitable because of the subsequent motives (i) they are not suitable for large-scale systems (ii) They are costly (iii) Users must bring the card with them every other time (iv) It is probable that the template can be assembled from a stolen card. Thus, prompted researchers to focus more onto different kinds of algorithm that can be used to generate distinctly unlikable and non-invertible references from biometric data. In 2008, Jain et al. [8] gave an indication of the present techniques and categorized them into feature transformation method and biometric cryptosystem [6, 27–29].

2.1The feature transformation

In these techniques, the template is transformed using the user's password during the enrollment and the same password in the transformed query during the authentication before being matched with the transformed template [2].The transformation function

is acquired in the biometric template and then recorded in the database. The elements of the transformation function are obtained from a random secrecy key or password. The same transformation function is placed to the feature query and the query is matched besides the transformed template [30]. Depending on the features of the conversion function, its patterns are characterized as salting and non-invertible transforms. In salting, its security is based on the function which is defined by user particular secret key. If an adversary wants to gain authority to the key and the transformed template, the original biometric template will be recovered. Nevertheless, non-invertible transformation patterns regularly apply a one-way function on the template and it is computationally hard to reverse a transformed template with known secret key. In 2007, Ratha et al. [31] proposed and analyzed three noninvertible transformations for producing cancellable templates for the fingerprint. Three transformation tasks existed Cartesian, polar, and functional. The tasks were used to convert fingerprint minutiae data, so that a minutiae matcher can be put to the transformed minutiae [32, 33].

2.2Biometric cryptosystems

According to Supriya and Manjunatha [34], suggested that the biometric template is encrypted using an encryption key, derived from a password. The stored information is deciphered using the matching deciphered key and is corresponded with the captured query for the authentication. The data were stored in the helper data or helper data-based approach. This helper data does not disclose any important message about the exceptional biometric template; it is desirable during matching to extract a cryptographic key from the query biometric features. Since the cipher key can be discarded after creating the secure template, the attacker cannot be able to replace the existing encrypted templates even if he/she steals the decryption key. These systems performed typically better than feature transformation methods [35]. Beside the operation, the biometric Cryptosystem patterns are further characterized into two parts; key-binding and key-generating method [34]. The key-binding is where the secured template is created with a key. The same key is used to extract the biometric trait from encrypted data. A number of additional template protection methods like fuzzy vault [36], shielding functions [10], and distributed source coding are considered as key-binding biometric cryptosystems [37]. In 2016, Yildiz et al. [38] proposed the fuzzy vault pattern which became the common methods for biometric template protection using fingerprint, face, iris, and signature modalities for the implementation process. The Key-generating method involves generating a key from biometric trait. It is an attractive method, but challenging problem because, it suffers from low discriminability. Discriminability refers to a number of dissimilar keys generated by the same biometric traits.

3.Biometric template protection techniques

In 2013, Jeny and Jangid [39] suggested, various techniques for biometric template protection, based on the most current biometrics traits (iris, fingerprint, face) pattern. They aimed at decreasing the faults and deliver higher security in the template protection [40]. Ratha et al. [41] suggested a framework of cancellable biometrics, where biometric data undergo a predefined non-invertible transformation during enrollment and testing, with the matching done in the converted universe. Though their work was crucial, finding one-way transformations that preserve distances were an elusive. Similarly, managing the transform functions was an issue and if cancellable biometrics transformational parameters were recognized by hackers, it will not be secure. If converted biometric data is tempered with then conversion variables must be reformed to prevent an imposter from tracing and cross-matching user's biometric templates [42].

Boyen et al. [43] and Bringer et al. [44] introduced the concepts of secure sketch and fuzzy extractor in the context of key generation from biometrics. Furthermore, Li and Chang [45] introduced a two-level quantization-based approach for obtaining secure sketches. Sutcu et al. [46] discussed the practical issues in secure sketch construction and proposed a secure sketch based on quantization for face biometric. The main challenge of producing fuzzy extractors from constant deliveries was recommended by Buhan et al. [47]. Secure sketch construction for other modalities such as fingerprints, 3D face, and multimodal systems (face and fingerprint) has also been proposed. Various protocols for secure authentication in remote applications by Boyen et al. [43] and Buhan et al. [48] were proposed based on the fuzzy extractor scheme.

In 2013, Malhotra and Kant [2] proposed watermarking for security of biometric template. They used pixel values to hide watermark information. In case an imposter tries to replace or

forge and change the secure biometric template, the system could signal to the database manager indicating that something is going wrong with the biometric template. This is because; the forged biometric template could disappear or present wrong pixel positions [49]. Although, the watermark information was inserted four times in the biometric template to prevent attacks from changing the template, there was still a very little change in the original template as well as few changes in the pixel. Hence, lead to insecure of the biometric template protection.

Furthermore, Nandakumar and Jain [50] presented the technique of the multi biometric template protection basing on the fuzzy vault pattern. They anticipated a method for securing multiple templates of a user as a single entity resultant from one multi biometric template using the fuzzy vault framework. Their study indicated that a multi biometric vault provides better recognition performance and highest security compared to a single biometric vault. For instance, the multi biometric vault based on fingerprint and iris achieved a GAR of 98.2% at FAR of 0.01%. The corresponding GAR values of the person's iris and fingerprint vaults were 88% and 78.8% respectively. Furthermore, they presented that the safety of the system was at 41 bits when the iris and fingerprint vaults were stored separately. On the other hand, the multi biometric vault established on fingerprint and iris provided 49 bits of security [40, 51].

In addition, Moi et al. [52] further proposed an approach for identity document using iris biometric cryptography. They proposed a technique to generate the modalities of secured cryptographic key from iris template. The iris images were processed to create an iris template for the cipher and decipher works. The international standard cryptographic algorithm name advance encryption standard (AES) was accepted in their work to generate a high security cryptographic strength of the iris data. Their proposed approach comprised of two processes, encryption and decryption process. Their outcomes showed that, the suggested method achieved better in providing authentication for the user than the traditional techniques.

Furthermore, Gaddam and Lal [53] proposed a novel practice to secure storage of fingerprint template by generating secured feature matrix and keys for cryptographic techniques. They proposed a technique to produce concealable key from fingerprint to overcome the limitations of traditional methods. They introduced the concept of concealable biometrics that was earlier proposed by Ang et al. [54]. Their approach facilitates every incidence of enrollment to utilize a distinct transform hence making depiction cross matching unachievable [55]. Mostly, the transformation utilized for distortion was chosen to be non-invertible. Thus, it was not possible to obtain the unique (accurate) biometric despite knowing the transform method and the resulting transformed biometric data.

In 2016, Mohammed [56] presented two fingerprints taken during the enrollment and authentication for the matching process. The minutiae and reference points from one finger and orientation and reference points from the other finger were combined to form a joint minutiae template. These combined minutiae templates are stored in the template database, RSA algorithm was applied to the extracted template to generate a key. While retrieving the template from the database, the user was required to give his/her two fingerprints, and apply the RSA keys. If the key matches with the data kept, then access to the template could be granted to the person and the person would then decrypt the template using the private key generated from the combined minutiae template. This technique is time consuming for the extra fingerprint minutiae.

Hao et al. [35] expressed use of iris biometrics to generate a repeatable cryptographic key to 140 bits. Sutcu et al. [57] used fuzzy commitment in a multi-biometric system comprised of fingerprint and face. Later, Al-Saggaf and Acharya [24] introduced the fuzzy vault scheme to resolve the concern of unordered feature extraction. The fuzzy vault was used to hide some data in a vault such that it can only be released when sufficiently matching data are provided; as such, it is very suitable for biometric template protection and indeed several applications have been implemented using fingerprints [58, 59], face [19, 20] and iris [59, [60]. To obtain a fingerprint vault, a secret is encoded as the coefficients of a polynomial that is evaluated at the minutiae points (x), that are hidden among the big quantity of chaff points [44]. During verification, the biometric of the user is matched to the vault and only a sufficient match of the minutiae points reveals the secret to unlock the vault. Geethanjali et al. [61] presented the variance amongst fuzzy vault and fuzzy commitment, they pointed that biometric traits secured by fuzzy commitment are symbolized in the practice of binary vectors which are distributed into a sum of sections

and each section is independently secured. The biometric traits in fuzzy vault are symbolized in the form of point set which is protected by hiding them with chaff points. Al-Saggaf and Acharya [24, 62] claimed that the ordinary fuzzy commitment scheme cannot satisfy hiding and binding properties of biometric traits and considered it insecure because the fuzzy vault encounters a lot of security defects in its naive application. They pointed that the cryptographic hash operation h (c) where the secret message c is hidden in the hash value h (c) is not adequately secure because the cryptographic hash functions like the MD5 and SHA families already been acknowledged theoretically and virtually vulnerable to collision and pre-image attacks.

According to Hooda and Gupta [63], fuzzy vault scheme suffers from the difficulty in revoking a compromised vault, which is liable to the cross matching of biometric templates over the databases; it is simple for an invader to stage attacks after statistically analysing points in the vault.; It is also possible for an invader to exchange his biometric characters with that of the targeted biometric template, consequently thrashing vault validation; finally, if the new template of the genuine user is provisionally exposed, then the attacker can acquire the template during this exposure[64].

Nevertheless, Fu et al. [65] proposed multi-biometric templates in order to increase privacy as well as security. They combined minutiae points from two distinct fingers of the same person using superimposition, creating a template with two biometric layers. Camlikaya et al. [66] combined fingerprint minutiae with a spoken password. If the template is compromised, cancelability is provided since the pronounced password can be substituted.

Similarly, Othman and Ross [67] suggested the technique for creating synthetic fingerprint images for a person, by mixing complementary phase components of two corresponding fingerprints [55]. The advantage of this method is that it can be easily integrated into any existing fingerprint verification system, where the created virtual fingerprints would be used for validation instead of real ones. They mixed two different fingers from the West Virginia University database; the authors report a rank-1 accuracy of ~85% and an equal error rate (EER) of ~6% on a dataset with an overall of 500 fingers. In another experiment, they evaluated the changeability property and showed that the mixed fingerprints do not match well (30% rank-1 accuracy) with the original ones. To evaluate cancelability, they ran matching and identification tests involving templates obtained from two impressions of the same fingerprint that were combined with 500 separate fingerprints. They obtained a high 85% identification rate, and 7% EER, showing the promise of the model, despite having similar templates in the gallery. One issue with the work was to obtain realistic looking fingerprints; their constituents must pass a compatibility criterion. Furthermore, Yang et al. [68], proposed a fuzzy extractor-based system. The primary features were the minutia region feature, network quantization, and a pin-sketch-based fuzzy extractor, and key-based polynomial. They generated indigenous characters based on the bordering points of the minutia. This trait is quantized based on a local point grid, generating binary vectors. A pin-sketch-based fuzzy Extractor is used to calm and guard the vectors, succeeding in a hashed vector. The hashed vectors were used to assess the key polynomial. The system was assessed on numerous databases, including FVC2002. They obtained an EER of 11.84% on DB1, and 10.38% on DB2. The EER is gradually condensed when used on high-quality images. The system used all available biometric data to produce a single match score. However, every component is matched differently, which allow multiple permutations to communicate. Nevertheless, the implementation was focused on regenerating a fixed message [64].

In addition, Ashish and Sinha [69] proposed the use of string rearrangement to ease the protection of the template. During the verification, the stored information is deciphered using the secret key and matched against the captured query. Because, the encryption key can be discarded after constructing the comfortable template in order for the adversary unable to update the present encrypted templates even supposing he/she steals the decryption key. The primary obstacle to the encryption based strategy is the insecure key control that the decryption secrets will expose to the machine for the duration of each trial to authenticate. The advantage is that sophisticated matching process may be hired and thereby maintaining the matching accuracy [29, 70].

4.Result evaluation

From the analysis of the evaluation, *Figure 1* shows the false reject rate and false accept rates associated with current biometric traits (fingerprint, face, iris and voice) using different tests to determine the estimated accuracy of the biometric verification system. The analysis indicated that, FPVTE

fingerprint performed better on testing results than FVC fingerprint. Furthermore, FRVT face and ICE iris have both low false acceptability rates compared to falsify reject rate. The false reject rate is the degree of the possibility that the biometric protection system will mistakenly refuse an access effort by a lawful individual, while the false accept rate is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

Furthermore, *Figure 2* analysis shows the accuracy of the experimental results based on the key multi biometric template protection scheme from different scholars [8, 57, 60, 67, 71−75].The result analysis indicated that, Random Projection cancellable technique provides better accuracy in the multi biometric fingerprints and iris sample with 95%, leaving 5% probability for the imposter to misbehave in the biometric template compared to other techniques which are almost at the risk of the attacker. Radha and Karthikeyan [4] suggested that, even though considerable advancement has been made in security enhancement of biometrics and template protection over the past decade, much remains to be done. Since every biometric trait has its specific weaknesses, the security required for all the applications should be adequate.

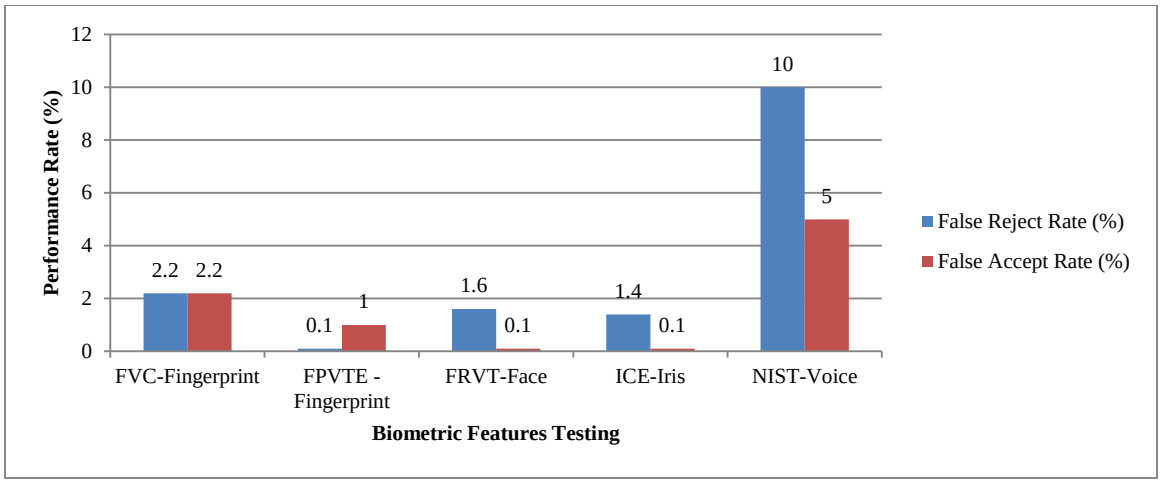

Figure 1 The false reject rate and false accept rate

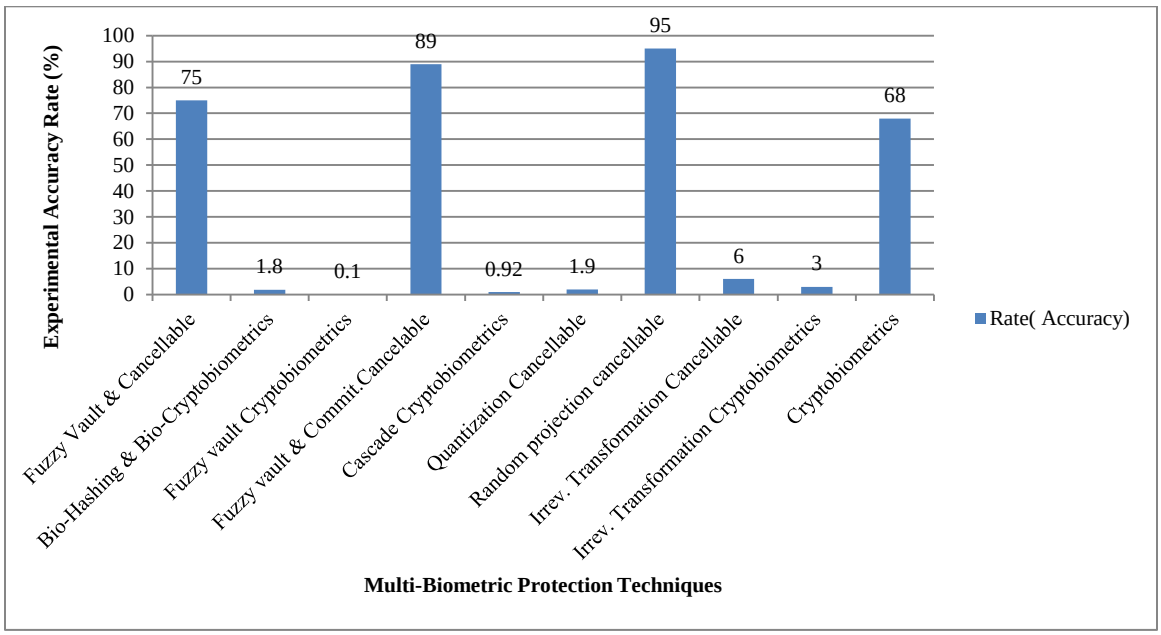

Figure 2 The Multi-biometric template protection patterns

5.Conclusion and future work

Biometric recognitions are extensively adopted and integrated to provide authentication measures that guarantee non-repudiation. Since biometrics is a dominant technology and has immense potential to enhance the security and safety of citizens by protecting and maintaining their identity and privacy. It impacts peoples' lives directly at the individual level, and also from a larger social perspective. Despite its benefits, biometric reveals part of a user's identity, if stolen, it can be used to forge legal documents, passports, or criminal records, which can ensure further destruction than a stolen credit card digit. Unlike passwords, credit cards, or other records, you can't replace physical identifiers. If somebody has photographs of your iris, you can't get another eye. This paper has discussed in details the various methods of protecting a biometric template and the different possible attacks that can be prevented to make a biometric identification system more secure and safe. For instance, at the points of attacks mentioned above, appropriate procedures must be taken both on a conceptual as well as on an organizational level before a biometric device is put into operation. In addition, the safety and secrecy intimidations need to be reserved when assessing the proportionality and the efficiency of the use of a biometric system for a particular aim and in the context of a specific type of application. The biometric deployments should not be presented if the privacy and security intimidations to persons are unpredictable in comparison to the advantages of the system.

From the template protection side, various techniques were discussed to analyze the experimental results. It was further analysed that the security of the present patterns was mostly based on the complexity of brute-force attacks which assumes that the distribution of biometric features is uniform. In practice, an adversary may be able to adventure the non-uniform location of biometric traits to undertake an attack that may need considerably less attempts to compromise the system security. It was, consequently, noted that there was no particular biometric template protection technique that proved satisfactory in the ideal template protection pattern. For that reason, there is still need for more research work to be done to establish secure, reliable, efficient and foolproof protection of the biometric template. This paper enthusiastically tried to raise the consciousness of people about the security of the information they give during the multiple registration in their day-to-day life activities. Thus, a necessity for the scientists working in this area to think about alternative measures for a better security and privacy of people's information. In future work, the multi biometric encryption & decryption approach for securing biometric fingerprint, facial or iris templates amalgamated could be the most efficient and popular approach in securing the biometric template database.

Acknowledgment

The authors acknowledge Muni University, Uganda and the Nelson Mandela African Institution of Science and Technology, Tanzania for providing financial and bibliographic resources. The authors are thankful to anonymous reviewers for their feedback and useful suggestions.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Gobi M, Kannan D. A secured public key cryptosystem for biometric encryption. International Journal of Computer Science and Network Security. 2015; 15(1):49-57.

[2] Malhotra S, Kant C. A novel approach for securing biometric template. International Journal of Advanced Research in Computer Science and Software Engineering. 2013; 3(5):397-403.

[3] https://www.theindependent.co.zw/2016/03/04/zanu-pf-not-sincere-in-re-engaging-world-bank-imf/. Accessed 26 May 2018.

[4] Radha N, Karthikeyan S. A study on biometric template security. ICTACT Journal on Soft Computing. 2010; 1(1):37-41.

[5] Asha S, Chellappan C. Biometrics: an overview of the technology, issues and applications. International Journal of Computer Applications.2012; 39(10):35-52.

[6] Xi K, Hu J. Bio-cryptography. In handbook of information and communication security 2010 (pp. 129-57). Springer, Berlin, Heidelberg.

[7] Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV. Biometric encryption. ICSA Guide to Cryptography. 1999:649-75.

[8] Jain AK, Nandakumar K, Nagar A. Biometric template security. EURASIP Journal on Advances in Signal Processing. 2008.

[9] Gowdhaman P, Antonyraj K, Annamalai V. An effective approach on physical and dielectric properties of PZT-PVDF composites. International Journal of Advances in Scientific Research. 2015; 1(8):322-8.

[10] Ratha NK, Connell JH, Bolle RM. An analysis of minutiae matching strength. In international conference on audio-and video-based biometric person authentication 2001 (pp. 223-8). Springer, Berlin, Heidelberg.

[11] Joshi M, Mazumdar B, Dey S. Security vulnerabilities against fingerprint biometric system. arXiv preprint arXiv:1805.07116. 2018.

[12] Latha MU, Rameshkumar K. A study on attacks and security against fingerprint template database. International Journal of Emerging Trends Technology in Computer Science. 2013; 2(5):13-7.
[13] Arjunwadkar M, Kulkarni RV. Biometric device assistant tool: intelligent agent for intrusion detection at biometric device using JESS. International Journal of Computer Science Issues. 2012; 9(6):366-70.
[14] Poongodi P, Betty P. A study on biometric template protection techniques. International Journal of Engineering Trends and Technology. 2014; 7(4):202-4.
[15] Alaswad AO, Montaser AH, Mohamad FE. Vulnerabilities of biometric authentication threats and countermeasures. International Journal of Information & Computation Technology. 2014; 4(10):947-58.
[16] Brindha VE, Natarajan AM. Multi-modal biometric template security: fingerprint and palmprint based fuzzy vault. Journal of Biometrics and Biostatistics. 2012; 3(6):1-6.
[17] Mwema J, Kimwele M, Kimani S. A simple review of biometric template protection schemes used in preventing adversary attacks on biometric fingerprint templates. International Journal of Computer Trends and Technology. 2015; 20(1):12-8.
[18] Mordini E. Biometrics, human body, and medicine: a controversial history. In ethical, legal and social issues in medical informatics 2008 (pp. 249-72). IGI Global.
[19] Jain AK, Nandakumar K, Nagar A. Fingerprint template protection: from theory to practice. In security and privacy in biometrics 2013 (pp. 187-214). Springer, London.
[20] Nagar A, Nandakumar K, Jain AK. Multibiometric cryptosystems based on feature-level fusion. IEEE Transactions on Information Forensics and Security. 2012; 7(1):255-68.
[21] Phillips PJ, Scruggs WT, O'Toole AJ, Flynn PJ, Bowyer KW, Schott CL, et al. FRVT 2006 and ICE 2006 large-scale results. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2010; 32(5):831-46.
[22] Przybocki M, Martin A. NIST speaker recognition evaluation chronicles. In odyssey: the speaker and language recognition workshop. 2004 (pp. 1-8).
[23] Wilson C, Hicklin AR, Bone M, Korves H, Grother P, Ulery B, et al. Fingerprint vendor technology evaluation 2003: summary of results and analysis report. NIST Technical Report NISTIR. 2004.
[24] Al-Saggaf AA, Acharya H. Statistical hiding fuzzy commitment scheme for securing biometric templates. International Journal of Computer Network and Information Security. 2013; 5(4):8-16.
[25] Maltoni D, Maio D, Jain AK, Prabhakar S. Handbook of fingerprint recognition. Springer Science & Business Media; 2009.
[26] Tigga R, Wanjari A. A survey on template protection scheme for multimodal biometric system. International Journal of Science and Research. 2015; 4(7):768-72.
[27] Nandakumar K, Jain AK. Biometric template protection: Bridging the performance gap between theory and practice. IEEE Signal Processing Magazine. 2015; 32(5):88-100.
[28] Sandhya M, Prasad MV, Chillarige RR. Generating cancellable fingerprint templates based on Delaunay triangle feature set construction. IET Biometrics. 2016; 5(2):131-9.
[29] Simoens K, Bringer J, Chabanne H, Seys S. A framework for analyzing template security and privacy in biometric authentication systems. IEEE Transactions on Information Forensics and Security. 2012; 7(2):833-41.
[30] Rathgeb C, Busch C. Multi-biometric template protection: issues and challenges. In New Trends and Developments in Biometrics 2012:173-90.
[31] Ratha NK, Chikkerur S, Connell JH, Bolle RM. Generating cancelable fingerprint templates. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2007; 29(4):561-72.
[32] Sutcu Y, Sencar HT, Memon N. A secure biometric authentication scheme based on robust hashing. In proceedings of the workshop on multimedia and security 2005 (pp. 111-6). ACM.
[33] Teoh AB, Toh KA, Yip WK. 2^ N discretisation of biophasor in cancellable biometrics. In international conference on biometrics 2007 (pp. 435-44). Springer, Berlin, Heidelberg.
[34] Supriya VG, Manjunatha SR. Chaos based cancellable biometric template protection scheme-a proposal. International Journal of Engineering Science Invention. 2014; 3(11):14-24.
[35] Hao F, Anderson R, Daugman J. Combining crypto with biometrics effectively. IEEE Transactions on Computers. 2006; 55(9):1081-8.
[36] Billeb S, Rathgeb C, Reininger H, Kasper K, Busch C. Biometric template protection for speaker recognition based on universal background models. IET Biometrics. 2015; 4(2):116-26.
[37] Draper SC, Khisti A, Martinian E, Vetro A, Yedidia JS. Using distributed source coding to secure fingerprint biometrics. In international conference on acoustics, speech and signal processing 2007 (pp. 129-32). IEEE.
[38] Yildiz M, Yanikoğlu B, Kholmatov A, Kanak A, Uludağ U, Erdoğan H. Biometric layering with fingerprints: template security and privacy through multi-biometric template fusion. The Computer Journal. 2016; 60(4):573-87.
[39] Jeny JV, Jangid CJ. Multibiometric cryptosystem with fuzzy vault and fuzzy commitment by feature-level fusion. International Journal of Emerging Technology and Advanced Engineering. 2013; 3(3):449-52.
[40] Gomez-Barrero M, Maiorana E, Galbally J, Campisi P, Fierrez J. Multi-biometric template protection based on homomorphic encryption. Pattern Recognition. 2017; 67:149-63.
[41] Ratha NK, Bolle RM, Pandit VD, Vaish V. Robust fingerprint authentication using local structural similarity. In workshop on applications of computer vision 2000 (pp. 29-34). IEEE.

[42] Patel VM, Ratha NK, Chellappa R. Cancelable biometrics: a review. IEEE Signal Processing Magazine. 2015; 32(5):54-65.
[43] Boyen X, Dodis Y, Katz J, Ostrovsky R, Smith A. Secure remote authentication using biometric data. In annual international conference on the theory and applications of cryptographic techniques 2005 (pp. 147-63). Springer, Berlin, Heidelberg.
[44] Bringer J, Morel C, Rathgeb C. Security analysis and improvement of some biometric protected templates based on Bloom filters. Image and Vision Computing. 2017; 58:239-53.
[45] Li Q, Chang EC. Robust, short and sensitive authentication tags using secure sketch. In proceedings of the workshop on multimedia and security 2006 (pp. 56-61). ACM.
[46] Sutcu Y, Li Q, Memon N. Protecting biometric templates with sketch: theory and practice. IEEE Transactions on Information Forensics and Security. 2007; 2(3):503-12.
[47] Buhan I, Doumen J, Hartel P, Veldhuis R. Fuzzy extractors for continuous distributions. In proceedings of the symposium on information, computer and communications security 2007 (pp. 353-5). ACM.
[48] Buhan I, Doumen J, Hartel P, Veldhuis R. Secure ad-hoc pairing with biometrics: SAfE. Proceedings IWSSI. 2007:450-6.
[49] Anitha P, Narayana Rao K, Rajashekhar VR, Hari Krishna C. Security for biometrics protection between watermarking and visual cryptography. SSRG International Journal of Electronics and Communication Engineering. 2017:64-71.
[50] Nandakumar K, Jain AK. Multibiometric template security using fuzzy vault. In international conference on biometrics: theory, applications and systems 2008(pp. 1-6). IEEE.
[51] Khan SH, Akbar MA, Shahzad F, Farooq M, Khan Z. Secure biometric template generation for multi-factor authentication. Pattern Recognition. 2015; 48(2):458-72.
[52] Moi SH, Saad P, Rahim NA, Ibrahim S. Error correction on iris biometric template using Reed Solomon codes. In Asia international conference on mathematical/analytical modeling and computer simulation 2010 (pp. 209-14). IEEE.
[53] Gaddam SV, Lal M. Efficient cancelable biometric key generation scheme for cryptography. IJ Network Security. 2010; 11(2):61-9.
[54] Ang R, Safavi-Naini R, McAven L. Cancelable key-based fingerprint templates. In Australasian conference on information security and privacy 2005 (pp. 242-52). Springer, Berlin, Heidelberg.
[55] Jo YH, Jeon SY, Im JH, Lee MK. Security analysis and improvement of fingerprint authentication for smartphones. Mobile Information Systems. 2016.
[56] Mohammed MA. Biometric based authentication using two-stage fingerprint privacy protection for file storage on server. International Journal of Computer Science and Mobile Computing. 2016; 5(3):377-87.
[57] Sutcu Y, Li Q, Memon N. Secure biometric templates from fingerprint-face features. In conference on computer vision and pattern recognition 2007 (pp. 1-6). IEEE.
[58] Uludag U, Pankanti S, Jain AK. Fuzzy vault for fingerprints. In international conference on audio-and video-based biometric person authentication 2005 (pp. 310-9). Springer, Berlin, Heidelberg.
[59] Lu L, Peng J. Finger multi-biometric cryptosystem using feature-level fusion. International Journal of Signal Processing, Image Processing and Pattern Recognition. 2014; 7(3):223-36.
[60] Jain AK, Nandakumar K, Nagar A. Biometric template security. EURASIP Journal on Advances in Signal Processing. 2008:1-17.
[61] Geethanjali N, Thamaraiselvi K, Priyadharshini R. Feature level fusion of multibiometric cryptosystem in distributed system. International Journal of Modern Engineering Research. 2012; 2(6):4643-7.
[62] Al-Hamami AH, Alhafez MA. Enhancing security to protect e-passport against photo forgery. Global Journal of Computer Science and Technology. 2016; 16(6).
[63] Hooda R, Gupta S. Fingerprint fuzzy vault: a review. International Journal of Advanced Research in Computer Science and Software Engineering. 2013; 3(4):479-82.
[64] Nguyen MT, Truong QH, Dang TK. Enhance fuzzy vault security using nonrandom chaff point generator. Information Processing Letters. 2016; 116(1):53-64.
[65] Fu B, Yang SX, Li J, Hu D. Multibiometric cryptosystem: model structure and performance analysis. IEEE Transactions on Information Forensics and Security. 2009; 4(4):867-82.
[66] Camlikaya E, Kholmatov A, Yanikoglu B. Multi-biometric templates using fingerprint and voice. In biometric technology for human identification V 2008. SPIE.
[67] Othman A, Ross A. On mixing fingerprints. IEEE Transactions on Information Forensics and Security. 2013; 8(1):260-7.
[68] Yang W, Hu J, Wang S, Stojmenovic M. An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures. Pattern Recognition. 2014; 47(3):1309-20.
[69] Ashish M, Sinha G. Biometric template protection. Journal of Biostatistics and Biometric Applications. 2016; 1(2):1-7.
[70] Rathgeb C, Gomez-Barrero M, Busch C, Galbally J, Fierrez J. Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris. In international workshop on biometrics and forensics 2015 (pp. 1-6). IEEE.
[71] Canuto AM, Pintro F, Xavier-Junior JC. Investigating fusion approaches in multi-biometric cancellable recognition. Expert Systems with Applications. 2013; 40(6):1971-80.
[72] Cimato S, Gamassi M, Piuri V, Sassi R, Scotti F. Privacy-aware biometrics: design and implementation of a multimodal verification system. In annual

computer security applications conference 2008 (pp. 130-9). IEEE.
[73] Fang C, Li Q, Chang EC. Secure sketch for multiple secrets. In international conference on applied cryptography and network security 2010 (pp. 367-83). Springer, Berlin, Heidelberg.
[74] Kelkboom EJ, Zhou X, Breebaart J, Veldhuis RN, Busch C. Multi-algorithm fusion with template protection. In international conference on biometrics: theory, applications, and systems 2009 (pp. 1-8). IEEE.
[75] Paul PP, Gavrilova M. Multimodal cancelable biometrics. In international conference on cognitive informatics & cognitive computing 2012 (pp. 43-9). IEEE.

Taban Habibu is currently a PhD Scholar in the Department of Applied Mathematics and Computational Sciences; Nelson Mandela African Institution of Science and Technology. He works as Assistant Lecturer and Senior Cisco Instructor in the Department of Computer and Information Science, Muni University-Uganda. His area of research and interest are; Biometric Technology, Data Security, Network Security, Mobile and Web Technologies, Artificial intelligence, Data Mining and Parallel Computing, Machine Learning, Image Processing and ICT4D.
Email: habi20008@gmail.com

Anael E. Sam is a Senior Lecturer in the Department of Communication Science and Engineering, School of Computational and Communication Sciences and Engineering (CoCSE). The Nelson Mandela African Institution of Science and Technology.