Review Analysis of Properties for an Ideal Secure Biometric Template Scheme

Phiwa Mzila
Modelling and Digital Sciences, Information Security, CSIR, Meiring Naude, Pretoria, South Africa

Keywords: Biometric Templates Protection, Privacy, Security, Performance, Accuracy, Cancellable Cryptosystem.

Abstract: With new advances in technologies, biometrics is becoming emerging technology for verification and authentication of individuals. However, the storage of biometric templates still needs necessary attention since it poses major threats to user privacy and system security. To mitigate this problem, various biometric protection techniques have been proposed. Most of these schemes aim to satisfy diversity, revocability, security and performance properties, as requirements for ideal secured biometric template storage. Conventionally, priority is given to robustness of biometric system in terms of its accuracy, and high performance with regards to matching and recognition rate. Little attention is payed to user privacy and system security. In this paper, existing work in biometric template protection schemes are reviewed, analysed, and compared with reference to properties of an ideal biometric secured template system. The question of properties needed for a complete and ideal biometric secured template system is beyond the scope of this research.

1 INTRODUCTION

Biometric systems are adopted in many applications to fight crime such as illegitimate access to information, fraud, and attacks on computerized systems. As biometric technology advances, so does hacking technology. In most cases, hackers aim to exploit weaknesses in biometric systems. One of the areas that is vulnerable to such an attack is the biometric templates database. This challenge has enticed developers and researchers to study and propose different techniques, approaches, and schemes to ensure a secure storage of biometrics templates.

Four properties are essential for every biometric template protection system: (Breebaart et al., 2009):

- Diversity: the protected template should by no means allow cross matching in the databases. This is to ensure that user's privacy is not compromised.
- Revocability:it should be possible to revoke a template when it is compromised by the hackers and reissue a different one based on the biometric information.
- Performance: the template protection techniques should not reduce the performance of the system.
- Security: it should be computationally difficult to recover the original biometric template from the stored template. This will go a long way to ensure that hackers do not fabricate a physical spoof of the biometric trait from the stolen template.

Application of these properties involves a repeated distortion of biometric signals or features using noninvertible transforms. This approach is intended to reduce attacks on stored templates by replacing an original biometric traits with one that has been transformed (Feng et al., 2008). This technique is very useful when each person is enrolled with more than one application or system.

The focus of biometrics research has been on accuracy, speed, cost, and robustness challenges. However, more attention has been given to security and privacy issues of biometric systems in recent research. This means that the acceptancy of modern biometric systems should rely more on the ability of the system providing a direct answer to questions such as "What happens when the biometric template is compromised or stolen", "Can my template, registered for voting purposes, still be used by the vetting system somewhere else?".

Biometric template protection schemes which address the properties of an ideal system are normally categorized as biometric cryptosystems and feature

Mzila, P.
Review Analysis of Properties for an Ideal Secure Biometric Template Scheme.
DOI: 10.5220/0005727303330339
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 333-339
ISBN: 978-989-758-167-0

transformation (Jain et al., 2008). Biometric cryptosystems generate a digital key from a biometric trait and securely bind it to a biometric. This offers a solution to biometric-dependent key-release and biometric template protection (Uludag et al., 2004). Feature transformation biometrics consist of intentional and repeatable distortions of biometric signals based on transforms that provide a comparison of biometric templates in the transformed domain (Ratha et al., 2011). Both technologies are designed to meet two major requirements of biometric information protection, (Rathgeb and Uhl, 2011) which are:

- Irreversibility: it should be computationally expensive to reconstruct the original biometric template from the stored reference data, while it should be easy to generate the protected biometric template;
- Unlinkability: different versions of protected biometric templates can be generated based on the same biometric data, while protected templates should not allow cross-matching.

Security and privacy play an important role in user acceptancy of biometric systems. Threats to both these properties are imperative and counter-measures need to be considered for ideal biometric template protection scheme. Security, in the context of biometrics, refers to the difficulty level to obtain false acceptance. Privacy refers to the protection level of the system against an unintended use of biometric data (other than the verification work). Privacy threats in a biometric system are defined as the ability to get the data and cross match it with other systems for benefits (Turk and Pentland, 1991).

In this review, existing work (on both biometric systems and template protection schemes) are reviewed, analyzed, and compared with reference to the degree to which they address user privacy, system security, performance, and accuracy in developing ideal biometric secured template system. The question of properties needed for a complete and ideal biometric secured template system is beyond the scope of this research.

The rest of the paper is structured as follows: Section 2 presents problem definition, in section 3 its literature review, biometric template protection scheme requirements are analysed in section 4 , in section 5 major advantage of cancellable aproach is presented, section 6 we discuss challenges facing biometric template protection shemes and finally its our conclusion.

2 PROBLEM DEFINITION

There are seven basic criteria or properties for a biometric system: uniqueness, universality, permanence, collectability, performance, acceptability, and circumvention (Rahultech, 2010). On the other hand, there are four properties for biometric template protection scheme: revocability, diversity, performance and security (Radha, 2011). A well-developed traditional biometric system, can be measured its free error matching ability, with high accuracy and performance. In a basic biometric system performance vs. accuracy approach is employed, however this approach overlooks the very critical aspect and requirement of modern biometric systems, which is user privacy and system security. For such a system to be accepted by users, it should be sufficiently robust against fraudulent methods and attacks to the system, thus providing sufficient privacy.

In attempting to address these concerns, various biometric template protection schemes have been proposed. The fundamental purpose of these schemes is to provide counter measures against most potentially damaging attacks on biometric templates stored in the system database, by adopting security vs. privacy approach. Figure 1 shows a relationship between performance vs. accuracy and security vs. privacy, projecting an ideal robust secure biometric template system.

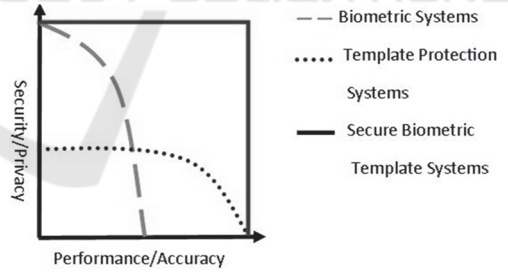

Figure 1: Security/Privacy vs. Performance/Accuracy.

Normally, in a biometric system a user claims an identity and provides a biometric sample from the sensor. After feature extraction, features are compared with existing biometric templates stored in a database and if the new biometric matches the one in the database, the user is verified to be a genuine user of the system or denied access as shown in figure 2.

Any compromise of the biometric template database can lead to the following vulnerabilities:

- A biometric template can be substituted by an impostor's template for future unauthorized ac-

access;

- An imposter can create a physical spoof from the stored template to gain unauthorized access to the system, and cross match other systems which use the same biometric trait;
- The stolen template can be replayed to the matcher to gain unauthorized access.

A prospective act of abuse to biometric system is cross-matching, where the biometric traits are used for purposes other than the intended purpose. This can be a case where a fingerprint template that has been stolen from a financial institution's database (such as a bank) is used to search a vetting system's database or crosslink to a person's health records.

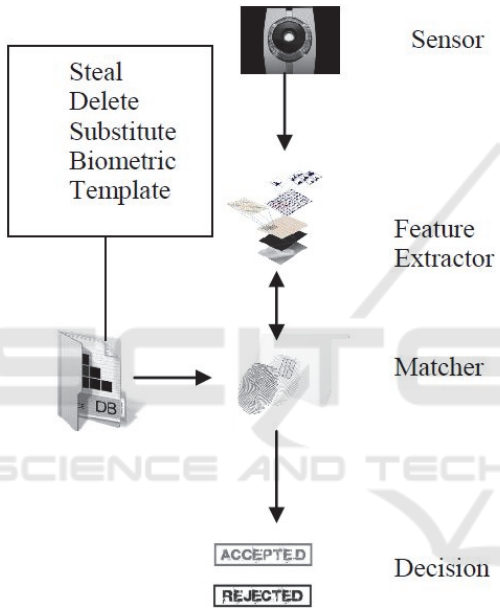

Figure 2: Overview of Biometric Authentication System.

Revocability is one requirement out of the other four that draws much interest in this paper. Based on the biometric template protection scheme metrics in Table 1, hybrid approach and modern cryptosystems perform better with revocability and diversity. The main reason for that (mostly for hybrid schemes) is the employment of user chosen key/password as one of the techniques to form a hybrid scheme. Every time a transformed template is compromised, it can be revoked and a new template can be generated from new user password/key. But when a template transformation is based on a key released or key generated from the minutiae, it means even if a compromised template is revoked it can be regenerated from the same fingerprint (minutia points location). This means that an attack such as brute force attack has the ability hand to crack that particular hybrid scheme hence compromising the whole security feature. It is the same reason why key binding and key generation score is low for revocability and diversity.

3 LITERATURE REVIEW

In the literature, properties of an ideal biometric template protection scheme are found in cancellable techniques. Attacks against biometric templates stored in database are potential security threats. As a result, cancellable approaches have been proposed to provide security and user privacy against such attacks (Ratha et al., 2011).

A cancellable approach implements cancelability by designing methods to transform the true signal and create alternatives for matching. This type of method can be divided into two categories. One that tries to mask original patterns by mixing artificial texture or noise (Connell et al., 2010). The other that uses some non-invertible transformations to distort the original biometric patterns (Ratha et al., 2007). Transformation functions are non-invertible because of their one-way orientation. This is easy to calculate but difficult to change (in polynomial time) even if the attacker steals a transformed template and/or transformation key. The transformation parameters are determined using external added pseudo-randomness, (such as a user pin or token). The transformed patterns can be changed (or revoked/reissued) by altering the user pin or token. As a result, this method achieves cancelability. Compared to other template protection methods, cancellable biometrics can preserve the biometric representation. Traditional cancellable approaches often reduce recognition accuracy (Ratha et al., 2007).

Teoh et al., 2006, and Kanade et al., 2009 proposed applying cryptographic methods to biometrics in order to deal with privacy and security. These methods require extracting non-changing patterns from biometric data, which is often challenging. Among them, one widely used method is biometric biohashing (Lumini and Nanni, 2007). In this scheme, the template is mixed with user specific random information, yielding a new representation. An error-tolerant discretization method is used to quantize the feature description and reduce uncertainty. The projection acts as a linear transformation of the biometric pattern. It can protect the true template and ensure high-security, since the user specific random information can be generated with different keys, ensuring the revocability of the

Table 1: Biometric template protection scheme metrics.

	Diversity	Revocability	Security	Performance
Biohashing	high	high	low	medium
Salting	high	high	low	low
Cancellable	high	high	high	low
Key binding	low	low	high	low
Key generation	low	low	high	low
Hybrid	high	high	medium	medium
Modern Systems	high	high	medium	medium

templates.

Moreover, the introduction of user keys can further increase the discriminability of the templates. However, external randomness needs to be stored in a smart card or a token, making it inconvenient in large scale applications. If the key is compromised, the scheme is insecure since the projection process is invertible.

Chang et al., 2004 and Sutcu et al., 2007 presented another scheme called key-generation. In contrast with the key-binding method discussed below, the helper data of the key-generation scheme is only derived from the biometric traits. The cryptographic key is directly generated from the help data. The idea of secure sketch and fuzzy extractor (Dodis et al., 2008) is an example design of key-generation cryptosystem. The secure sketch is the helper data extracted from the original biometric patterns which leaks limited information of the biometric data while the fuzzy extractor can generate cryptographic a key from biometric features. This scheme also suffers from privacy issues. In addition, the stability and diversity of the generated key is difficult to achieve simultaneously (Jain et al., 2008).

A popular scheme in cryptosystems is key-binding (Hao et al., 2006) and (Uludag and Jain, 2006). It is designed to protect the security of both biometric templates and cryptographic keys. This method depends on storing a helper data obtained by binding a key with the biometric template (Jain et al., 2008). This scheme is non-invertible since it is computationally infeasible to decode the key or biometric template without knowing the biometric data. One typical design of key-binding system is the fuzzy vault. It was proposed by (Juels and Sudan, 2006). The fuzzy vault incorporates error correction code (ECC) with local biometric features to tolerate the within-class variance. The method has proved to be effective in tolerating biometric data variations. ECC based fuzzy schemes were first designed for a cryptosystem, but are particularly suited to biometric data and biometric template protection. Therefore, it is often used in conjunction with other template protection methods, such as biometric hardening, to achieve cancelability.

However, (Simoens et al., 2009) show that attacks on the fuzzy template protection scheme is possible. In particular, it is possible for an attacker to determine whether two documents are encrypted using the same biometric data. Even if this does not mean that the biometric templates are compromised, it is still a potential threat to user privacy.

4 BIOMETRIC TEMPLATE PROTECTION SCHEME REQUIREMENTS

The major challenge in the biometric template protection schemes is to design an approach to template protection, which meets all four requirements (diversity, revocability, security and performance) without compromising either of them, or the accuracy of the system. The need for trusted biometric systems that protect against security and privacy vulnerabilities while maintaining high performance and accuracy is absolute.

Table 1 depicts the relationship between biometric template protection schemes and properties defining an ideal secure biometric template system. The measurement criteria are high, medium and low for each of the schemes, where high indicates that a requirement is met fully, medium indicates that a requirement is met partially and low indicates that a requirement is least met or not met at all. These schemes are described briefly below.

Biohashing is a biometric template protection approach in which features from a biometric template are transformed, using a transformation function defined by a password or a key known only to the user (Mwele and Kiman, 2015). This key or password needs to be securely stored and remembered by the user for authentication. The major drawback of biohashing, when compared to cancellable biometrics, is its reduced performance when a

legitimate token is retrieved and presented by an adversary purporting to be a legitimate user.

In a salting based scheme, biometric features are transformed using an invertible function defined by a user-specific key or password, which must be kept secret. The introduction of a secret key ensures revocability. In fact, in case a template is compromised, it is easy to revoke and replace it with a new template generated by a different user-specific key.

If the user-specific key is compromised, the template is no longer secure, because the transformation is invertible (Das et al., 2012).

A hybrid scheme (Malhotra and Verma, 2013) is a multimodal biometric system that utilizes more than one physiological or behavioural characteristic for enrolment, verification, or identification. In this work, they combined one physical and one behavioural approach for identification or verification to uniquely identify a person. The approach takes two different biometric traits. One being a fingerprint as a physiological, and the other is an online signature (as behavioural biometric trait).

Both are sensed by a sensor, features are extracted by feature extractor modules, matcher modules match the traits with stored templates, and each decision module decides the perfect matches. Finally, decisions are combined in a fusion unit using a simple "AND" operator and the decision is taken whether the individual is an intruder or not.

Biometric cryptosystems can be classified into two main categories: key binding schemes, and key generation schemes (Maltoni et al., 2009). In the key binding approach, a cryptographic and an unprotected fingerprint template are bonded together within a cryptographic framework, to generate the helper data. It is computationally difficult to decode the key or the template from the helper data without the knowledge of the user's fingerprint data. The helper data is obtained by combining the enrolment template with cipher-text obtained from an error correcting code using the key as the message. A cipher-text recovered from a feature set (that is similar but not identical to the template) is affected by a certain amount of error correction code. The exact key is recovered from the cipher-text that contains some error. If the correct key is recovered, it means that the feature set and the protected template resulted in a match. In the key generation approach, a key is derived directly from the biometric signal. The advantage of this approach is that there is no need for user-specific keys or tokens as required by a biometric salting approach. A problem with this approach is that is very hard to generate a key with high stability and entropy.

Modern cryptography systems have emerged in recent years, and a number of papers have been published on biometric systems in which biometrics and homomorphic encryption work together, for either authentication or identification purposes. These systems have cryptographic protocols based on secure multiparty computation and most of them use the superior properties of homomorphic encryption schemes to overcome security and privacy threats.

5 MAJOR ADVANTAGES OF CANCELLABLE APPROACH IN BIOMETRIC TEMPLATE PROTECTION

Cancellable biometrics offer several advantages over generic biometric systems (Rathgeb and Busch, 2013):

- Privacy: within biometric cryptosystems and cancellable biometrics the original biometric template is obscured such that a reconstruction is unfeasible
- Secure key release: biometric cryptosystems provide keys release mechanisms based on biometrics
- Pseudonymous authentication: authentication is performed in the encrypted domain and thus the biometrics reference is a pseudonymous identifier.
- Revocability and renewable of templates: several instances of secured templates can be generated.
- Increased security: biometric cryptosystems and cancellable biometrics are prevented from several traditional attacks against biometric systems.

With respect to the design goals, biometric cryptosystems and cancellable biometrics offer significant advantages to enhance the privacy and security of biometric systems, providing reliable biometric authentication at a high-security level. Several new issues and challenges arise by deploying these technologies (Cavoukian and Stoianov, 2009).

6 CHALLENGES FACING BIOMETRIC TEMPLATE PROTECTION SCHEMES

One challenging aspect regarding biometric template protection is the issue of alignment, since template protection technologies tend to obscure original

biometric signals in an irreversible manner. The majority of published approaches to template protection schemes indicated a significant decrease in recognition accuracy (Rathgeb and Uhl, 2011).

When considering biometric template protection technologies, it is not actually clear which biometric characteristics to apply in which type of application. In fact, it has been shown that even the iris may not exhibit enough reliable information to bind or extract sufficiently long keys, to providing acceptable trade-offs between accuracy and security. Stability of biometric features is required to limit information leakage of stored helper data. In addition, feature adaption schemes that preserve accuracy must be utilized in order to obtain common representations of arbitrary biometric characteristics. Several approaches to address such impediments in biometric template protection schemes have been developed. Extracting fixed-length binary fingerprint templates (Bringer and Despiegel, 2010) and (Xu and Veldhuis, 2010) are an example.

7 CONCLUSIONS

In this paper we have reviewed the properties for a generic biometric system and biometric template protection schemes. These requirements were analysed and measured against different approaches proposed in the literature to define an ideal biometric template protection schemes, which provides high performance vs. accuracy and security vs. privacy. In the future we would like to develop a more secure hybrid scheme that will use password hardening technique with one or more of the well-known schemes such as surface folding and fuzzy vault without compromising performance to improve the revocability aspect of the scheme.

REFERENCES

Breebaart, J., Yang, B., Dulman, B., Busch, C., 2009. Biometric Template Protection: The need for open standards. *Privacy and Data Security Journal.*

Bringer J., Despiegel, V., 2010. Binary Feature Vector Fingerprint Representation from Minutiae Vicinities. *In Proc. of the 4th IEEE Int. Conf. on Biometrics: Theory, applications and systems (BTAS'10), pp. 1–6.*

Cavoukian, A., Stoianov, A., 2009. Biometric Encryption: The New Breed of Untraceable Biometrics. *In Biometrics: fundamentals, theory, and systems. Wiley.*

Chang, Y., Zhang, W., and Chen, T., 2004. Biometrics-Based Cryptographic Key Generation. *Multimedia and Expo, ICME'04, IEEE Imternational Conference on, Taipei, pp. 2203-2206.*

Connell, J. H., Ratha, N. K., and Zuo,J., 2010. Salting System and Method for Cancelable Iris Biometrics. *US Patent, No. 0046808.*

Das, P., Karthik, K., and Garai, B. C., 2012. A Robust Alignment-free Fingerprint Hashing Algorithm Based on Minimum Distance Graphs. *Pattern Recognition, 45(9), 3373-3388.*

Dodis, Y., Ostrovsky, R., L. Reyzin and Smith, A., 2008. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT '04), Interlaken, Switzerland, pp. 523-540.*

Feng, Y. C., Yuen, P. C. and Jain, A. K., 2008. A Hybrid Approach for Face Template Protection. *SPIE Defense and Security Symposium, Vol. 102, No. 2, pp. 169-177.*

Hao, F., Anderson, R and Daugman, J., 2006. Combining Crypto with Biometrics Effectively. *IEEE Transactions on Computers, pp. 1081-1088.*

Jain, A., Nandakumar, K., Nagar, A., 2008. Biometric Template Security. *Journal on Advances in Signal Processing, pp. 1-17. doi:10.1155/2008/579416.*

Juels, A., Sudan, M., 2006. A Fuzzy Vault Scheme. *Designs, Codes and Cryptography, Vol. 38, No. 2, pp. 237- 257. doi:10.1007/s10623-005-6343-z.*

Kanade, S., Petrovska-Delacretaz, D., and Dorizzi, B., 2009. Cancelable Iris Biometrics and Using Error Correcting Codes to Reduce Variability in Biometric Data. *Computer Vision and Pattern Recognition, CVPR, IEEE Conference, Miami, pp. 120-127.*

Kerschbaum, F., Atallah, M. J., M'Raïhi, D., Rice, J. R., 2004. Private Fingerprint Verification without Local Storage. *In ICBA. (Hong Kong, China), pp. 87–394.*

Lumini, A., Nanni, A., 2007. An Improved BioHashing for Human Authentication. *Pattern Recognition, Vol. 40, No. 3, pp. 1057-1065. doi:10.1016/j.patcog.2006.05.030.*

Malhotra S., Verma, C., 2013. A Hybrid Approach for Securing Biometric Template. *International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Vol. 2, No. 5.*

Maltoni, D., Maio, D., Jain, A. and Prabhakar, S., 2009. *HandBook of Fingerprint Recongnition.* Springer, 2nd Edition.

Mwele, J., Kiman, S., 2015. A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates. *International Journal of Computer Trends and Technology, 20(1), pp. 12-18.*

Radha, N., Karthikeyan, S., 2011. An Evaluation of Fingerprint Security Using Non-invertible Biohash. *International Journal of Network Security & Its Applications (IJNSA), 3(4).*

Rahultech, 2010, IT trends-latest/recent trends in information technology http://rtmnuittrends.blogspot.com/2010/09/biometrics.html

Ratha, N., Chikkerur, S., and Connell, J., 2007. Generating

Cancelable Fingerprint Templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 4, pp. 561-572. doi:10.1109/TPAMI.2007.1004.*

Ratha, N. K., Connell J. H., Bolle, R. M., 2011. Enhancing Security and Privacy in Biometrics-based Authentication Systems. *IBM Syst J 40: 614-634.*

Rathgeb, C., Busch, C., 2013. Multi-Biometric Template Protection: Issues and Challenges. *In New Trends and Developments in Biometrics, chapter 8, pp. 173-190.*

Rathgeb, C., and Uhl, A., 2011. A Survey on Biometric Cryptosystems and Cancelable Biometrics, *EURASIP JIS, vol. 3, pp. 1–25.*

Simoens, K., Tuyls, P., and Preneel, B., 2009. Privacy Weaknesses in Biometric Sketches. *Security and Privacy, 2009 30th IEEE Symposium, pp. 188-203.*

Sutcu, Y., Li, Q., and Memon, N., 2007. Protecting Biometric Templates with Sketch: Theory and Practice. *Information Forensics and Security, IEEE Transactions on, Vol. 2, No. 3, pp. 503-512. doi:10.1109/TIFS.2007.902022.*

Teoh, A., Goh, A., Ngo, D., 2006. Random Multispace Quantization as an Analytic Mechanism for Biohashing of Biometric and Random Identity Inputs. *IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 28, No. 12, pp. 1892-1901. doi:10.1109/TPAMI.2006.250*

Turk, M. A., Pentland, A. P., 1991. Face recognition using eigenfaces. *In Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 586–591.*

Uludag, U., Jain, A., 2006. Securing Fingerprint Template: Fuzzy Vault with Helper Data. *Proceedings of the Conference on Computer Vision and Pattern Recognition Workshops, New York, p. 163.*

Uludag, U., Pankanti, S., Jain, A., 2004. Biometric cryptosystems: Issues and Challenges, pp. 948–960. *In Proceedings of the IEEE.*

Xu, H., Veldhuis, R. N., 2010. Binary Representations of Fingerprint Spectral Minutiae Feature. *In Proc. of the 20th Int. Conf. on Pattern Recognition (ICPR'10), pp. 1212–1216.*