American Research Journal of Computer Science and Information Technology (ARJCSIT)
Volume 1, 17 pages

AMERICAN RESEARCH JOURNALS
An Academic Publishing House

Research Article Open Access

Combining Iris Biometric System and Cryptography Provide a Strong Security Authentication

Abdullah Alsulami, Darren Teo, Weiyi He

Monash University, Australia
abu7ala1@hotmail.com

Abstract: Combining iris biometric system and cryptography will provide a strong security authentication and high performance. Iris-based cryptosystem appears to be the strongest way to generate a key and authenticate users among other biometric recognition such as voice and fingerprint that because the randomness, uniqueness, and stability of Iris. Iris biometric cryptography is a technique used to secure communication and encrypt data between parties using biometric features to provide a False Accept Ratio (FAR) and a False Reject Ratio (FRR).

This report also described the effective biometric security techniques for iris recognition system with high confidence and high performance. The Iris system is based on an experimental analysis of chosen iris images for same and different persons using several steps. The system steps based on the segmentation, normalization, image enhancement, feature extraction, and encoding.

Introduction

With the rapid increasingly of using computer systems and Internet services, a user authentication must be used in order to authenticate users that use the computer systems and internet services. There are several ways that can be used to authenticate the user, what user has such as tokens and identification cards, what user knows such as passwords, and what user is such as iris. However, using such traditional security authentication as passwords, tokens, and identification cards cannot satisfy the advanced security requirements. In general with moving forwards, biometrics are a trustworthy way to authenticate users accurately and robustly. In particular, biometric is the most reliable and secure biometric that a human has. This is because of some reasons that can be listed as the following:

- Iris has a unique feature for each individual.
- Iris is the most unchanged biometrics over the time.
- It is very hard to imitate because of its randomness.

The iris recognition technology is a considerably the popular new phenomenon identification technology that is widely trusted day after day with new methods and applications to provide a high-level security in systems and applications. Nowadays, in commercial and governmental installation the iris cryptography applications are widely used to secure the information and assets that they have in the systems. It is also can be used to restrict access to applications, accounts, and documents that could be used by user/customer.

One of the new developments in this topic is that combining iris feature with the security measures to maximise the security aspects. The main aim of this report is to discuss the techniques that are used to generate both symmetric and asymmetric key schemes as well as demonstrate real life applications.

Key Generation

Biometrics is defined as the automated recognition of a person based on their behavioral or biological characteristics (Kanade, Petrovska-Delacrétaz, & Dorizzi, 2012). There are many different types of biometric

characteristics. Frequently used biometric characteristics are fingerprint, voice, iris and DNA. According to (Hashiyada, 2004), Biometric DNA is the most secure form of cryptography. However, this assignment discusses the accuracy of the Iris in relation to biometric cryptography. The Iris is the centre of the eye pupil. Although it is small (11mm) and hard to capture, the iris provides a unique identity to the individual, as the possibility of incurring a false match rate is very low (Daugman, 2004). Therefore, the iris provides a highly secure authentication for biometric cryptography.

Key generation is defined as the process of generating keys by using symmetric or Rivest-Shamir-Adleman (RSA) algorithms to be applied in cryptography for encrypting and decrypting user data (Ballard, Kamara, & Reiter, 2008). The difference in symmetric and RSA algorithm is such that symmetric encryption makes use of the Data Encryption Standards (DES) and Advanced Encryption Standards (AES) while RSA uses a public key algorithm (Kanade et al., 2012). The symmetric algorithm technique (DES & AES) is considered to be faster and therefore much more suited for real time applications compared to RSA. However, the problems associated with symmetric encryption involves the key used to be kept secret.

Biometrics is an attractive option for key generation, as it is simply reproduced by a legitimate user's own biometrics (Ballard et al., 2008). It will also deter unauthorised users to access, as they do not possess a similar biometric data to the legitimate user. However, according to (Lee, Park, Lee, Bae, & Kim, 2008), one of the main problems is storing the biometric templates in a database, as it is open to attacks as biometric cryptography involves the access of the user biometric features to access protected data. Therefore, the user's biometric feature can be compromised.

Key Generation Security

Biometric authentication compared to regular passwords is more secure as biometrics is part of a legitimate user's own data, hence users do not need to remember any form of passwords. In a typical biometric cryptography system, the key being generated originates from the initial biometric data (Kanade et al., 2012). In cryptography, the strength of a cryptographic key is measured by its entropy (Ballard et al., 2008). The entropy is dependent on the type of biometric and the set of features being used by the biometric key generation. For instance, should there be an access to population statistics, it will greatly reduce the entropy of an individual's data as other individuals with similar biometric templates will be able to falsify a legitimate user's biometric data. A biometric iris data of an individual possess a very high level of entropy as the false match rate for irises are very low. According to (Daugman, 2004), a study conducted to compare 9.1 million different iris images from individuals across Britian, USA, Japan and Korea revealed that the iris can generate a discrimination entropy of about 3.2 b/mm2, meaning the chances of a false match rate for a legitimate user is very low. This enables the iris to identify a legitimate user with a very high level of confidence. Therefore, the security strength of an individual's iris provides a very good biometric template to work on.

Biometric key generators are almost similar to traditional cryptography key generation techniques with the exception of one thing. According to (Ballard et al., 2008), biometric key generators consists of two algorithms; the enrolment algorithm (Enrol) and the key generation algorithm (KeyGen). During the enrolment phase, the biometric samples from an individual are collected and a representation of the output is stored in a data structure called a biometric template (Ballard et al., 2008). After the enrolment phase is complete, the individual can then sign in to the system using their iris, and the system will sign them in. A different user however, will not be able to sign into the system, as each individual's biometric template is different. There is a higher quality of security in iris recognition as the false match rate for an individual's iris is exceptionally low.

The biometric key generation process has many approaches. One of the basic approaches to the biometric key generation is when a new user enrols into the system and their biometric data is entered into the system and

collected. This is the enrolment algorithm. In order to effectively generate a key from the enrolment process for an individual's iris, the imaging system should be able to capture a minimum of 70 pixels (Daugman, 2004), however, ideally the imaging system should be between 80-130 pixels. In order not to damage the human eye when capturing the image, monochrome CCD camera are used as they provide a safe illumination of the iris within the 700-900 nm band (Daugman, 2004).

The enrolment algorithm is an algorithm based on the probability that accepts the number of an individual's input. This input then provides the output of a biometric template to be stored in the system (Ballard et al., 2008). Therefore, in this particular case of the individual's iris, the individual's iris data once input into the system, undergoes a transformation process where a transformation parameter is given to transform the scanned iris data into a key with the verification string. Once the key and verification string is generated from the transformation of the scanned iris, the verification string is extracted from the results and the key is destroyed, as there is no more use for it. The verification string then goes into a database for authentication of future log in for the user as illustrated in Figure 1.

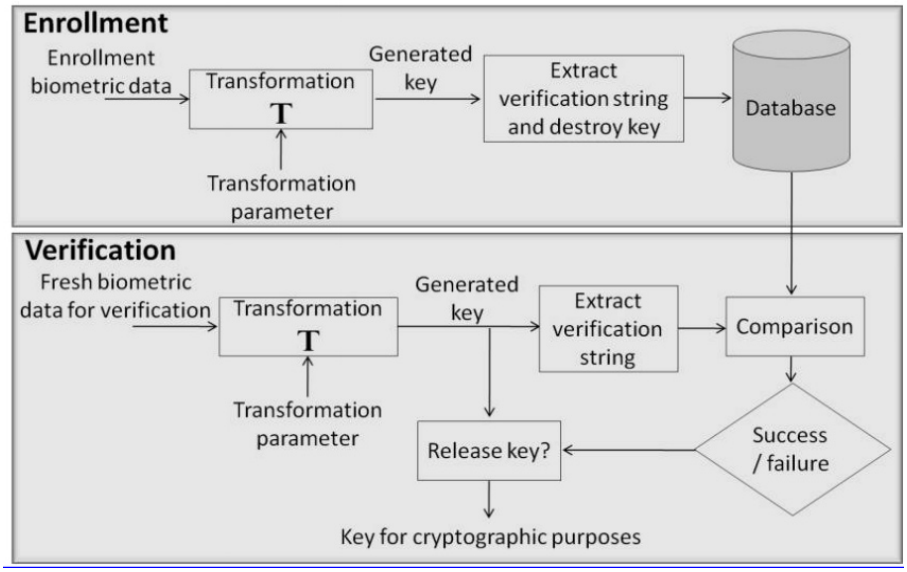

Fig 1. *Use of classical encryption for protection of biometric data. Adapted from (kanade et al., 2012)*

Once the process of the enrolment is completed, and the verification string has been stored in the database, the verification stage can then take place. The verification stage scans in a user's biometric data, in this case, the user's iris. This biometric data similarly undergoes a transformation with the similar transformation parameter as that of the enrolment process. This will generate the key together with the verification string, and then the verification string is extracted from the generated key and compared with the existing database verification string. If both of the verification string matches each other, then the system will release the key for cryptographic purposes and authenticates the individual.

In order for this to be computationally secure, the biometric key generation has to fulfil three requirements for every enrollable user

1. Key Randomness (REQ-KR) (Ballard et al., 2008).
2. Weak Biometric Privacy (REQ-WBP) (Ballard et al., 2008).
3. Strong Biometric Privacy (REQ-SBP) (Ballard et al., 2008).

Key randomness (REQ-KR) is to ensure that the key generated from the biometric template must be statistically or computationally indistinguishable from random. Weak biometric privacy (REQ-WBP) suggest that hacker will not be able to use or learn any of the information should they have access to the user's biometric template. Strong biometric privacy (REQ-SBP) explains that a hacker will not be able to use or learn any of the information even though they have access to the user's biometric template or even if they obtain the key as it is near impossible to compute the function of how the biometric data is processed.

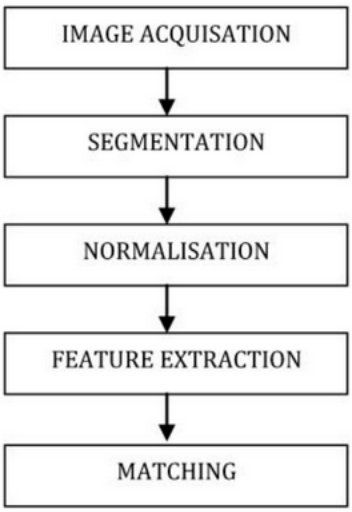

Fig 2. *Steps involved in iris. Adapted from (Balamurugan, Jayarraman, Arulalan, & Lokesh, 2015).*

Figure 2. explains how the iris image is converted from the initial biometric iris of the registered user to eventually obtaining the matching of the user.

Steps involved in iris

Step 1: Image Acquisition

The iris image is captured from the cameras and sensors. The image must clearly display the individual's entire eye with the focus on the iris and pupil. Certain forms of operations may be required in this step to enhance the image clarity such as using histogram equalization or noise removal using filtering (Balamurugan et al., 2015).

Step 2: Segmentation

Segmentation is used to extract only the iris part of the eye from the image to be used. Both the inner and outer boundary of the iris is calculated (Balamurugan et al., 2015).

Step 3: Normalisation

The iris is normalized in this step. Normalisation will allow the system to obtain the iris regions that have a stable dimension in a 2 dimensional form. It will ensure that two images of the identical iris under distinctive limitations possess the same characteristics. This is done through the use of a Hamming Distance where two irises templates are cross-referenced with each other. The Hamming Distance will also create a noise-masking feature to the image to ensure that the image is usable (Balamurugan et al., 2015).

Step 4: Feature Extraction

The normalized 2 dimensional image of the iris is converted into a 1 dimensional signal. These signals are used

to entwine with 1 dimensional Gabor wavelets. Once this has been done, an individual shuffling feature vector is fused with it. The shuffling feature will then concatenate the shuffled vectors to result with two vectors. These vectors will then be merged together (Balamurugan et al., 2015).

Step 5: Matching

Matching is the part of the biometric key generation for the iris. The generation of the key is from a multi modal template. The key is generated from this matching process (Balamurugan et al., 2015).

In this iris feature extraction, applying the transformation parameter with the iris data generates both the key and the verification string. As the iris itself contains a very low false match rate, the key generated and the verification string provides a very unique data that is only coded to the individual. Thus, by extracting the verification string, the individual's biometric data can be kept secure. The individual's iris acts as the private key while the verification string acts similarly to a public key in cryptography. Therefore, whenever an unauthorised user tries to access the individual's secret files, they are unable to do so as they do not have the private key, being the iris of the individual.

However, there a several flaws to this key generation process. As the biometric key generation relies on solely the user's iris, should an unauthorised intruder scan their biometric iris, the intruder will be able to gain access to the system. Therefore, it is necessary for an extra set of authentication to strengthen the biometric security. These extra security measures will be further discussed in the method that combines keys from iris with public key cryptosystems and cancellable biometric features.

Biometric Key Binding with Iris

Key Binding

General definition

Key binding is an approach to obtain keys combining biometric with cryptography. The main difference between key binding and key generation approach is how the key is acquired. In the key generation method, the key is directly extracted from biometric data. However, in the key binding method, the fundamental idea is to combine the enrolment biometric data with a random key. Therefore, the key generated later is binding with a random key instead of just achieved from the original biometric data (Kanade et al., 2012).

Generally, in this key binding system, there are two stages as enrolment and verification. The idea is, at the part of enrolment, the system obtains enrolment biometric data so that the biometric template can be combined with a random key and then transformed into the database. Afterwards, at the verification part, the system captures fresh biometric data for verification. Then the biometric data transformed and compared with the template (Kanade et al., 2012).

Fuzzy vault based on iris images

More specific, the method of biometric key binding on iris images based on Fuzzy Vault scheme (Juels & Sudan, 2006) is proposed recently.

As the same function as enrolment stage mentioned above, the stage is locking the vault in this specific method. Locking the vault stage needs two input factors that are a cryptographic key (S) and iris data (I). And as the result, the fuzzy vault (V) is created and constituted with iris data codes(I), a cryptographic key (S) and random chaff point set (C). In the input factors, the key (S) is a 128-bits AES cryptographic key which is used to construct the polynomial, and the iris data codes(I) is generated and extracted by the iris image of each user. In the output result, the vault(V) is the product that can be stored in the devices, such as smartcards, storage devices and

servers as shown in Figure 3. Cryptographic key(S) was divided into sixteen 8-bits segments and used as the polynomial(P). The genuine set (G) was formed by the template iris codes(I) and the polynomial(P). The set chaff point set(C) is made by a random generator, which plays a crucial role. The chaff point set(C) will XOR with the genuine set(G) in order to protect the genuine set(G) which is very significant step. Another step is to convert the template iris codes(I) into a set(R) using the Reed–Solomon Encoding. With the three sets (G,C,R), the vault(V) can be created (Lee, Bae, Lee, Park, & Kim, 2007).

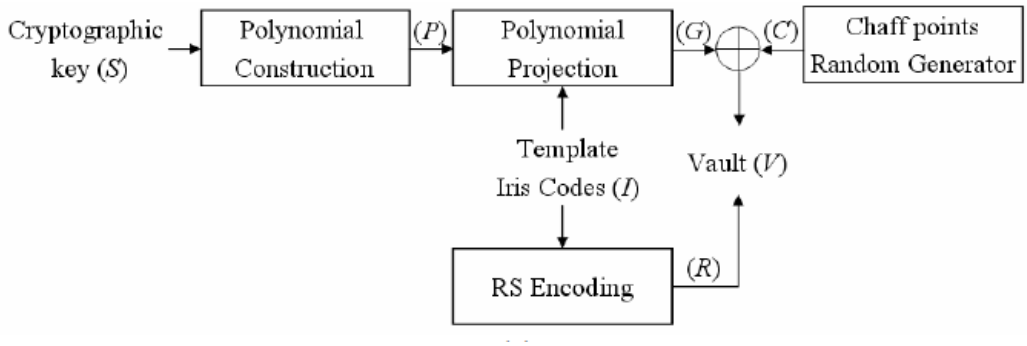

Fig 3. *Fuzzy vault system based on iris data: locking the vault. Adapted from (Lee et al., 2007)*

Act as the verification part of the concept of key binding, unlocking the vault is the part of this method to achieved the recovered key(S*). This procedure needs two input aspects that are the query iris codes(Q) and the vault(V). As indicated in Figure 1, the vault(V) is generated and can be stored in the devices and the query iris codes(Q) is extracted from the iris images of users. As the details, the query iris codes(Q) can product set(R) through the Reed–Solomon Decoding. With the vault(V) is known, it is not difficult to find out the set(G*) with the genuine points identification. As the conversion of the locking stage, the recovered key(S*) can be obtained. Finally, the recovered key(S*) can be compared with the original key stored in the database for verification as shown in Figure 4 (Lee et al., 2007).

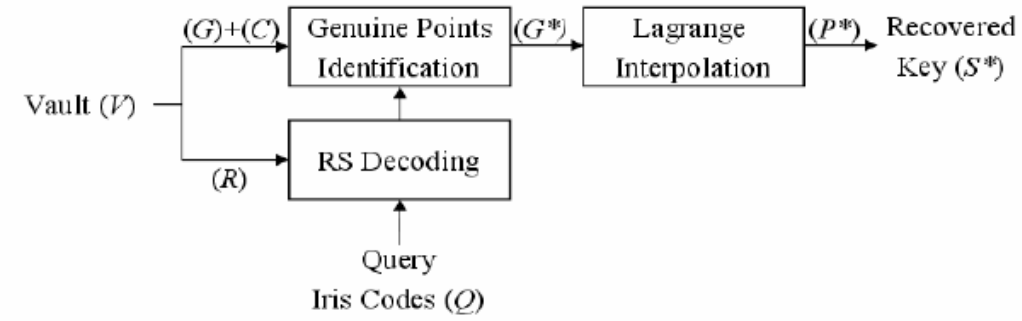

Fig 4. *Fuzzy vault system based on iris data: unlocking the vault. Adapted from (Lee et al., 2007)*

With the processes of locking and unlocking the vault, it achieves the purpose of securing the biometric data from been compromised.

Evaluate the Security

In a biometric system, there are several potential and vulnerable security holes that can be used by the attackers to attack the systems.

a) Unlike the traditional keys, the biometric features are inherent in single user that cannot be changed. The stolen original biometric template cannot be revoked or updated. So the system could collapse when the templates are compromised or missing (Lee et al., 2007).

b) The original biometric template contains critical personal information that you cannot change easily, for instance people cannot change their iris, fingerprint and palm prints. The loss of data would cause a serious threat to users' privacy and the influence is permanent (Lee et al., 2007).

c) The key diversity is also a serious problem. The biometric templates of one user may be stored and shared in many databases with more and more biometric systems appearing in our daily life, such like a user cannot have several iris biometric data. The significant information leaked may be used to match cross-database by offenders (Lee et al., 2007).

d) In some extend, the biometric data are not very secret. People leave fingerprints when touching anything, and the iris images also can be photographed by others. With the techniques are becoming more and more powerful, even public people could extract the information from the biometric template in daily life, and fabricate the user biometric features (Lee et al., 2007).

Therefore, to overcome these problems, it is crucial to provide an effective mechanism to protect the biometric templates. In crypto-biometric system, keys and templates are combined together and stored in the database. So that the attackers cannot get the keys without the original biometric templates, and that makes both the keys and biometric templates secure (Lee et al., 2007).

In this Fuzzy Vault scheme, the design based on two factors: a biometric data and a 128-bits AES cryptographic key. In the scenario that only one factor is compromised, such as the biometric data was leaked, the other key is still unknown by the attacker. These two input aspects are completely independent, so that it is unlikely for the attackers to get both two independent input factors. In the experimental results, the two fundamental statics are False Rejection Rate (FRR) and the False Acceptance Rate (FAR). The FRR is the false rate when a user trying to use his iris and user's vault, but the system reject his request. The FAR is the rate that the system is incorrectly accept an unauthorised person using the wrong iris image or the vault. As mentioned in the report, the FAR is considered more important than FRR, in case of the system is meant to be used for banking service etc. Therefore, when the FAR rate was set to 0%, the FFR is 0.775% as shown in Figure 5 (Lee et al., 2007).

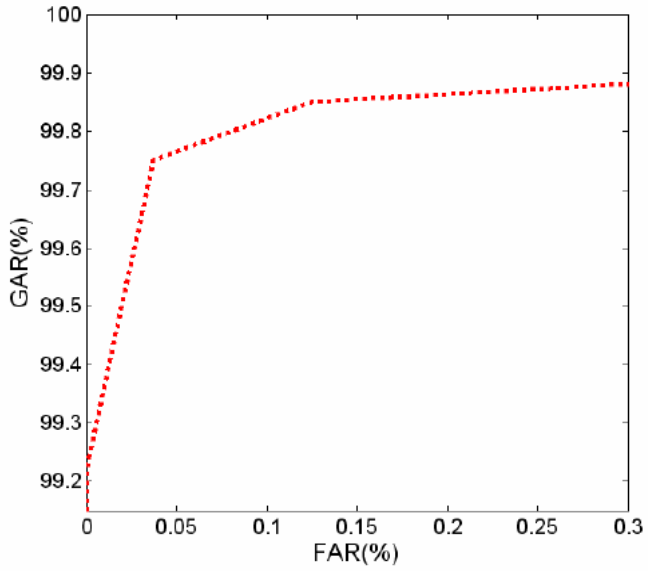

Fig 5. *ROC curves of the proposed Fuzzy Vault system. Adapted from (Lee et al., 2007)*

- Scenario A: the attacker has the storage device that contains user's vault information and tries to use many irises templates to attack the system. In this case, the possibility to success fully decrypt the message is the FAR rate, which is not indicated clearly in the report. However, it is undoubted that attacker need to try thousands of different iris images for brute force attack. That is unlikely to get so many iris images in a short time; furthermore, the system may have a limited count for trying in a certain time (Lee et al., 2007).
- Scenario B: the attacker gets user's iris image and tries to use every possibility of the vault. The cryptographic key(S) is a 128-bits key, so it has $\mathbf{2}^{128}$ possibility. Apparently, this is also impossible for attacker to brute force (Lee et al., 2007).
- Scenario C: the attacker somehow obtain the iris template and the cryptographic key(S). However, the vault(V) is generated by the cryptographic key(S) and the Chaff point set(C) duo to the algorithm and transformation, so the possibility of success is still $\mathbf{2}^{128}$ (Lee et al., 2007).

Overall, the security analysis confirms that the system's security level is high enough to resist variety kinds of attacks.

How the Method Overcome the Difficulties that Arises in Iris

Difficulties

As all kinds of pattern recognition, the fundamental point is to distinguish the problem between the inter-class and intra-class variability. The iris has its great advantage that iris of different person has huge differences from each other; in the meantime the iris itself is well protected and stable all over time (Daugman, 2004). However, there are still some difficulties. Essentially, iris recognition is based on the pattern-recognition to images of the irises. In some cases, duo to pupil dilation effects, it can be varying size that could reduce the performance of iris recognition (Hollingsworth, Bowyer, & Flynn, 2008). Also, there are researches claim wearing lenses will not affect the system (Ali & Hassanien, 2003). But a recent study claim there would be negatively impact the performance of systems (Baker, Hentz, Bowyer, & Flynn, 2009). Overall, all kind of changes to either irises or images of iris will affect reliability, stability and performance of iris recognition. Therefore, the recognition system should be flexible enough to accommodate these problems.

Corresponding solutions

As we can see, error-tolerant cryptographic algorithms are so necessary for this scenario, because the recognition system depends on human factors that are not always stable and accuracy over the time. In this Fuzzy Vault scheme, a pattern clustering technique is used in order to reduce the variations between the iris templates and the fresh input iris data. An approach of generating a set of iris codes from the input iris image which is an unordered set is a method to increase the flexibility and accurate of the recognition system. In details, multiple iris feature vectors were obtained from multiple iris image blocks. The iris extraction process takes several steps, the first step is to localize the iris regions and translate into a polar coordinate. Then iris features invariant is acquired which can be translated and rotated. The second step is to choose two iris regions that can be clearly analysed, and divided into sixteen iris image sub-regions that can be extracted for iris features using algorithm. Finally, to generate the iris codes, a random integer of a finite field is assigned to prototypes of each cluster. To compare the final generated iris code with the data stored in the database, there is a threshold was set in the system. It means it does not need the unlocking should be exactly same as the one locking in the database, so in this way it presents a way of error tolerant. It cannot be unlock by the differing substantially, but can be open with the set that overlaps largely (Lee et al., 2007).

Cancellable Biometrics

An advantage of a simple user string password compared to biometrics is that a user string password can always be reissued should there be a compromise in the user's account. According to Rathgeb & Uhl (2011), biometric characteristics that are stored in a database are unable to be changed as it contains the users biometric templates. As an individual only has two irises, should their iris biometric data be stolen, they will have run out of alternatives (Zuo, Ratha, & Connell, 2008). This poses security risks should a biometric template containing the user's biometric data be stolen or accessed into. Therefore, in order to ensure the security of biometric cryptography, a cancellable feature is adopted to protect the true iris pattern of the individual. A cancellable biometric feature acts similarly to a password changer to ensure it is kept unique and highly secure. Cancellable Biometrics will repeatedly distort the biometric features over time in order to keep the user-specific data secure and deter hacking (Kanade et al., 2012; Rathgeb & Uhl, 2011). In order to effectively use the cancellable biometric system, a shuffling feature is adopted. The shuffling feature will generate a random shuffling key to randomize the biometric feature codes. In the case where a stored biometric data is compromised, it can be cancelled, and a new biometric template can be generated using the shuffling key (Daugman, 2004).

Hence, every time an individual logs onto the system using their iris, the biometric template verifies their authenticity with the biometric template in store. The biometric template for that user is intentionally distorted when an unauthorised user tries to access the system. Therefore, this generates the two requirements in cryptography for cancellable biometrics that are irreversibility and unlinkability. Irreversibility is the process where it is very difficult or near impossible to reconstruct the biometric template but easy to generate the protected biometric template (Rathgeb & Uhl, 2011). Unlinkability is when different versions of the protected biometric template can be created using the same biometric data, and these protected templates do not cross match each other. Hence, this will render the biometric system to be secure for authorised users only.

In addition, for cancellable biometric to be secure, there are four objectives that must be followed; diversity, reusability/revocability, non-invertibility and performance (Jin & Hui, 2010). Diversity is ensuring that no similar cancellable feature is used across various applications, which will then require a large number of protected templates from the same biometric feature. Reusability/revocability suggest that the biometric data can be revoked and reissued should be there a compromise in the system. Non-invertibility suggests that it should be computationally difficult to recover the original biometric data. Performance is to ensure that the cancellable feature does not weaken or make the recognition performance of the system to become less secure. These four features have to be considered in order to implement a securely effective and usable cancellable biometric system.

An application of the cancellable biometric feature in the iris system can be whenever an individual first enrols into the system using their iris as the biometrics. After the iris is scanned in, the cancellable feature works by distorting the scanned data of their iris by introducing a biometric salting function to generate the cryptography key and verification string similar to the key generation technique. Once the individual has been enrolled into the system, he/she can then log onto the system. The cancellable feature will take effect every time the user logs on to the system and it will generate a new cryptography key and a verification string. Therefore, the more times the user logs onto the system, the more secure it will become as the cancellable features constantly distorts the previous log in session biometric template to ensure that it will be more accurate to the user's specific iris every time he/she log on.

A Method that Combines Keys from IRIS with Public-Key Cryptosystem

In public-key cryptosystem, client and server are the two parties that have their own pairs of private and public keys. The client encrypts a message with the server's public key which can be acquired by everyone, and the

message can only be decrypted with the server's own secret private key. Therefore, the server is the only one can get its private key and decrypt the message. The advantage is that the asymmetric cryptosystems do not need additional key management techniques and secure channels to pass the public keys.

To ensure the system which combining the public-key cryptosystem with biometric keys could share the keys securely, some assumptions be arose for the protocol. First of all, the communication channel between client and server may not be secure, so that information being transferred can be compromised. Furthermore, the server and client does not trust each other, therefore, the client will not pass the authentication (biometric data, password, etc.) directly to the server. Also, the server will not share the information with the client. To overcome this problem, incorporating the asymmetric RSA cryptosystem with the biometric keys generated by iris could utilize the advantages of biometrics as well as the asymmetric cryptosystems.

Clients in the system need to have their own pair of public-private key that generated by their own biometric features. In this case, the key could generated by their iris images using the method mentioned above (The Fuzzy Vault). In the process of locking and unlocking the vault, the client's iris data code that is a secret could be their private key, and the vault which constituted by iris data codes, a cryptographic key and random chaff point set can be the public key.

However, there are still problems. In the RSA cryptosystem, the length public key indicates the strength of the encryption, that the shorter the public key is; the easier it is for an attacker to brute-force. The vault that assigning 16 coefficients to is 128-bit key, and the asymmetric RSA cryptosystem requires the minimum public and private key size to be 1024-bit. So in this case, the security will not reach a regular level unless the key is extended from 128-bit to 1024-bit (Lenstra & Verheul, 2001).

Also, the Fuzzy Vault scheme has a drawback that when the client encrypts the vault with the receiver's public key and transmit to the receiver. The receiver is also able to decrypt the message by its private key in order to generate the vault. Therefore, the receiver can pretend to be the client. To solve this situation, the RSA cryptosystem could add extra information to the encrypt message. After that, the receiver still can verify the new message but it would not be able to recreate a fake vault (Nagar & Chaudhury, 2006). The cryptosystem consists of encryption modules between server and users, and each RSA module has its protocol. The system has filed n, encryption key e and decryption key d.

The following is the complete steps:

1. After the iris code is extracted from the iris image and the vault is assembled through the phase locking the vault (Nagar & Chaudhury, 2006).
2. The message is separated into several parts and encrypted using the encryption key e in the RSA cryptosystem (Nagar & Chaudhury, 2006).
3. Random digits are appended to the decryption key d, which is from the Fuzzy Vault (Nagar & Chaudhury, 2006).
4. The Fuzzy Vault that along with d is created then encrypted using the module encryption key and can be sent to the receiver (Nagar & Chaudhury, 2006).
5. The receiver has the fuzzy vault-unlocking key, and then gets the message. After that the receiver decrypts the vault by the decryption key d (Nagar & Chaudhury, 2006).
6. The receiver could use the module decryption key to confirm that the message was came from a legitimate user (Nagar & Chaudhury, 2006).

Conclusion

This report has analysed the Biometric Cryptography of the Iris mainly for key generation, key binding, cancellable biometrics, and combing keys from iris with public key cryptosystems. The basic biometric key generation technique can be broken down into enrolment phase and verification phase. The enrolment phase scans in the user data and extracts a verification string to be compared with the verification phase when a legitimate user wants to sign in. This basic type of biometric cryptography has been proven to not be secure enough as an unauthorised user can still break into the system. Therefore, the key binding technique explains further on how the security of the biometric iris can be improved through the use of a fuzzy vault system where there is an added security measure whenever a legitimate user wants to sign in. The fuzzy vault system incorporates the added security through the use of an extra verification token such as a card. This will allow the legitimate user to ensure that there is an added token to be used and their iris alone is not enough to sign into the system. This brings us to cancellable biometrics and combining keys from iris with public key cryptosystem. Cancellable biometrics is a further security measure for biometric iris cryptosystems. It is used to ensure the security of the legitimate biometric user by distorting the biometric template of the legitimate user when the system has been compromised. This will protect the legitimate user's biometric template as well as deter unauthorized users to access the template. This will bring us to combining keys from iris with public key cryptosystems. By using a public and private key similar to traditional cryptography techniques, the system can be furthered securitized. The public key is generated through the use of the server's public key. The message can only be decoded by using the private key that is generated through combining the user's iris template with the server's generated key. The key generated in the process will therefore be unable to be broken through cryptanalytic attacks. Therefore, these methods discussed in this report will ensure biometric iris cryptography can be a secure and efficient way of cryptography.

References

Ali, J. M., & Hassanien, A. E. (2003). An iris recognition system to enhance e-security environment based on wavelet theory. *AMO-Advanced Modeling and Optimization, 5*(2), 93-104.

Baker, S. E., Hentz, A., Bowyer, K. W., & Flynn, P. J. (2009). *Contact lenses: Handle with care for iris recognition.* Paper presented at the Biometrics: Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on.

Balamurugan, G., Jayarraman, K. B., Arulalan, V., & Lokesh, V. (2015). Multimodal BIometric Key Generation for Cryptographic Security using Face and Iris. *AENSI Journals, 9(6)*, 525-530. Retrieved from http://www.academia.edu/11383834/Multimodal_Biometric_Key_Generation_for_Cryptographic_Security_using_Face_and_Iris

Ballard, L., Kamara, S., & Reiter, M. K. (2008). *The Practical Subtleties of Biometric Key Generation.* Paper presented at the USENIX Security Symposium.

Daugman, J. (2004). How iris recognition works. *Circuits and Systems for Video Technology, IEEE Transactions on, 14*(1), 21-30.

Hashiyada, M. (2004). Development of biometric DNA ink for authentication security. *The Tohoku journal of experimental medicine, 204*(2), 109-117.

Hollingsworth, K. P., Bowyer, K. W., & Flynn, P. J. (2008). *The importance of small pupils: a study of how pupil dilation affects iris biometrics.* Paper presented at the Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on.

Jin, A. T. B., & Hui, L. M. (2010). Cancelable biometrics. *Scholarpedia, 5*(1), 9201. Retrieved from http://www.scholarpedia.org/article/Cancelable_biometrics

Juels, A., & Sudan, M. (2006). A fuzzy vault scheme. *Designs, Codes and Cryptography, 38*(2), 237-257.

Kanade, S. G., Petrovska-Delacrétaz, D., & Dorizzi, B. (2012). Enhancing information security and privacy by combining biometrics with cryptography. *Synthesis Lectures on Information Security, Privacy, and Trust, 3*(1), 1-140.

Lee, Y. J., Bae, K., Lee, S. J., Park, K. R., & Kim, J. (2007). Biometric key binding: Fuzzy vault based on iris images *Advances in Biometrics* (pp. 800-808): Springer.

Lee, Y. J., Park, K. R., Lee, S. J., Bae, K., & Kim, J. (2008). A new method for generating an invariant iris private key based on the fuzzy vault system. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on, 38*(5), 1302-1313. Retrieved from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4595625

Lenstra, A. K., & Verheul, E. R. (2001). Selecting cryptographic key sizes. *Journal of cryptology, 14*(4), 255-293.

Nagar, A., & Chaudhury, S. (2006). *Biometrics based asymmetric cryptosystem design using modified fuzzy vault scheme.* Paper presented at the Pattern Recognition, 2006. ICPR 2006. 18th International Conference on.

Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security, 2011*(1), 1-25.

Zuo, J., Ratha, N. K., & Connell, J. H. (2008). *Cancelable iris biometric.* Paper presented at the Pattern Recognition, 2008. ICPR 2008. 19th International Conference on.

Appendix A: Practical Part – Classification with OSIRIS and Result Analysis

For the practical exercise part, the OSIRIS reference system is required to be used in order to classify and assess 14 iris image and analyze the final result of the comparisons. The OSIRIS reference system is used to perform normalization, segmentation, and encoding at once. After setting up and configure the system correctly, a user can generate a result of computing 14 iris images. After getting the results of iris codes, the system would be reconfigured to check the similarities and the differences of the iris images. The hamming distance would be performed as an indicator to verify the iris codes belong to the same person, which is called the intra-person distance, or different persons which is called inter-person distance.

Task A: Intra-Person Distances

Output data gathering from intra-person distances using the OSIRIS reference system:

Table 1. *Intra-person distances*

Image1	Image2	Distance
01L0001.bmp	01L0002.bmp	0.190896
01L0001.bmp	01L0003.bmp	0.202643
01L0001.bmp	01L0004.bmp	0.204277
01L0001.bmp	01L0005.bmp	0.196769
01L0002.bmp	01L0003.bmp	0.0634921
01L0002.bmp	01L0004.bmp	0.090708
01L0002.bmp	01L0005.bmp	0.0646552
01L0003.bmp	01L0004.bmp	0.0998532

01L0003.bmp	01L0005.bmp	0.0753623
01L0004.bmp	01L0005.bmp	0.103245
	min	0.0634921
	max	0.204277
	mean	0.12919008
	No. Comparisons	10

- When configuring the script code for the intra-person distances in order to generate the score matching for the intra-person, the result will be produced as scores in the score_matching_intra.txt file. the ten comparisons are required to exhaustively compare all the intra-images and can be calculated using the following formula:

$$\frac{n(n-1)}{2}$$

where the n is the number of the intra-person images.

then the calculation will be:

$$\frac{5(5-1)}{2} = \frac{5*4}{2} = 10$$

- Due to the multi-factors that can affect the final result of the iris code, the values of hamming distance could not be the same as shown in Figure 6. The factors that could affect the iris code are the size of the pupil within the iris, the optical of the iris in the images, the iris orientation, the location of the iris within the image, the camera position, and camera angles (Daugman, 2004).

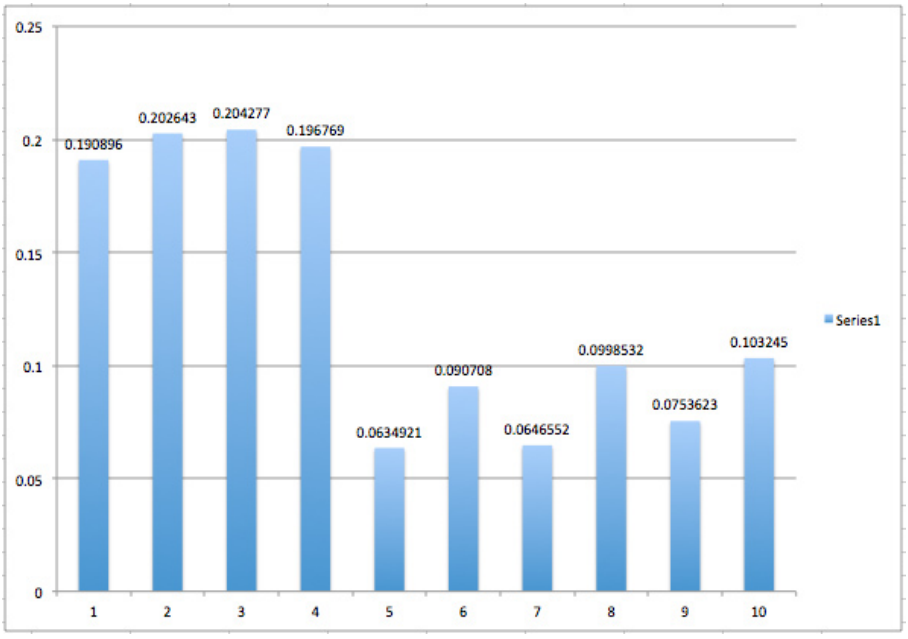

Fig 6. *Intra-person distances*

- Based on the results of matching score that generated by the OSIRIS reference system for the intra-person distances the maximum, minimum, and mean hamming distances are 0.204277, 0.0634921 and 0.12919008 respectively.

In order to calculate the mean, we need to sum the values of hamming distances and divide the result by the number of hamming distances.

Task B: Inter-person distances

Output data gathering from inter-person distances using the OSIRIS reference system is shown in Table 2:

Table2. *Inter-person distances*

Image1	Image2	Distance
01L0001.bmp	02L0001.bmp	0.471599
01L0001.bmp	03L0001.bmp	0.463704
01L0001.bmp	04L0001.bmp	0.440252
01L0001.bmp	05L0001.bmp	0.482906
01L0001.bmp	06L0001.bmp	0.453704
01L0001.bmp	07L0001.bmp	0.438547
01L0001.bmp	08L0001.bmp	0.483844
01L0001.bmp	09L0001.bmp	0.469109
01L0001.bmp	10L0001.bmp	0.450081
01L0002.bmp	02L0001.bmp	0.464286
01L0002.bmp	03L0001.bmp	0.462054
01L0002.bmp	04L0001.bmp	0.446288
01L0002.bmp	05L0001.bmp	0.470672
01L0002.bmp	06L0001.bmp	0.432761
01L0002.bmp	07L0001.bmp	0.458101
01L0002.bmp	08L0001.bmp	0.480442
01L0002.bmp	09L0001.bmp	0.431034
01L0002.bmp	10L0001.bmp	0.464744
01L0003.bmp	02L0001.bmp	0.474589
01L0003.bmp	03L0001.bmp	0.462222
01L0003.bmp	04L0001.bmp	0.453968
01L0003.bmp	05L0001.bmp	0.482117
01L0003.bmp	06L0001.bmp	0.439914
01L0003.bmp	07L0001.bmp	0.451852
01L0003.bmp	08L0001.bmp	0.475214
01L0003.bmp	09L0001.bmp	0.430316
01L0003.bmp	10L0001.bmp	0.459135

01L0004.bmp	02L0001.bmp	0.467424
01L0004.bmp	03L0001.bmp	0.462054
01L0004.bmp	04L0001.bmp	0.438301
01L0004.bmp	05L0001.bmp	0.476812
01L0004.bmp	06L0001.bmp	0.442029
01L0004.bmp	07L0001.bmp	0.439815
01L0004.bmp	08L0001.bmp	0.469072
01L0004.bmp	09L0001.bmp	0.440789
01L0004.bmp	10L0001.bmp	0.460128
01L0005.bmp	02L0001.bmp	0.467862
01L0005.bmp	03L0001.bmp	0.457589
01L0005.bmp	04L0001.bmp	0.444444
01L0005.bmp	05L0001.bmp	0.474856
01L0005.bmp	06L0001.bmp	0.44181
01L0005.bmp	07L0001.bmp	0.450652
01L0005.bmp	08L0001.bmp	0.470085
01L0005.bmp	09L0001.bmp	0.4329
01L0005.bmp	10L0001.bmp	0.463141
	min:	0.430316
	max:	0.483844
	mean:	0.45762707
	No. Comparisons:	45

- For the inter-person hamming distances, the required number of comparisons that exhaustively compare all inter-person images is 45. This number can be calculated using the following mathematical formula:

$$\sum_{i=1}^{n} m_i = m_1 + m_2 + \ldots + m_n$$
$$= 9 + 9 + 9 + 9 + 9 = 45$$

Where n=5 is the number of intra-person images and mi=9 for all i, is the number of inter-person images.

- Based on the results of matching score for the inter-person distances that are generated by the OSIRIS reference system, the maximum, minimum, and mean hamming distances are 0.483844, 0.430316, and 0.45762707 respectively.
- When comparing between the results of the intra-person distance and inter-person distance, user can notice that in Figure 7 the inter-person distances are grater than the distances of the intra-person. The hamming distances results should be between 0 and 1 in iris recognition in iris recognition and the inter-person distances is greater than the intra-person distances as described in (Daugman 2004) no matter the decision

environment is under ideal condition or not. The OSIRIS reference system is using HD to calculate the iris chosen points. Because the comparisons in the inter-person distances comparing two different person's iris, the results must be greater than the intra-person distance this is because there are not many similarities between two person. The more similarities results to low values of the comparisons.

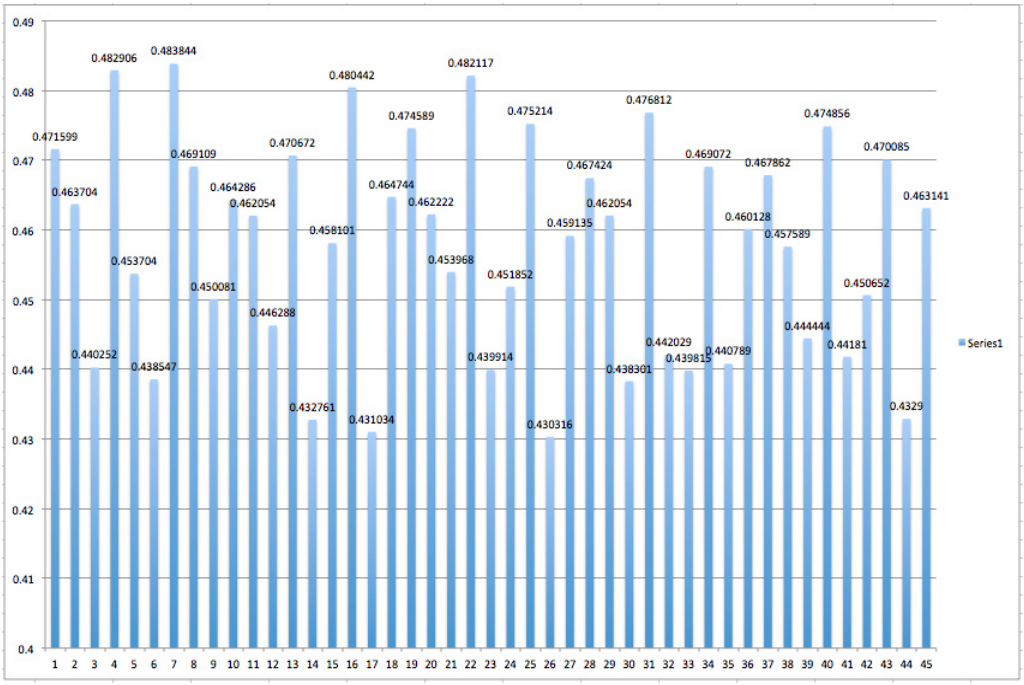

Fig 7. *Inter-person distances*

- We could say that the OSIRIS reference system achieved a good separation between the intra-person and inter-person distances because the results of the comparisons show that the inter-person distance is much greater that the intra-person distance. When comparing the two values of the inter-person and intra-person, the higher values of the inter-person can be noticed. For example, the maximum distance in inter-person is 0.48 while the maximum distance in intra-person is 0.20, which means that it more than twice the intra-person distance. So, the OSIRIS reference system is able to achieve a good separation between the inter-person and intra-person.

Part C:

We would suggest the decision threshold is 0.29340858. The number that we suggested can be calculated as the average of intra-person mean distance and inter-person mean distance. This number has been chosen based on the False Acceptance Rate (FAR), which is the most important factor that needs to be minimised as possible.

Table 3. *Mean values and Suggested threshold*

Intra-person mean Distance	Suggested threshold	Inter-person mean Distance
0.12919008	0.29340858	0.45762707

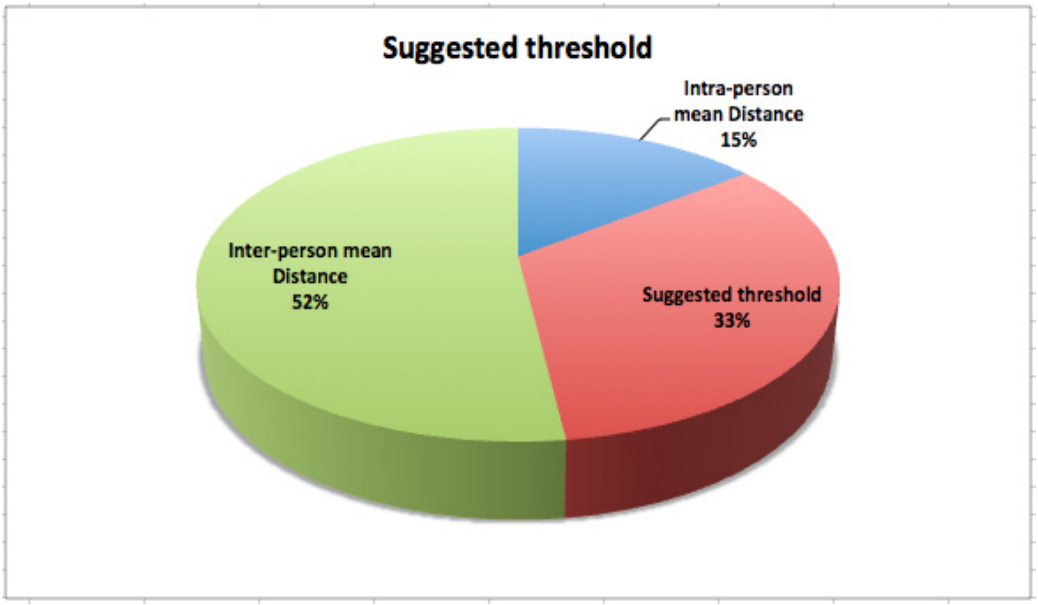

Fig 8. *Suggested threshold*

Citation: **Abdullah Alsulami, Darren Teo, Weiyi He,** *"Combining Iris Biometric System and Cryptography Provide a Strong Security Authentication". American Research Journal of Computer Science and Information Technology, Volume 1; pp:1-17*