Journal of Scientific Research and Development 2 (14): 38-46, 2015
Available online at www.jsrad.org
ISSN 1115-7569

Multibiometric systems and template security survey

Emad Taha Khalaf*, Norrozila Sulaiman

Faculty of Computer Systems & Software Engineering, University Malaysia Pahang, 26300, Kuantan, Malaysia

Abstract: multimodal biometric systems are capable of utilizing, more than one physiological or behavioral characteristic for enrolment either in verification or identification mode, It is generally believed that several biometric sources usually compensate for the weaknesses of single biometric fusion techniques. The features that extracted from the biometric samples considered a critical part of biometric system which is called biometric template it is one of the most crucial issues in designing a secure system.

Key words: Uni-Biometric; Multi-Biometric; Template security

1. Introduction

Biometric field has taken a huge interest by global industry with protect and safeguard information as an everlasting necessity, Biometric is uses to identify authorized person based on specific physiological or behavioral features (Rajni, 2014). Most biometric systems that are currently in operation usually utilize a single biometric trait which called unibiometric systems. Other systems utilize two or more biometrics traits which called Mutlibiometrics systems (Aly et al., 2013) which utilize, or are capable of utilizing, more than one physiological or behavioral characteristic for enrolment either in verification or identification mode. It is generally believed that by integrating various biometric traits into one single unit, the limitations of unibiomatic systems can be alleviate (Ross et al., 2006). Given that several biometric sources usually compensate for the weaknesses of single biometric fusion techniques has dealt primarily with the fusion at the score matching level. A number of anatomical and behavioral body traits can be used for biometric recognition (see Fig. 1). It can be divide into two types as below (Shoa'a and AbdulAziz, 2011):

1) Physiological attributes: These attributes identify the person on the basis of anatomical traits such as face, fingerprint, iris, palm print, DNA, hand geometry and ear shape. Biological features are strong durable “link” between the person and identity and these qualities cannot be easily lost, forgotten, shared, or forged. Biological systems require the user to be present at the time authentication and it can also be used to deter users from making false claims disclaimer. For these reasons, adopting of biometric systems is increased in a number of government and civilian applications.

2) Behavioral attributes: based on the analysis of the behavior of an individual while he is performing a specific task, example gait, signature, keystroke dynamics and voice (Griaule Biometrics, 2012). Certain characteristics of a person’s voice such as pitch, tenor and nasality are due to physical factors like vocal tract shape, and other characteristics such as word or phoneme pronunciation (e. g., dialect), use of characteristic words or phrases and conversational styles are mostly learned (Shoa'a and AbdulAziz, 2011). There are other characteristics called "Ancillary characteristics" such as gender, ethnicity, age, eye color, skin color, scars and tattoos also provide some information about the identity of a person. However, since these ancillary attributes do not provide sufficient evidence to precisely determine the identity, they are usually referred to as soft biometric characteristic (James, 2011).

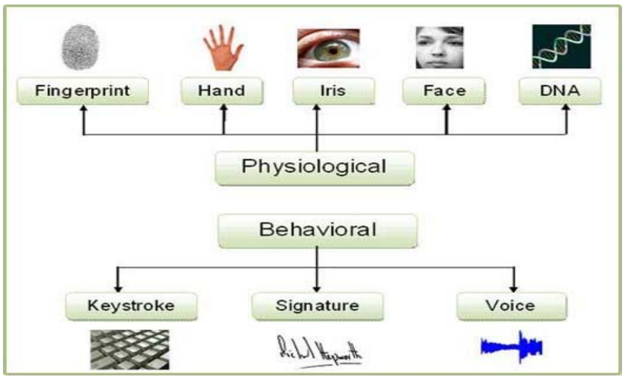

Fig. 2: Biometrics System Type

Salient features are extracted from biometrics using some feature transformation technique and get converted into digital form. This digital information is stored in the database which is known as Biometric Template. Later the template is used during authentication purpose, compromised

[*] Corresponding Author.

biometric templates are unlike passwords and tokens they cannot be revoked and reissued this led to become biometric template security is an important issue and protecting the template is a challenging task due to intra user variability in the acquired biometric traits, based on knowledge of the biometric characteristics (Malhotra and Dr.Kant, 2013).

2. History of biometrics

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). Among all the biometric techniques, fingerprint-based identification is the oldest method it has been used by the ancient Assyrians, Babylonians, Japanese and Chinese for signing certificates. In ancient Babylon, fingerprints were used on clay tablets for business. The survey of handprints was the only way to distinguish an illiterate another because they could not write their own name. In the 1870s, an anthropologist and the receptionist Police in Paris, France, named Alphonse Bertillon tried the problem on the basis of his system to the assertion that the measurement of adult bone does not resolve to change after the age of twenty year old. The method was to identify people by. Measurements that the height of a person, arm length and the width of the head, the length of the individual fingers, the length of the forearm, etc. calipers He developed a method of multiple measurements of the body, which is named after him and is called Bertillon Ages. His system has been used worldwide by police, but it quickly disappeared when it was discovered that some people share the same measures in parts of the body (Miller, 1971). In the late 19th century, Francis Goldstein wrote a detailed study of fingerprints in which he presented a new classification system with prints of all ten fingers. After Galton calculations were 1 in 64 billion chances of two distinct impressions, even. Galton identified characteristics of fingerprints which are identified (minutiae) which (Goldstein et al., 1970) are essentially the same today, still in use. This classification of minutiae is often referred to as Galton details. Also in the 1890s, police in Bengal, India, under British policeman Edward Richard Henry started with fingerprints to identify criminals. As an Assistant Commissioner of the Metropolitan Police, Henry founded the first fingerprint files of the UK in London in 1901 (Chawki and Abdel Wahab, 2006). Some of the earliest work on face recognition system can be panorama of the 1960s at a company called Research in Palo Alto, California predicted. This type of research is then referred to as artificial intelligence, by Woody Bledsoe, was a pioneer in the field of automated reasoning. His method called "human face recognition and machine" using a technique known as feature extraction. In 1974 was a year of breakthrough for automated biometric data, such as hand geometry at the University of Georgia campus food service areas to get started. Both Stanford Research Institute at the National Physical Laboratory in the United States and Britain signed detection systems (Chawki and Abdel Wahab, 2006) started. In 1985, one of the first scanning systems of the retina to secure access to a Department of Defense facility at the Naval Postgraduate School was used. In the mid-1980s, the State of California had been fingerprinting as a requirement for all license applications. The first organization of the biometric industry, International Biometric Association (IBA), founded in 1986-1987.Iris recognition technology in the 1980s by John Daugman was developed at the University of Cambridge. Other new technologies in the production of commercially available include arcograph face and the face recognition system (Chawki and Abdel Wahab, 2006). 1987 River develop an algorithm obtained a patent for the human iris identification approach (NSTC, 2006) and in the same year was the recognition Sok Gek solution visual form of objects classified by hierarchical syntax extraction in which objects and then reduce the binary thin line image and distinguish chief Moving from a wide range of where moving objects in a family environment. (National center, 2005) In 1998, the International Biometric Industry Association (IBIA) in Washington, DC was founded to advance as a professional association of non-profit industry, common global interests of the biometric industry. The National Biometric Security Project (NBSP) was established in 2001 in response to the events of September 11, 2001, and the need to accelerate the development and deployment of biometric technologies. (National Biometric Security Project, 2008) In April 2002 Staff Paper Technology palm print and IAFIS skills to palm print identification services (IS) Advisory Council Subcommittee CJIS policy (PDB) has been submitted. The Joint Working Group then moved "for strong support for planning, costs and the development of an integrated latent print function with the palm of the CJIS Division of the FBI. This should be seen as an attempt on the same parallel lines passing IAFIS developed and integrated into the CJIS technical skills "as a result of these and other supporting evolving business needs of the prosecution, said the initiative Next Generation FBI IAFIS (NGI). An essential part of the NCI initiative is the development of the needs and the use of an integrated national Palm Print service. Show law enforcement authorities at least 30 percent of prints lifted the knife handles crime scenes, gun grips, steering wheels and windows - are palm, not your fingers. For this reason, detection and scanning latent palm become an area of increasing interest in the application of the law. National service Palm Print is based on improving the ability of law enforcement to provide a complete set of biometric data (George, 2005) exchange developed.

3. Related works

The Researchers have been working on systems to help protecting the privacy of humans. Many ideas were implemented such as the fingerprint, face, iris recognition, and voice; this is a review of some of the research that used different methods. (Duca et al., 1997) propose an algorithm based on Bayes theory in order to fuse individual experts opinions. The modalities used in their system are face and speech for each person involved. Experimental results show that fusion improves accuracy over the uni-biometric systems by reaching success rates of 99.5%. A multi-view face and gait recognition system was proposed by (Shakhnarovich et al., 2001) using an image-based visual hull. Image sequences captured from multiple cameras are passed to an unmodified face or gait recognition algorithm, the proposed algorithm shows an integrated face and gait recognition provides improved performance over a single modality of one of them alone. The researcher (Karthik, 2008) in his thesis fusion methodology based on the Neyman-Pearson theorem for combination of match scores provided by multiple biometric matchers, the likelihood ratio (LR) test used in the Neyman-Pearson theorem directly maximizes the genuine accept rate (GAR) at any desired false accept rate (FAR). (Park, 2009) proposed video-bases face recognition framework using 3D face modeling technique and show how it is used to compensate for age variations to improve face recognition performance. The aging modeling technique adapts view invariant 3D face models to the given 2D face aging database, an automatic facial mark detection method and a fusion scheme that combines the facial mark matching with a commercial face recognition matcher to improve the recognition performance. In 2010 (Emanuela, 2010) proposed a security perspective dependence to multimodal biometrics system to be protected against number of vulnerable points that may be attacked by a hacker who may choose to fake only a subset of them to improve the performance of the existing integration mechanisms in presence of degraded data and their security in presence of spoof attacks. (Youmaran, 2011) presented a face and iris images and that can be applied for low quality face and iris images recognition in a non-cooperative, the proposed algorithms can be used to detect the subject's face, locate the eyes, reduce iris noise, segment the iris, generate a template and then identify the subject through typical pattern matching algorithms. In 2012 (Almayyan, 2012) applied multi model biometrics system fusion Online signature and iris authentication techniques, which combined the feature-level and decision-level fusions, have improved the final authentication performance. Therefore, she has been proposed hybrid approach offers considerable improvements to the accuracy of multimodal biometrics. In 2013 (Malkhasyan, 2013) examines security problems of biometric based authentication. An authentication method is suggested, which is based on fingerprints with steganographic data protection in all stages of functioning. Suggested procedures of fingerprint based enrollment and authentication are also functionally described. In 2014 (Chin et al., 2014), proposed fuse multiple biometric modalities and to secure the fused templates using a hybrid template protection method by made out of a feature transformation technique known as Random Tiling and an equal-probable 2N discretization scheme. The former enables the revocability of the template and the latter converts the feature elements into binary representations according to the area under the genuine interval curve, in order to offer better privacy protection to the template. Many techniques have been proposed to keep the security of biometric data; one of the suggested techniques was by (Jain and Uludag, 2003) with two scenarios of hiding data, first one in a cover image not related to the template data, other scenario by using the fingerprint image to hiding the facial information. (Wang et al., 2010) (Pravin and Shubhangi, 2011) use DCT transformation method to hiding the iris code and the secret information after encrypting in random blocks of the coefficients. Another security system have been proposed by (Klimis et al., 2011) based on DWT transformation method to hides biometric signals in video objects over open network.

4. Biometric systems

The basic steps of any typical authentication biometric system comprise four steps Fig. 3:

4.1. Data requirement

Suitable user interface incorporating the biometric sensor or reader is needed to measure or record the raw biometric data of the user using any device such as (digital camera, sensor, scanner…. etc.) is the interface between the real world and the system, It in the form of raw biometric data to capture data about any part that need to be used to recognize the person. Data requirement is very important because the quality of raw biometrics depends on the characteristics of device which capture the images (Claus, 2011).

4.2. Feature extraction

Usually, the raw biometric data required is subjected to pre-processing operations before features are extracted from it; the feature extraction shown as third block in Fig. 2 refers to extract the features. This step is really important to choose which features to extract and how to do it. Feature extraction refers to the process of generating a compact but expressive digital representation of the underlying biometric trait, called a template which contains the data to glean only the salient information from the acquired biometric sample to form a new representation of the biometric trait, called the feature set. Ideally, the feature set should be unique for each person and also invariant with respect to changes in the different samples of the same biometric trait collected from the same person (extremely small intra-user variability). The feature set obtained during enrollment is stored in the system database as a template. It performs the necessary preprocessing: it has to remove artifacts from the data required, and make some process to enhance the input (e. g. removing some noise), to use some kind of normalization, rotate etc. (Claus, 2011; Anil, 2002).

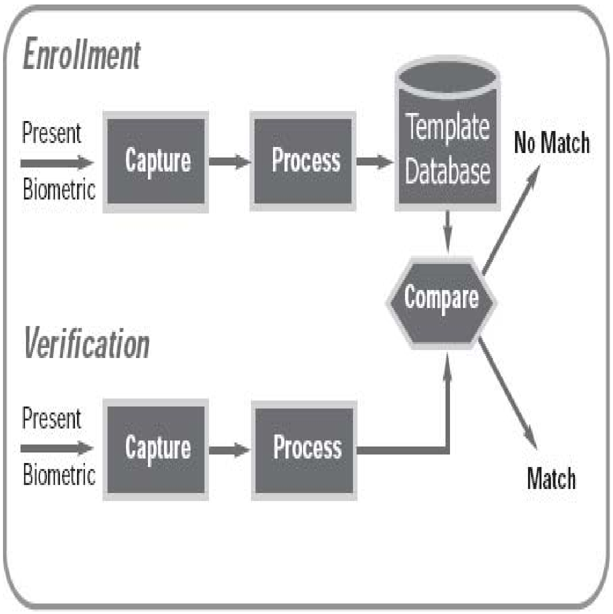

Fig. 2: Basic building blocks of a generic biometric system

4.3. Matching module

This step of a biometric recognition system is to compare the extracted feature set with a database of known features of the biometric application. Generate matching scores, which determines the large degree of similarity (dissimilarity) between the two features sets (Claus, 2011). Matching represents a similarity metrics which determine the accuracy performance of the system for a given population of identities; hence the election of appropriate similarity scheme and representation is critical.

5. Properties of biometrics

Biometric systems are widely implemented worldwide for boarder control, restricted access of privileged information, secured online banking systems, and social insurance programs and so on. Although, uni-biometric systems (biometric systems based on single source of evidence) are widely deployed and used, they have several limitations that hinder their reliability and make them less reliable in identification and authentication applications. Some of these limitations are outlined below (Ross et al., 2006):

Accuracy: Noisy sensor data, non-universality, inter-class similarity and lack of invariant representation.

Scalability: If the number of data samples, N, is large, identification becomes an issue.

Security and Privacy: Spoofing can take place in many traits such as fingerprint, signature and voice.

In response to these limitations, multibiometric systems have been recently introduced as an improved means for person's identification and recognition purposes. Such systems rely on multiple evidence rather than single biometric evidence (Ross et al., 2006). By integrating multiple biometric samples or multiple traits, more efficient and reliable systems can be devised. Information fusion has been proposed to achieve the integration of the multiple biometric traits at different stages of multibiometric systems (Snelick et al., 2005; Ulery et al., 2006). It should be noted that the resulting systems can be either be hybrid or simple systems depending on the type of information fusion strategy being adopted and applied. Fig. 3 shows the major differences between uni- and multibiometric systems. The integration of several biometric samples and/or traits is made possible only by the incorporation of the information fusion module which highlights the importance of the latter module in the successful development of multibiometric systems since uni-modal could be considered in an ensemble but without allowing possible an improved matching and recognition performance.

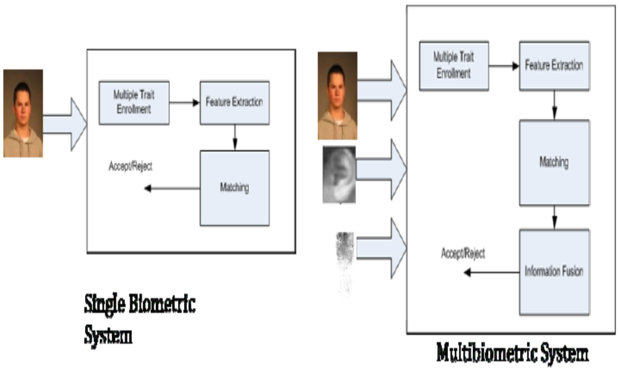

Fig. 3: Single Biometric vs. Multibiometric System

Multimodal biometric systems can be designed to operate in five different modes (Ross et al., 2006):

5.1. Multiple-sensor mode

In this mode, the raw biometric data is acquired from multiple sensors, processed and integrated to generate new data from which features can be extracted, Needless to notion the increased hardware, software and computational costs caused by such integration. However, the incorporation of sources from multiple sensors significantly improves the segmentation and registration procedures in addition to improving the matching accuracy (Ross et al., 2006).

5.2. Single-biometric multiple-representations mode

In these systems, the same biometric data is processed using multiple algorithms at the mapping and feature levels. For instance, a multiresolution algorithm based on texture analysis and a minutiae-based algorithm can operate on the same fingerprint image in order to extract diverse feature sets that would greatly improve the performance of the overall system. This mode is characterized by its cost efficiency since it does not require the use of multiple sensors. Furthermore, the user is not required to interact with multiple sensors thereby enhancing user convenience and comfort. It does require the introduction of new feature extractor and/or matcher modules which may increase the computational requirements of the system (Ross and Jain, 2003).

5.3. Single-biometric multiple-units mode

Multiple instances of the same biometric trait are considered in this mode. For example, the left and right irises of the same person are considered for fusion and further processing. Systems pertaining to this mode generally do not necessitate the introduction of new sensors nor do they entail the development of new feature extraction and matching algorithms and are, therefore, more cost efficient than those systems belonging to the previous mode. In some cases, a new sensor arrangement might be necessary in order to facilitate the simultaneous capture of the various units (Ross and Jain, 2003).

5.4. Single-biometric multiple- snapshots mode

In this mode, a single sensor is used to capture multiple snapshots of the same biometric trait. A mosaicking scheme may then be used to assemble the multiple impressions and create a composite image. One of the main issues in this mode is the determination of the number of samples or snapshots that have to be acquired from an individual. It is important to well capture the variability, as well as the typicality, of the individual's biometric data in the captured samples (Ross et al., 2006).

5.5. Multiple-biometrics mode

Multibiometric systems requiring more than one modal are classified under this mode. For instance, the iris and fingerprint of the same person can be used for the matching, identification and recognition purposes. Systems belonging to this mode are usually known as multimodal biometric systems (Group, 2014). Unlike the first four modes where multiple sources of information are derived from the same biometric trait, in the last mode, useful biometric information is derived from different biometric traits. However, fusion at the matching score level seems to be the logical choice as it is relatively easy to access and combine scores presented by the different modalities. Furthermore, incorporating the fusion process at earlier stages of the multibiometric system is more effective. In summary, the main advantages of multibiometric systems are outlined below (Ross et al., 2006):

* Improve accuracy. * Address the issue of non-universality problem. * Provide flexibility to the user. * Reduce the effect of noisy data. * Provide the capability to search a large database in computationally efficient manner. * Resistant to spoof attacks. * Fault tolerant systems.

Each of the above-mentioned features mitigates one or some of the limitations found in uni-biometric systems. Table 1, gives a comparative summary of the various biometric traits with respect to key factors such as universality, performance, acceptability and distinctiveness.

Table 1: Comparison of various biometric technologies (H=High, M=Medium, L=Low)

Biometrics	Universality	Uniqueness	Permanence	Collectability	performance	Acceptable	Circumvention
Face	H	L	H	H	L	H	L
Fingerprint	H	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke	L	L	L	M	L	M	M
Hand Vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear	M	M	H	M	M	H	M

6. Template protection technologies

Biometric Template Protection Schemes are classified into *Feature Transformation* and *Biometric Encryption*. Jain et al in (Jain et al., 2006) categorized the various biometric template protection techniques as:

6.1. Feature transformation

In Feature Transformation, a biometric template *(BT)* is transformed to *F (BT, X)* after a function *F* with a randomly generated key *X* is applied to it. Feature Transformation is further categorized into either *invertible* or *non-invertible* transform. In *invertible* transform, the key *X* can be used to recover the original biometric template *(BT)* while in *noninvertible* transform the key *X* is a one-way key that makes it hard to recover the original biometric template *(BT)* even if the key *X* is known as was pointed out by (Radha and Karthikeyan, 2010). Existing literature identify *bio-hashing* as an invertible transformation and *cancellable biometrics* as noninvertible transformation (Rathgeb and Uhl, 2011).

6.1.1. Cancellable biometrics

Unlike passwords, PINs and access codes, biometric templates can never be replaced with newer ones if they are compromised. To circumvent this challenge, cancellable biometrics were introduced such that biometric templates could be cancelled and replaced (Radha and Karthikeyan, 2011). Cancellable biometrics scheme is an intentional and systematic repeatable distortion of biometric template data with the purpose of protecting it under transformational-based biometric template security (Rathgeb and Uhl, 2011).

6.1.2. Bio-hashing

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 (Schmitt and Jordaan, 2013). This key or password needs to be securely stored and remembered by the user for subsequent authentication.

6.2. Biometric cryptosystems

In an earlier research, Jain et al in (Jain et al., 2006) subdivided biometric cryptosystems into *Key Generation* and *Key Binding.*

6.2.1. Key Generation

In Key Generation a biometric key is derived directly from biometric data (Blanton & Aliasgari, 2013). Under Key Generation we discuss secure sketches and fuzzy extractors.

4.2.1.1. Secure sketches and fuzzy extractors

Dodis et al. originated with *secure sketches* and *fuzzy extractors* in a preliminary version of their research work in year 2004 which was later published in (Dodis et al., 2008). They defined *Fuzzy Extractor* and *Secure Sketch* as follows;

i. *Fuzzy Extractor*: reliably extracts almost uniform randomness *R* from its input: The significance of fuzzy extraction is that it is error-tolerant in the sense that *R* will not change even if the input changes e.g. if another biometric template from the same finger is used, as long as it is almost similar to the original *R* implying *R* can be used in a cryptographic application as a *key*.

ii. *Secure Sketch*: produced public information about its input *w* that did not reveal *w* and yet allowed exact recovery of *w* given another value that is close to *w* which was an advantage that made it possible for it to be reliably used to reproduce error prone biometric inputs without incurring security risks inherent in storing them.

6.2.2. Key binding

It is where a secret key and the biometric template are monolithically bound within a cryptographic framework whilst it is computationally infeasible to decode the key or biometric template without prior knowledge of the user‟s biometric data (Schmitt and Jordaan, 2013).

6.2.2.1. Fuzzy vault

It is where secret information is encrypted and decrypted securely using a fuzzy unordered set of genuine points and haff points (Juels and Sudan, 2002). The limitations of a fuzzy vault scheme as listed by Hooda & Gupta in (Hooda and Gupta, 2013) are; i. Difficulty in revoking a compromised vault which is also prone to cross-matching of biometric templates across databases. ii. Easy for an attacker to stage attacks after statistically analyzing points in vault. iii. It is possible for an attacker to substitute his biometric features with that of the targeted biometric features thus beating vault authentication. iv. The other threat is that, if the original template of the genuine user is temporarily exposed, the attacker can glean the template during this exposure.

4.2.2.2. Fuzzy commitment

It is a biometric cryptosystem which is used to secure biometrics traits represented in binary vector (Jeny and Jangid, 2013). Jeny & Jangid added that, a fuzzy commitment scheme is one where a uniformly random key of length 1 bits is generated and used to exclusively index an *nbit* codeword of suitable error correcting code where the sketch extracted from the biometric template is stored in a database. The difference between *fuzzy vault* and *fuzzy commitment* as brought out by Geethanjali et al. is that biometric traits secured by fuzzy commitment are represented in the form of binary vectors which are divided into a number of segments and each segment is separately secured while biometric traits in fuzzy vault are represented in the form of point set which are secured by hiding them with chaff points (Geethanjali et al., 2012).

6.3. Other biometric template protection

Schemes: watermarking scheme, RSA and ECC algorithms.

6.3.1. Watermarking

In a biometric watermarking scheme, if an attacker tries to replace or forge the biometric template then he must have the knowledge of pixel values where watermark information is hidden as shown by (Malhotra and Kant, 2013).

6.3.2. Rivest, Shamir and Adleman (RSA) technique

RSA is an encryption algorithm for public key cryptography based on the practical difficulty problem of factorization of large integers as was described by (Nasir and Kuppuswamy, 2013). RSA algorithm‟s debut was in 1978 when it was first introduced by Rivest, Shamir and Adleman and was named after their names i.e. Rivest, Shamir and Adleman. The implementation of RSA algorithm involves a public key and a private key where the public key can be known to everyone and used for encrypting messages.

6.3.3. Elliptic Crypto Curve (ECC) Technique

Muthukuru & Sathyanarayana described an Elliptic Curve Cryptography also known as ECC as a public key cryptography that makes use of algebraic forms of elliptic curves over elements restricted to finite fields (Muthukuru and Sathyanarayana, 2013).

7. Summary and conclusions

Most of biometric systems used in real applications are unimodal, which means they rely on only one area of identification. So, they are not reliable enough like the systems that use more than one attributes ,such as collecting voice and face or palmprint for two hands to the same person, this system known" multibiometrics system". Multibiometrics systems are fusing separate information or separate features to provide integrate information. That make the systems more reliable recognition of individuals, also if don’t enable to obtains for required data to any traits the other traits enough led the system more is become more especially when used more than two traits reliable. The problems associated with biometrics are less obvious. Thinking about security and privacy, if a biometric is stolen, it cannot be regenerated like a password or PIN – it is compromised for the duration of the owner's life. Further, if biometric data is used in an unprotected setting, such as the Internet, the chance of compromise is high. We must remember that the Internet is composed of more than just unsecured transport channels - databases and other storage servers store biometric data. The prevalence of biometrics also means that common biometric data is stored in several locations for different purposes - allowing a searcher to link a particular user across disjoint databases and applications.

References

A A. Juels, M. Sudan, (2002). A Fuzzy Vault Scheme. IEEE International Symposium Information Theory.

A. K. Jain and U. Uludag, (2003). Hiding Biometric Data, IEEE transactions on pattern analysis and machine intelligence, 25(II), pp. 1494-1498.

A. K. Jain, K. Nandakumar, A. Nagar, (2008). Biometric Template Security. EURASIP Journal on Advances in Signal Processing.

A. O. George, (2005). Finger nail plate shape and size for personal identification a possible low technology method for the developing world - Preliminary report, Dermatology Division, University College Hospital, African Journal of Health Sciences, Vol. 12, No. 1-2, pp. 13-20.

A.J. Goldstein, M. Hill, N. J., Harmon, D. Leon, A.B. Lesk , (1970). Identification of Human Faces, Proc. IEEE, V. 59, No. 5, pp 748-760.

B. Duc, E. S. Bigün, J. Bigün, G. Maître, and S. Fischer, (1997). Fusion of audio and video information for multi modal person authentication, Pattern Recognition Letters, Vol. 18, No. 9, pp. 835-843.

B. Ulery, A. R. Hicklin, C. Watson, W. Fellner, and P. Hallinan, (2006). Studies of Biometric Fusion, Technical Report IR 7346, NIST, September.

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

G. Shakhnarovich, L. Lee, T. Darrell, (2001). Integrated Face and Gait Recognition From Multiple Views, cvpr, IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'01), Vol. 1, pp.439.

Griaule Biometrics, (2012). Book-Understanding Biometrics,.

Group, I. B. (2014). www.biometricgroup.com, Retrieved May 12th.

J K. Anil , (2002). Biometrics Personal Identification in Networked Society, Michigan State University ,book Kluwer Academic Publishers New York, Boston, Dordrecht, London, Moscow.

J. M. Chawki, M. S. Abdel Wahab, (2006). Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica,(Printemps/ Spring. http://www.lexelectronica.org/ articles, Vol 11, No.1.

J. Muthukuru, B. Sathyanarayana, (2013). A Survey of Elliptic Curve Cryptography Implementation Approaches for Efficient Smart Card Processing. Global Journal Of Computer Science and Technology, 12(1).

J. Shoa'a, M. AbdulAziz, (2011). Biometrics in Health Case Security System, Iris-Face Fusion System ”, International journal of academic research, Vol3, No. 1, pp 11-19.

J. V. Jeny, C. J. Jangid, (2013). Multibiometric Cryptosystem with Fuzzy Vault and Fuzzy Commitment by Feature-Level Fusion. International Journal of Emerging Technology and Advanced Engineering , (Volume 3, Issue 3, March 2013).

M. Blanton, M. Aliasgari, (2013). Analysis of Reusability of Secure Sketches and Fuzzy Extractors. Journal of Computer and System Sciences, 58, 148-173.

M. Emanuela, (2010). Secure Multbiometric Systems, PH.D thesis submitted to University of Naples Federico.

M. S. Nasir, P. Kuppuswamy, (2013). Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm. International Journal of Innovative Research in Computer and Communication Engineering, 1(8), 1741-1748.

M. S. Pravin and S. Shubhangi, (2011). Stegano-Crypto System for Enhancing Biometric-Feature Security with RSA. International Conference on Information and Network Technology, pp 196-200.

N. Geethanjali, K. Thamaraiselvi, R. Priyadharshini, (2012). Feature Level Fusion of Multibiometric Cryptosystem in Distributed System. International Journal of Modern Engineering Research (IJMER), 2(6), 4643-4647.

N. Karthik, (2008) , Multibiometric Systems: Fusion Strategies and Template Security, Mc.S thesis Submitted to Michigan State University, Department of Computer Science and Engineering.

N. Klimis, T. Nicolas, and D. Athanasios, (2011). Video-Object Oriented Biometrics Hiding for User Authentication under Error-Prone Transmissions. EURASIP Journal on Information Security. pp 12.

N. Malkhasyan,(2013). Authentication based on fingerprint with steganographic data protection, International Journal “Information Theories and Applications”, Vol. 20.

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

N. Radha, S. Karthikeyan. (2010). A Study on Biometric Template Security. ICTACT Journal on Soft Computing(01), 31-41.

N. Wang, C. Zhang , X. Li, and Y. Wang, (2010). Enhancing IrisFeature Security with Steganography. IEEE conference on Industrial Electronics and Applications, pp. 2233-2237.

National Biometric Security Project, (2008). Biometric Technology Application Manual, Biometric Basics, Updated Summer, Vol 1.

National center, (2005) individual Biometrics :Iris scan,http://ctl.ncsc.dni.us/biometweb / BMIris.html.

NSTC, (2006) biometrics History, book issue from National Science and Technology.

O. M. Aly, H. M. Onsi, G. I. Salama, T. A. Mahmoud, (2013). A Multimodal Biometric Recognition system using feature fusion based on PSO, International Journal of Advanced Research in Computer and Communication Engineering,Vol 2, Issue 11, November.

P. Rajni, (2014). Physical Security: A Biometric Approach, International Journal Of Engineering And Computer Science, Vol 3, No.2, pp. 3864-3868.

R. Hooda, S. Gupta, (2013). Fingerprint Fuzzy Vault: A Review. International Journal of Advanced Research in Computer Science and Software Engineering, 3(4), 479-482.

R. P. Miller, (1971). Finger dimension comparison identification system, US Patent, No. 3576538, 1971.

R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. K. Jain, (2005). Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol27, No.3, pp450-455, March.

R. Youmaran , (2011). Algorithm to Process and Measure Biometric Information Content in Low Quality Face and Iris Image” Ph.D thesis Faculty of Graduate and Postdoctoral Studies University of Ottawa Ottawa, Canada,

Ross, A. K. Jain, (2003) Information Fusion in Biometrics, Pattern Recognition Letters, Vol24, No 13, pp2115-2125, September.

Ross, K. Nandakumar, and A. K. Jain, (2006). Handbook of Multibiometrics. Springer.

S. Malhotra, and C. Dr.Kant, (2013). A Novel Approach for securing Biometric Template, Internal Journal of Advanced Research in Computer Science and Software Engineering, 3(5), pp 397--403.

S. Malhotra, C. Kant, (2013). A Novel approach for securing biometric template. International Journal of Advanced Research in Computer Science and Software Engineering, 3(5).

U. Park, (2009). Face Recognition: face in video, age invariance, and facial marks, PH.D thesis submitted to Michigan State University, computer science.

V. Claus, (2011). Biometrics and ID Management” COST 2011 European Workshop, Bio ID 2011 Brandenburg (Havel), Germany, March 8-10.

V. Schmitt, J. Jordaan, (2013, April). Establishing the Validity of Md5 and Sha-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in these Algorithms. International Journal of Computer Applications, 68(23), 0975 – 8887.

W. Almayyan, (2012). Performance Analysis of Multimodal Biometric Fusion " PhD Thesis Faculty of Technology De Montfort University England, United Kingdom February.

W. James, (2011). Introduction to Biometrics, book in Library of Congress Control Number, pp942231.

Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, (2008). Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. SIAM Journal on Computing, 38(1), 97-139.

Y.J. China, T.S. Onga, A.B.J. Teohb, and K.O.M. Goha, (2014). Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion, Volume 18, July 2014, pp. 161–174.