SHIV SHAKTI

International Journal of in Multidisciplinary and Academic Research (SSIJMAR)

Vol. 4, No. 3, June 2015 (ISSN 2278 – 5973)

Biometric Template Security using a Composite Approach

Ms. Versha Tomer
M.Tech
Department of Computer Science & Engineering
MDU University, Haryana, India

Impact Factor = 3.133 (Scientific Journal Impact Factor Value for 2012 by Inno Space Scientific Journal Impact Factor)

Global Impact Factor (2013)= 0.326 (By GIF)

Indexing:

Abstract: Biometric Template Security using a Composite Approach

In today's technology savvy world there is enormous increase in the number of biometric recognition systems. At the same time the number of attacks on the biometric systems is also increasing. So there is a need to protect these systems and ensure system security and reliability. This work presents a comprehensive analysis of the vulnerabilities of a biometric recognition system with emphasis on the vulnerabilities related to the information stored in biometric systems in the form of biometric templates. To encourage the improvement of techniques to protect biometric templates, we show the use of biometric cryptography and the cancellable biometrics in the existing systems. The techniques to safeguard the biometric templates are categorized into two main groups: biometric cryptosystems and template transformation methods. While biometric cryptosystems permit binding a secure key to the biometric data to obtain a so called secure sketch from which no information regarding the biometric data or the key can be retrieved again, cancelable biometric template transformation techniques non-invertible transform the biometric template with the user's password. To analyze and improve the biometric cryptosystems, we have studied its two main examples: fuzzy vault and the fuzzy commitment. Fuzzy vault is the technique used to secure templates characterized in the form of a finite set of points whereas fuzzy commitment is used for the security of templates represented as binary vectors. A superior security analysis is provided that makes biometric template more secure. A framework to effectively combine multiple biometric representations and efficiently verify an individual is also proposed.

1. Introduction: In today's modern and high-tech world the security concern is highly significant to overcome the imposters and the fake authenticated users for the authentication purposes. To identify a person with a high confidence is a serious issue in various applications, such as access control, passenger clearance, e-banking, etc. The objective of personal authentication is to determine or confirm the identity of individuals such that the right person is found out from the number of suspects, and requested services or facilities are accessed by a legitimate user, etc. Traditionally, personal authentication is fulfilled based on what the person has (e.g. ATM, keys and ID cards) or what the person knows (e.g. PIN). These approaches however have at least the following two drawbacks.

1) Both the tokens the user has and the knowledge the user knows can be lost, forgotten or stolen.

2) They have the problem of repudiation, e.g., a person accesses a certain resource and later claims that another person must have used it under counterfeited credentials. Two Biometrics based methods, which use unique inherent physical or behavioral characteristics of human beings, can solve above problems. It is well known that human beings instinctively make use of somebody characteristics, e.g. face, gait, or voice, to recognize each other. Because the biometric traits are inherent in people, one is not bothered by forgetting or losing them or having them stolen and consequently he/she cannot deny his/her ever use of his/her biometric traits. Biometrics is the most accurate form of identifiers and, if used properly, can greatly simplify life.

1.1 The Foundations of Biometrics

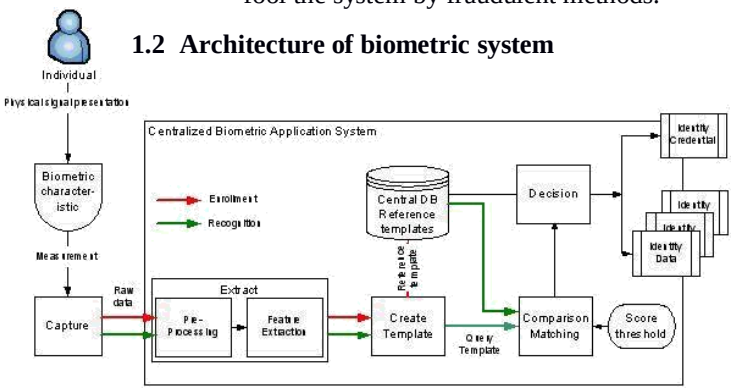
A biometric system is basically a pattern recognition system that acquires biometric data from an individual, extracts a salient feature set and compares this feature set against the feature set(s) stored in the database, and takes an action based on the result of the comparison. A number of physical and behavioral body traits can be used for biometric recognition. Examples of physical traits include face, fingerprint, iris, palm print, hand geometry and ear shape. Gait, signature and keystroke dynamics are some of the behavioral characteristics that can be used for person authentication.

. As identified by Ross et al., there are seven factors that can determine the suitability of a physical or behavioral trait to be used as a biometric identifier, including:

- Universality: it means that every person should possess the trait.
- Uniqueness: it indicates that no two persons should be the same in terms of the trait.
- Permanence: it means that the trait should not change with time. A trait that changes significantly with time is not a good biometric trait.
- Collectability: it means that it should be possible to acquire and digitize the trait using suitable devices without causing any inconvenience to user.
- Performance: it refers to the possible recognition speed, robustness, accuracy, and the resources required to achieve the accuracy and speed.
- Acceptability: it specifies the degree to which people are willing to accept a particular biometrics in their daily life.

- Circumvention: it refers to how easy it is to fool the system by fraudulent methods.

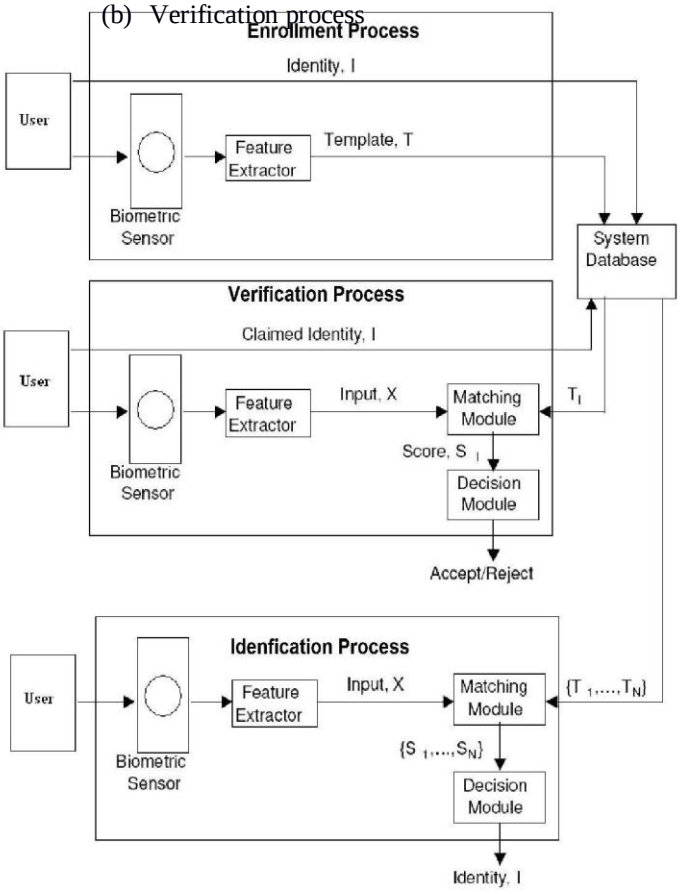
1.2 Architecture of biometric system



Any biometrics system operates in two phases -

(a) Enrollment process

(b) Verification process



A usual biometric system consists of four major modules.

(a) **The sensor module**- is responsible for extracting the biometric data from an individual.

(b) **The feature extraction module**- processes the extracted biometric data and extracts only the main information to form a new illustration of the data known as template. This new representation or template should be unique for each person and also relatively invariant with respect to changes in the various samples collected from the same biometric data taken from the same person.

(c) **The matching module**- at feature extraction level compares the feature set extracted with the templates stored in the system database and helps to determine the degree of similarity (dissimilarity) between the two.

(d) **The decision module**- either verifies the identity that is claimed by the user or it determines the user's identity based on the degree of similarity between the features extracted and the stored template(s).

1.3 Security issues in biometric identification

(a) Performance limitations-

Biometrics does not provide perfect (unique) identification. The matching process is probabilistic and is subject to statistical error. A mistaken identification or verification where the wrong person is matched against an enrolled user is termed a False Acceptance and the rate at which these occur is the False Acceptance Rate (FAR).

Conversely, an error that occurs where a legitimate user fails to be recognized is termed a False Rejection and the corresponding rate is the False Rejection Rate (FRR). These errors are dependent not only on the technology but also on the application and the environment of use.

(b) Enrolment integrity-

Ensuring enrolment integrity is a vital underlying requirement for all authentication systems whether or not biometrics are used. If the enrolment integrity is compromised, all bets are off regarding security. System implementers will need to determine what credentials are necessary and sufficient to validate users prior to enrolment, and then to ensure that the enrolment process itself is secure – in most cases this will mean supervision by trusted trained staff.

(c) Spoofing (physiological biometrics)

Spoofing through the use of artifacts is generally a concern for physiological biometric technologies such as fingerprint, hand, iris etc. Several studies dating from around 1998 have demonstrated the potential for successfully mounting a spoofing attack under carefully controlled conditions. If spoofing attacks can be successful, the fundamental tenet of biometrics – the "something you are" – is undermined. Spoofing involves 2 stages: a) - the capture of a biometric "image" belonging to an enrolled user, and b) - transferring the biometric image onto an artefact.Some features will be more difficult to observe and capture than others, and the skill needed to create a successful artefact will be dependent on both the biometric feature and how resistant the system is to artefacts. Faces are easily captured by photography. Fingerprint patterns may be captured through the lifting of latent or residual images left on smooth surfaces. Voices may be captured on tape or other audio recorder. Some

biometric images will be difficult to capture, e.g. retinal patterns, without the use of sophisticated and conspicuous equipment. Of course, given cooperation by the legitimate user, the capturing of biometric features is likely to be much easier. Constructing an artefact containing the biometric features is also subject to varying difficulty depending on the feature involved and the sophistication required of the artefact, which in turn depends on the countermeasures in place.

(d) Template integrity

Template integrity and confidentiality are distinctly different issues related to template data though similar solutions may be employed to deal with both problems. Template integrity is concerned with threats to the authentication process caused by planted or modified templates, whereas template confidentiality relates to the legal and privacy issues around the template data and the way in which the data could be misused.

The integrity of the authentication process depends, among other factors, on the integrity of the template. If either the reference template or the "live" biometric sample is untrustworthy, the resulting authentication will be untrustworthy. Untrustworthy templates could occur for one or more of several different reasons:

- Accidental corruption due to a malfunction of the system hardware or software.
- Intentional modification of a bona-fide template by an attacker;
- The insertion of a biometric template corresponding to the attacker to substitute for the reference template of an authorized enrollee.
- The addition of a biometric template corresponding to the attacker to create a bogus "enrolment" on the system.

(e) Capture/replay attacks

Capture/replay is the name given to attacks where the biometric signals from an enrolled user are captured at one place and time and replayed later (usually at the same place) in an attempt to fool the system that the enrolled used is present. Although this can arguably occur at many points in the biometric system, the terminology usually applies to electrical signals captured between the capture device and the rest of the system. It may be a particular problem where there is a large and unsupervised path between the 2 components such as a network connection.

1.4 Biometrics template security-

(a) Invisible watermarking technique:

The invisible watermarking technique uses an algorithm to include hide data with the template.

The algorithm is described as under:

Step 1: Read the watermark information that we want to hide in the biometric template.

Step 2: Read the biometric template

Step 3: Find out the pseudorandom pixel location in the biometric template where watermark is to be inserted by using pseudorandom number generator which is seeded with the secret key.

Step 4: If at a pixel location we want to hide 0, then go to step 5 else go to step 6.

Step 5: a) Check whether there exists odd parity at the selected pixel location, then insert 0 at the pixel location (no change in pixel value is required in this case). Go to END. **b)** If even parity exists, then make the odd parity at that location by adding or subtracting 1 to that pixel location (change in pixel is required in this case). Go to END.

Step 6: a) Check whether there exists even parity at the selected pixel location, then insert 1 at the pixel location (no change in pixel value is required in this case). Go to END.

b) If odd parity exists, then make the even parity at that location by adding or subtracting 0 to that pixel location (change in pixel is required in this case). Go to END.

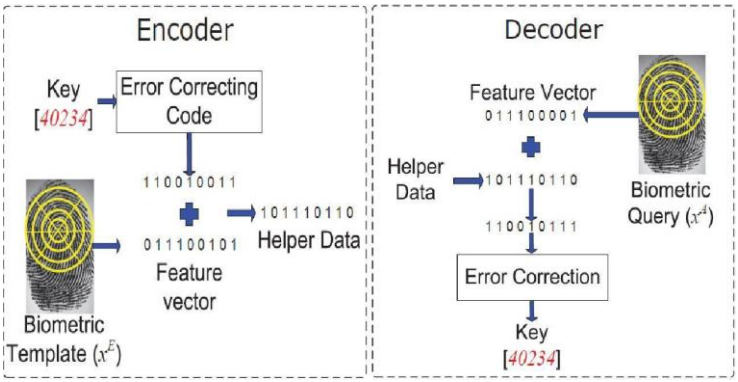
Step 7: END.

(b) Biometrics cryptosystem:

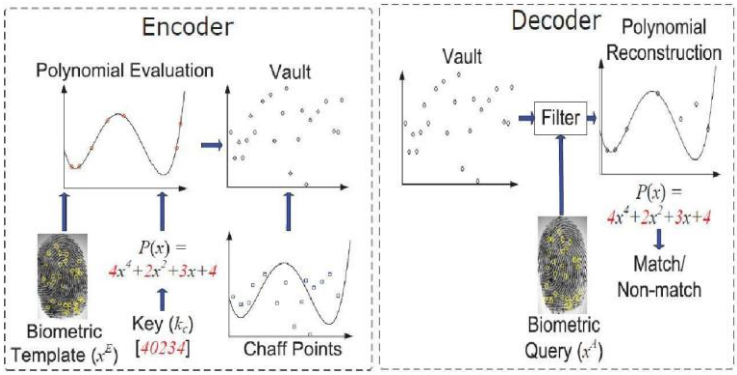
A fuzzy commitment: scheme consists of a function F, used to commit a codeword c 2 C and a witness x 2 f0; 1gn. The set C is a set of error correcting codewords c of length n and x represents a bit stream of length n, termed witness (biometric data). The difference vector of c and x, _ 2 f0; 1gn, where x = c + _, and a hash value h(c) are stored as the commitment termed F(c; x) (helper data). Each x0, which is sufficiently ―close‖ to x, according to an appropriate metric, should be able to reconstruct c using the difference vector _ to translate x0 in the direction of x. A hash of the result is tested against h(c). With respect to biometric key-binding the system acquires a witness x at enrollment, selects a codeword c 2 C, calculates and stores the commitment F(c; x) (_ and h(c)). At the time of authentication, a witness x0 is acquired and the system checks whether x0 yields a successful recommitment.

Fuzzy Vault: One of the most popular BCSs called fuzzy vault was introduced by Juels and Sudan [17] in 2002. The key idea of the fuzzy vault scheme is to use an unordered set A to lock a secret key k, yielding a vault, denoted by VA. If another set B overlaps largely with A, k is reconstructed, i.e. the vault VA is unlocked. The vault is created applying polynomial encoding and error correction. During the enrollment phase a polynomial p is selected which encodes the key k in some way (e.g. the coefficients of p are

formed by k), denoted by p k. Subsequently, the elements of A are projected onto the polynomial p, i.e. p(A) is calculated. Additionally, chaff points are added in order to obscure genuine points of the polynomial.

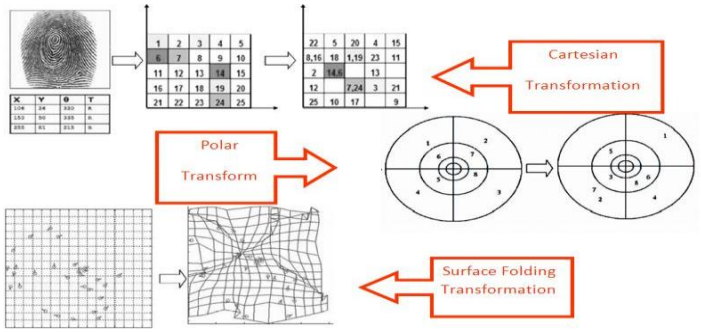


Fig(a) Fuzzy Commitment



Fig(b) Fuzzy Vault

(c) Cancellable templates:



2. Literature Survey/ Related Work

2.1. Past-

(i) European explorer Joao de Barros recorded the first known example of fingerprinting, which is a form of biometrics, in China during the 14th century. Chinese merchants used ink to take children's fingerprints for identification purposes.

(ii) In 1890, Alphonse Bertillon studied body mechanics and measurements to help in identifying criminals. The police used his method, the Bertillonage method, until it falsely identified some subjects.

(iii) The Bertillonage method was quickly abandoned in favor of fingerprinting, brought back into use by Richard Edward Henry of Scotland Yard. Karl Pearson, an applied mathematician studied biometric research early in the 20th century at University College of London. He made important discoveries in the field of biometrics through studying statistical history and correlation, which he applied to animal evolution. His historical work included the method of moments, the Pearson system of curves, correlation and the chi-squared test.

(iv) In the 1960s and '70s, signature biometric authentication procedures were developed, but the biometric field remained fixed until the military and security agencies researched and developed biometric technology beyond fingerprinting.

2.2. Present- Biometrics authentication is a growing and controversial field in which civil liberties groups express concern over privacy and identity issues. Today, biometric laws and regulations are in process and biometric industry standards are being tested. Face recognition biometrics has not reached the prevalent level of fingerprinting, but with constant technological pushes and with the threat of terrorism, researchers and biometric developers will stimulate this security technology for the twenty-first century. In modern approach, Biometric characteristics can be divided in two main classes:

a) Physiological are related to the shape of the body and thus it varies from person to person Fingerprints, Face recognition, hand geometry and iris recognition are some examples of this type of Biometric.

b) Behavioral are related to the behavior of a person. Some examples in this case are signature, keystroke dynamics and of voice. Sometimes voice is also considered to be a physiological biometric as it varies from person to person.

Recently, a new trend has been developed that merges human perception to computer database in a brain-machine interface. This approach has been referred to as cognitive biometrics. Cognitive biometrics is based on specific responses of the brain to stimuli which could be used to trigger a computer database search.

2.3. Future- A biometric system can provide two functions. One of which is verification and the other one is Authentication. So, the techniques used for biometric authentication has to be stringent enough that they can employ both these functionalities simultaneously. Currently, cognitive biometrics systems are being developed to use brain response to odor stimuli, facial perception and mental performance for search at ports and high security areas. Other biometric strategies are being developed such as those based on gait (way of walking), retina, Hand veins, ear canal, facial thermogram, DNA, odor

and scent and palm prints. In the near future, these biometric techniques can be the solution for the current threats in world of information security. Of late after a thorough research it can be concluded that approaches made for simultaneous authentication and verification is most promising for iris, finger print and palm vain policies. But whatever the method we choose, main constraint will be its performance in real life situation. So, application of Artificial System can be a solution for these cases. We have given emphasis on the Iris recognition. According to us, after detection of an iris pattern, the distance between pupil and the iris boundary can be computed. This metric can be used for the recognition purposes because this feature remains unique for each and every individual. Again, an artificial system can be designed which will update the stored metric as the proposed feature may vary for a particular person after certain time period. After doing the manual analysis of the above discussed method, we have got a satisfactory result. Due to the dynamic modification of the proposed metric, the rejection ration for a same person reduces by a lot. The work is being carried out to make the system viable.

3. Objective

3.1 Proposed Work-1

In this paper, we have tried to provide a theoretical approach to provide more secure biometric template. A biometric template (or simply template) is a digital orientation of distinctive characteristics that have been taken out from a biometric sample. Biometric templates are extracted from stored database and used during the authentication process. Securing Template is very crucial these days. In this chapter, a more secured approach is proposed which provides higher level of security to the templates.

3.1.1 Objective of proposed work

(i) Diversity- To ensure privacy, the template should be unique. Individual differences should be easily recognized

(ii) Revocability- it means to review. The new template can be easily reissued based on same biometric data.

(iii) Security- The prevention of template and protection against danger. It must be difficult to biometric template from the stored template.

(iv) Performance- The biometric template protection scheme should have high recognition performance. Hence, the main objective of proposed work is to provide an ideal protection approach and possess all the above mentioned properties of an ideal protection scheme.

3.1.2 Methodology

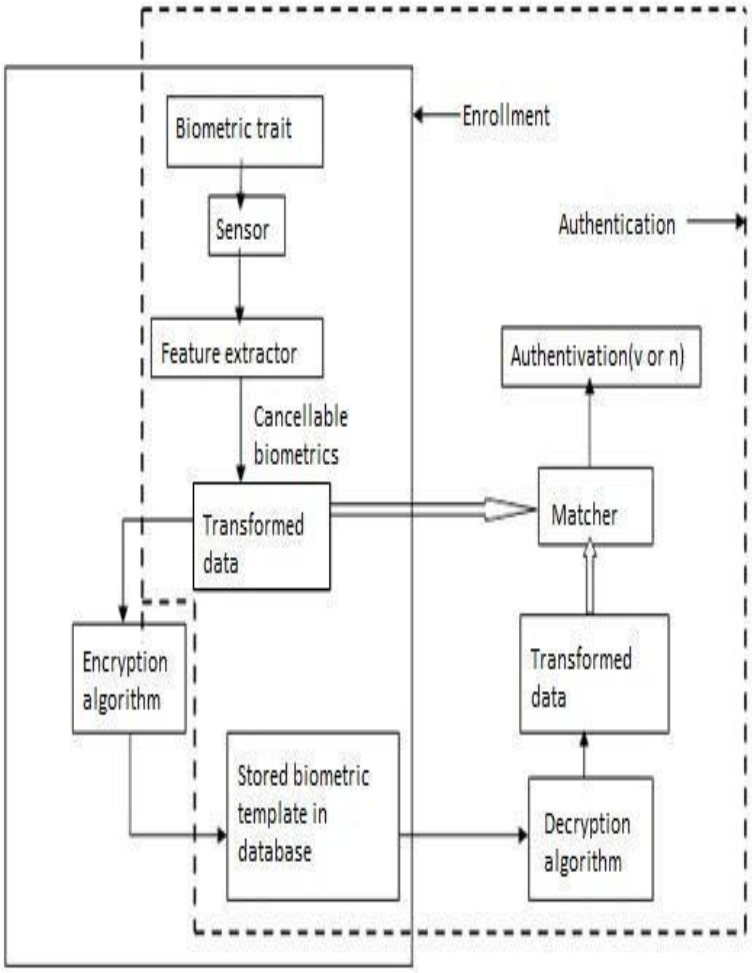
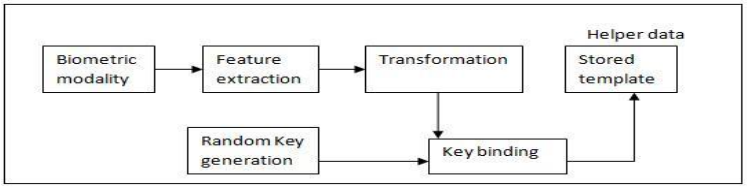


Fig. Architecture of proposed approach

Encryption algorithm: The following encryption algorithm has been used for cryptography. It is used because of its simplicity as it uses matrix multiplication and inversion for enciphering and deciphering, its high speed, and high throughput an encryption technique in which a key can be generated for the encryption of a biometric template. This algorithm generates the different key matrix for each block encryption instead of keeping the key matrix constant. This increases the secrecy of key. The new matrix we obtain after modification of the key matrix is called the encryption matrix [111].

i. Let ID be the unique identification number of the individual (Assume ID = 7)
ii. Generate a random number R in range [2, ID] (Assume R = 5)
iii. Create a magic matrix of random size key X key, where key = R X ID (then key = 7 X 5 = 35 and random Magic matrix = 35 X 35)
iv. Add magic matrix with template to create BE template.
v. Shuffle the BE template



Decryption Algorithm: The following decryption algorithm has been used.

i. Read BE template from the database corresponding to the ID. (E.g. retrieve the BE template corresponding to the ID = 7)
ii. Rearrange the BE template in the original order.
iii. Subtract the new Template so created at the time of authentication from original BE template.
iv. Then the difference matrix should satisfy preset threshold value.
v. The size of the magic matrix is retrieved (key retrieved = 35).
vi. Key is divided by ID, if result obtained through division lies in the range [2, ID], and then the user is authenticated. (Here result = 35/7 = 5 which lies in the specified range).
vii. After subtracting magic matrix from BE template, it is matched with the new template in order to make the system more robust.

3.2 Proposed work

In this proposed work, we have combined one physical and one behavioral approach for identification or verification to uniquely identify a person. The approach takes two different biometric traits. One finger print as physiological and other online signature as behavioral biometric trait. Both are sensed by sensor, features are extracted by feature extractor modules, matcher module matches the traits with stored template, each decision module decide the perfect matches. Finally decisions are combined in fusion unit using simple ―AND‖ and decision is taken whether the individual is not intruder.

3.2.1 Objective of proposed work

(i) The Objective of the proposed system is to reach an approach which is an ideal protection scheme and possess all the properties of an ideal protection scheme. The properties has been discussed above.
(ii) Secondly, it should be able to efficiently verify and identify an individual. It should be able to differentiate a genuine and an imposter.
(iii) Thirdly, it should be simple and not a complex system. It should meet the minimum requirements of cost, time and effort.

3.2.2 Methodology

Fig(c) General enrollment in proposed approach

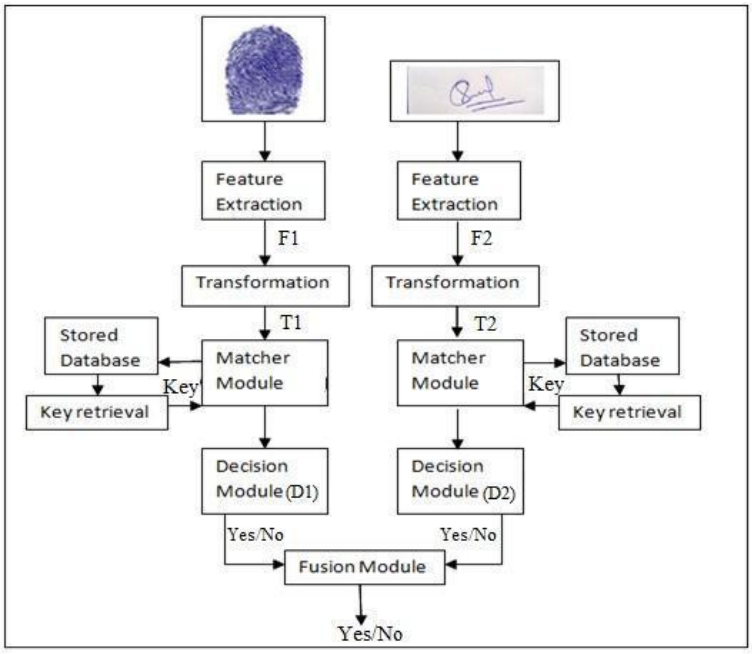


Fig (d) Authentication in proposed approach

Proposed approach consists of various modules of authentication-
(1). Feature extraction module: the clarity of internal structure is increased by extracting features of biometric trait and get proper minutiae features. The features of the fingerprint image can be extracted using reference point algorithm or minutiae matching method. The features of online signature are extracted using local and global features extraction. Global features are extracted the width and length of the signature and taking the signature as a whole. Local features are extracted by extracting every small point, hence calculation is large and framework notification is done very carefully.
(2). Matching module and the stored database: At this module matching of the biometric trait with the stored template is done. In the proposed approach working of the module is described in figure 4. During enrollment, the biometric trait is extracted and sandwiched with transformation and key to make it more secure. During authentication, using a matcher biometric trait is matched with the stored template. If the key bounded at the time of enrollment matches with the retrieved key only than the individual is same person otherwise not.
(3). Decision module and fusion module: The decision module represented the decision after the matching. The decision is yes if the individual is the same person otherwise decision is no. In the fusion module decision from both the decision modules is fused. Acceptance or rejection of individual is resulted from the fusion module.

Algorithm for the Enrollment phase

1) Capture fingerprint and signature from different sensors.
2) Extracts the feature set of respective biometric trait.
3) Apply Cartesian Transformation Technique (Cancellable Biometric) on the extracted feature sets to make these non invertible forms.
4) Bind the randomly generated key with transformed feature sets of fingerprint and signature.
5) Store the highly secure template (i.e. key binded with transformed template) in the database.

Algorithm for the Authentication phase

1) Capture fingerprint and signature from different sensors.
2) Extracts the feature set of respective biometric trait.
3) Apply Cartesian Transformation Technique (Cancellable Biometric) on the extracted feature sets F_1, F_2 respectively to make them non invertible.
4) Match the transformed template T_1 with the stored template (i.e. fingerprint transformed) to retrieve the key.
5) If (Key Retrieved = Key stored in database)
   Positive Response by the Decision Module D_1
6) Else
   Negative Response by the Decision Module D_1
7) End If
8) Match the transformed template T_2 with the stored template (i.e. signature transformed) to retrieve the key.
9) If (Key Retrieved = Key stored in database)
   Positive Response by the Decision Module D_2
10) Else
   Negative Response by the Decision Module D_2
11) End If
12) Apply "AND Fusion Rule" on decisions given by decision module D_1 and D_2 to compute the final result.

3.3.3 Comparison of proposed composite approach with other approaches

(1). Proposed composite approach is best approach as it satisfied the entire essential properties of template protection scheme. It is revocable, secure, diverse, and provides high performance.

(2). the transformation used over the extracted features is non invertible and makes the template highly secure which cannot be recovered by any of the imposter.

(3). the key binding cryptosystem approach provides improved secure templates and does not allow the real template to get exposed.

(4). the multimodal approach helps to uniquely identify a person accurately and the fusion are chosen at decision level, hence made the approach simple.

4. Recent advances in emerging biometrics

(a) India's national ID program-
India's national ID program called Aadhaar is the largest biometric database in the world. It is a biometrics-based digital identity assigned for a person's lifetime, verifiable online instantly in the public domain, at any time, from anywhere, in a paperless way. It is designed to enable government agencies to deliver a retail public service securely based on biometric data (fingerprint, iris scan and face photo), along with demographic data (name, age, gender, address, parent/spouse name, mobile phone number) of a person. The data is transmitted in encrypted form over the internet for authentication, aiming to free it from the limitations of physical presence of a person at a given place.

(b) Proposal calls for biometric authentication to access certain public networks.

(c) In recent times, biometrics based on brain (electroencephalogram) and heart (electrocardiogram) signals have emerged.The research group at University of Wolverhamptonled by Ramaswamy Palaniappan has shown that people have certain distinct brain and heart patterns that are specific for each individual. The advantage of such 'futuristic' technology is that it is more fraud resistant compared to conventional biometrics like fingerprints. However, such technology is generally more cumbersome and still has issues such as lower accuracy and poor reproducibility over time.

5. Conclusion and Future work

In today's high tech era, with the rapid increase in number of biometric recognition systems in commercial sector, security of the stored biometric data is increasingly becoming crucial. As assessed in this dissertation, current biometric systems have a number of vulnerabilities and a motivated adversary can undoubtedly cause severe harm to a biometric system as well as the users enrolled in the system.

Furthermore, due to the permanent nature of biometrics data its theft and misuse may be irreparable. If someone‘s fingerprints or iris patterns are stolen and are falsely linked to high susceptibility of a dreaded disease, the person may be unable to obtain a medical insurance. Stolen biometric data may devoid a person of any conveniences offered by the biometric systems due to the concern of being easily impersonated using spoof biometrics. While these threats may not appear to be imminent, the spaces at which biometric systems are increasing rapidly, the wealth of information one may harness by staging extensive theft of biometric data would definite motivate the con men.

Through this dissertation, we have provided better and more secure approach that we hope would be instrumental in circumventing any compromises of the biometric systems and in maintaining public trust in using biometric systems. The first chapter of this dissertation details various aspects of biometrics. A designer of a biometric system may use this discussion as reference while building a biometric system that is robust to any theft or sabotage. The second chapter discusses the biometric security techniques and vulnerability of current biometric data storage along with spoof detection techniques. The third chapter analyzes the different approaches that have been proposed and used in yesteryears for securing biometric template. The fourth chapter develops techniques to combine the advantages of biometric cryptography and cancelable biometrics.

The developed technique shows a significant improvement in terms of security as it combines the advantage of cryptography and cancelable biometrics. The system can be used for any biometric trait and can also be successful in multibiometric systems and hence will make a multibiometric system simpler as well as secure. The other proposed system is also developed which is overcomes the problem of time and cost in multimodal biometrics. The system can be used to efficiently verify a person in a simple way. Hence, in future we can use the former approach to be used in multimodal biometrics and and we can also extend the system for various other attack points.

6. References

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, “Biometric Recognition: Security & Privacy Concerns”, IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp. 33-42, March-April 2003.

[2] L. O’Gorman, “Comparing passwords, tokens, and biometrics for user authentication”, Proceedings of the IEEE, Vol. 91, No. 12, pp. 2019-40, Dec. 2003..

[3] Anil Jain, Lin Hong, and Sharath Pankanti, “Biometric Identification”, Communications of the ACM, Vol. 43, No. 2, February 2000.

[4] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, “Handbook of Fingerprint Recognition”. Springer-Verlag, 2003.

[5] Zhang L, Zhang L, Zhang D, Zhu HL (2010) Online finger knuckle print verification for personal authentication. Pattern Recogn 43(7):2560–2571..

[6] Balci, K., Atalay, V., “PCA for Gender Estimation: Which Eigenvectors Contribute?”, in16th International Conference on Pattern Recognition (ICPR’02) Vol. 3,QC, Canada, 363-366, 2002

[7] Arun Ross, “An introduction to multibiometrics”, In Proceedings of the 15th European Signal Processing Conference (EUSIPCO), pages 20–24, Poznan, Poland, 2007.

[8] H. Borgen, P. Bours, S. D. Wolthusen, “Visible-Spectrum Biometric Retina Recognition”, In International Conference on Intelligent Information Hiding and Multimedia Signal Processing IIHMSP’08, pp. 1056 – 1062, 2008

[9] M. Cheung, K. Yiu, M. Mak, and S. Kung, “Multi-Sample Fusion with Constrained Feature Transformation for Robust Speaker Verification”, In Eighth International Conference on Spoken Language Processing (ICSLP), pages 1813- 1816, Jeju Island, Korea, October 2004

[10] U. Uludag and A. K. Jain, “Attacks on biometric systems: a case study in fingerprints,” in Proc. SPIE-EI Security, Steganography and Watermarking of Multimedia Contents VI, San Jose, CA, vol. 5306, pp. 622–633, Jan. 2004.

.