ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

A Combined Robust Hashing and Secure Sketch Algorithm for Multi-Biometric Template Security

Ms. E.Durgadevi[1], Mrs. B.Karthiga[2], Mrs. B.Revathi[3], Ms. M.Revathy[4]

[1]PG Student [VLSI], Dept of ECE, Srinivasan Engineering College, Tamilnadu, India.

[2]Associate Professor, Dept of ECE, Srinivasan Engineering College, Tamilnadu, India.

[3]Associate Professor, Dept of ECE, Dhanalakshmi Srinivasan Institutions, TamilNadu, India.

[4]PG Student [CSE], Dept of CSE, Srinivasan Engineering College, Tamilnadu, India.

ABSTRACT: Multi-Biometric template security has become a very important issue in biometric authentication systems. If once a biometric template is compromised, it leads to serious security issues and privacy threats because unlike passwords, it is not possible for an authorized user to revoke his biometric identifiers and switch to another set of uncompromised identifiers. When using unimodal biometric systems (i.e., single Biometric Template) it leads to a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, unacceptable error rates, minimum key strength and so on. Some of these limitations can be resolved by deploying Multimodal Biometric systems that integrates the multiple sources of information at various processing stages. In a Multimodal Biometric system each template is processed independently and then fusion technique is applied to combine these templates at anyone of the stage. The input templates that have taken are face, iris and voice. Here, in the proposed work Biometric fusion is applied at the feature level to combine the features of those templates. And then, secure sketch, a recently proposed error-tolerant cryptographic primitive is applied to the biometric template. After that, to improve the key strength of the Sketch, Robust Hashing is applied. The Entropy of the key is measured, which measures the key strength. The FAR and FRR rates are also used to determine the key strength.

Keywords: Multi-Biometric System, Fusion, Secure Sketch, Robust Hashing.

I.INTRODUCTION

The term Biometric refers to “automatic recognition of human based on their behavioural and biological characteristics”. In the Biometric authentication system there are two phases: Authentication phase and Enrollment phase. In the Authentication phase fresh input template is obtained from the individual and stored either on smart cards or central database. In the Authentication phase the query template is obtained from the same individual and matched with the corresponding stored template by the matcher that determines the similarity between the templates. The templates are stored in the form of extracted feature sets. And in the authentication phase the feature sets are obtained for matching. If it is matched in the authentication phase the user can access the system. If once the stored template is compromised it leads to serious security issues such as a legitimate user cannot access the system, the unauthorized user can get authorization and can misuse the system.

The templates must be protected carefully unless it can be misused by the unauthorized user. Many types of attacks are possible: Intrinsic attack and Adversary attack. Intrinsic attack is due to change in pose or noise in sensors. Adversary attacks are outsider attacks may be at the user interface, the interface between the modules, on the modules and on the stored template. Attacks at the stored template are mainly focusing on this work. Many template protection schemes are available for protecting the stored template. The template protection scheme should satisfy the following properties: Diversity, Revocability, Security, and Performance. The two main template protection approaches are: Feature based transformation and Biometric cryptosystem.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

In Feature based transformation, the transformation function (*f*) is applied on the biometric template (*T*); only the transformed template is stored on the database. The same transformation function (*f*) is applied on the query template (*Q*). The parameters of the transformation functions are derived from a random key (*k*). During the authentication phase the transformed query template is matched against with the stored transformed template. The feature transforms scheme is further classified as: Bio-hashing and Robust Hashing. Bio-hashing is an invertible transform, whereas Robust Hashing is a non- invertible transform.

In Biometric Cryptosystem some public information is stored in the database. The public information is referred as helper data. The helper data does not reveal any information about the original biometric template but it is needed to extract the key during matching. Biometric Cryptosystem is further classified as: Key Binding and Key Generation. When the helper data are obtained by binding a key it is referred to as Key binding. If the key is directly obtained from the helper data query template then it is known as Key generation cryptosystem.

In the proposed method, the input templates that have taken for Multi-Biometric system is Face, Iris and voice. For combining those templates Feature level fusion is applied to the templates. After that Secure sketch and Robust hashing algorithms are applied to improve the secure storage of the template.

II.RELATED WORK

Multi-Biometric system [2], [4] deploys Unimodal Biometric templates to improve the security. In Unimodal Biometric system a single biometric template is obtained from the individual whereas in Multi-Biometric system it employs two or more templates of the same individuals are used. Multiple templates such as fingerprint, face, voice, hand geometry, palm print and some soft biometrics are obtain from the same individual for Multi-Biometric system.

Multiple templates are combined using fusion techniques [6]. Several fusion methods are available to combine the multiple templates of the same individual. Those are: Sensor level, Feature level, Decision level, and Score level. In the sensor level, the obtained templates are compressed to form a composite structure. In the Feature level, the features of each template are obtained individually and then those are combined to form a composite structure of high dimensionality feature set. In Score level, Feature vectors are processed independently and then matching scores are obtained, based on the accuracy of matching score, templates are classified. And in Decision level, each modality is pre-classified independently.

III.PROPOSED METHODOLOGY

In the presented work, a hybrid template protection scheme is applied to improve the security. A feature transforms and Biometric Cryptosystem based approach is used.

In the proposed work, Biometric templates such as face, iris and voice of the same individuals are taken and then stored in the database. Feature level fusion is applied to combine those templates. For that, features of each template are obtained individually and then a composite structure is formed by combining the feature sets of each template of the same individual. For face templates Eigen faces are used to extract the feature. For iris, Gabor filter is used for feature extraction. And for voice signal Cepstrum analyser is used to extract the feature. And then, feature level fusion is employed to combine the features of input templates. MACE filter is used for fusing the templates. Then template protection schemes such as Secure sketch and the Robust Hashing algorithm is applied to protect the Multi-Biometric templates.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

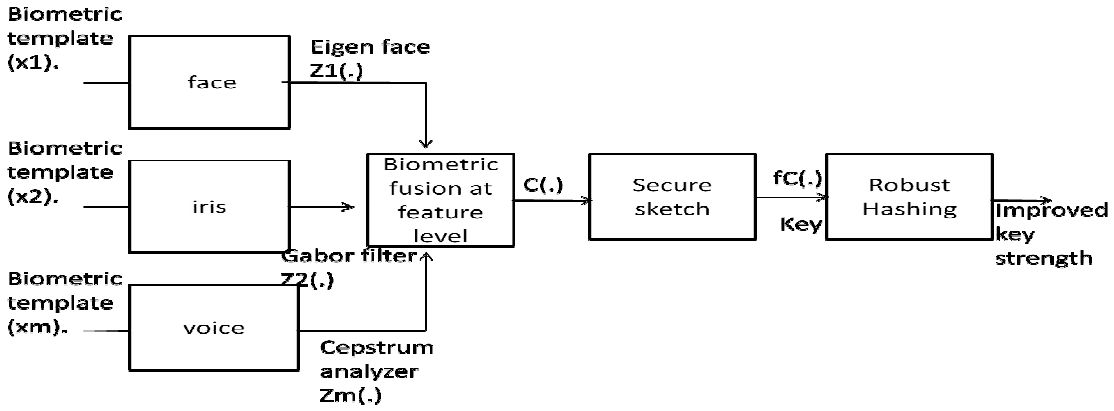

Fig.1 Proposed Methodology for Multi-Biometric Security

IV.FEATURE EXTRACTION

A. Face Feature Extraction

Eigen faces [1], [7] are used to extract the features from face templates. The following steps are involved to extract the features.

1. At first the training sets must be normalized to have the eyes and mouths aligned across all images. Then the images are reshaped to a common size of (r x c).
2. Each image is combined as a single vector by concatenating the rows of pixels in the input template.
3. The mean and standard deviations are calculated. This then subtracted from the image. The Eigen vectors and Eigen values are calculated for the covariance matrix. The Eigen vectors of this covariance matrix are called as Eigen faces.

B. Iris Feature Extraction

Multichannel Gabor filter [5] is used to extract the iris features. The filtering is done by convolution with a pair of filters. Gabor is a sine wave modulated by a Gaussian. Information is extracted in the frequency domain. The Gabor filters have adjustable orientation, radial frequency and centre frequency. The following steps are involved to extract the features.

1. In the first step, iris image is segmented which isolates eye by locating pupil, two eye lid and eye lashes. Segmentation is performed using Hough transform.
2. In the second step the normalization is performed which unwrap it into a rectangular block of fixed dimensions. Normalization is done by using Daugman's rubber sheet model. Polar coordinates are used for normalizing the templates.
3. Then feature vectors are extracted using Gabor filter. The centre frequency of the filter is given by sine and cosine waves. Only the phase information is needed for encoding.

C. Voice Feature Extraction

The Speech signal is usually obtained in the form as an analogue signal. Before extracting the feature from voice signal it must be transformed from analogue to digital domain. Speech signals are sampled at 8 KHz. Pre-Emphasize is done to raise the signal-to-noise ratio. And then the next step is framing. The length of each frame is around 30 msecs. Then the window function is applied to reduce the abrupt changes at the start and end point. And then the features are extracted from the signal. Most popular feature that is used for speech processing is Mel Frequency Cepstrum Coefficient (MFCC). The most efficient feature identity is the Cepstral coefficient. Cepstrum usually represents the articulate movements. A set of scaled non-linear filters or filter banks is used to filter the signal. Filter bank is a set of band pass signal whose centre frequency is spread across the frequency of the input signal.

To obtain MFCC of N samples, the magnitudes of Discrete Fourier Transform (DFT) are passed to the filter, and then the output of the filter is used to obtain MFCC using Discrete Cosine Transform. For Speaker verification Vector Quantization is used.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

V.FEATURE LEVEL FUSION

Fusion can be done at Score level, Feature level or Decision level. Generally Score level and Feature level are used. Score level fusion is easy to obtain but the information obtained is lesser than the Feature level fusion. Hence, Feature level fusion is applied. The difficulty that arises from the feature level fusion is that the features that are extracted from different templates are obtained in different domain. Therefore the features obtained from different domain must be converted to a same domain. Here the input templates face and iris are image based and voice is signal based which is obtained in the frequency domain. Correlation pattern recognition is proposed to fuse face, iris and voice templates.

Here Correlation Pattern recognition with Minimum Average Correlation Energy filter (MACE) is used to convert the features of different domain into a same frequency domain. MACE itself can be used as a feature extractor. For same domain input templates MACE filter is used as a feature extractor. The MACE filter is one of the correlation filters. The basic idea is to find the template that consists of features of the sample in a same class. FFT is applied on face and iris feature vectors to convert it to the frequency domain. The Voice signal is directly applied to MACE filter. Thus a composite feature vector is obtained that consists of features of face, iris and voice. Template protection schemes are then applied to the new feature vector.

VI.SECURE SKETCH

Secure Sketch [8], [10], [14] is one of the Biometric cryptosystem based approach. It is a key generation based approach. Biometric cryptosystem is also known as a helper data method. Helper data itself does not reveal the original biometric template. A sketch is generated for each template. The generated sketch instead of the original biometric template is stored in the database.

Sketch consists of two algorithms: Generation and Reconstruction.
Generation: A Sketch P is generated from the original image X.
Reconstruction: The original image can be reconstructed from the query image Y, which is similar to the original image X and the generated sketch P.

The steps involved in generating a sketch are, at first Feature vectors are extracted using the above methods. Fusion is then applied. Features are taken as a single column vector V_i. And then Randomization and Quantization are performed and Codebook is generated. The sketch algorithm is then applied. Entropy is measured to determine the key strength.

A. Randomization

A Randomized matrix is obtained by using uniformly distributed random numbers between $-\theta$ and θ. These random numbers are applied in obtaining feature vector. θ value is fixed to be 1. The resulting matrix is referred as Randomized matrix R_i.

The weighted matrix $W_i$is then obtained by multiplying the Feature Vector V_i with Randomized matrix R_i. The midpoint of the weighted matrix is obtained from the minimum (min_i) and maximum (max_i) value of the weighted matrix (midpoint = $(min_i + max_i)/2$). The reason for random mapping is for noise tolerance. This maximum and minimum value are used for calculating the range size $\delta_i = (min_i - max_i)/2$.

B. Quantization

Quantization is employed to discretize the image. A Scalar quantifier is used to discretize each vector. The global values of maximum and minimum values are calculated. $MN_i = \min(min_i)$ and $MX_i = \max(max_i)$. The quantization step is determined as $\delta = \alpha \min(\delta_i)$.

C. Codebook

Codebook C_i is generated for the quantized vector. Codebook consists of codeword's of each image.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

D. Sketch Generation and Reconstruction

Generation:

The Sketch P_i is generated, which is closest to the Codeword C_i.

Reconstruction:

Reconstruction is done by using the query template and the generated sketch.

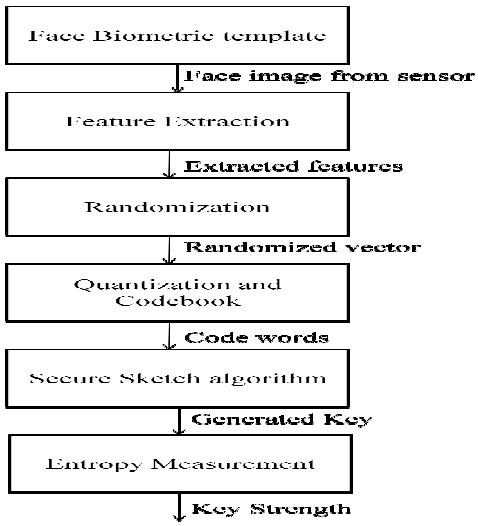

Fig. 2 Flow of Secure Sketch algorithm

E. Security

Security of Secure Sketch algorithm is determined by calculating the entropy of the generated sketch P_i. FAR and FRR rate is also used for security analysis in the authentication stage.

VII.ROBUST HASHING

Robust Hash function [3], [12], [13] is a one way transformation. Robust hashing is a non-invertible transforms. Here, a non- invertible transform is used to map biometric data to another space and it is stored in the database instead of the original template. The one way transformation is designed as a Gaussian function. The general steps involved in the Robust Hashing algorithm are:

A Robust hash function has two inputs: Key and an input image. The output is a short binary vector which called as Hash value of the given image.

1. For the given input, feature vector is obtained, and then one way transformation function is applied.
2. A secret key is generated by using pseudo random numbers.
3. And then a hash function is generated for the obtained feature vector with the help of generating secret key.

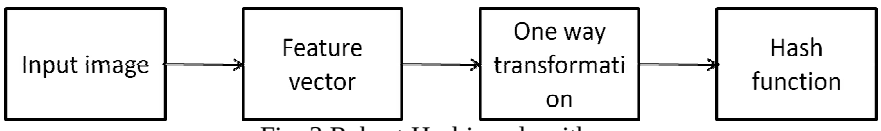

Fig. 3 Robust Hashing algorithm.

In our proposed scheme Secure Sketch algorithm is applied prior to robust hashing. The key generated from secure sketch is applied to robust hashing as a secret key to generate a hash function. The sketch is obtained in the form of

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

matrices. The one way transformation is applied to the extracted feature set and then hash function is generated for the image.

A. Security of Robust Hashing

Security measured in terms of Differential Entropy. The generated hash value is Gaussian distributed with mean and variance. The differential entropy is a function of variance and the sample points. As the variance increases, differential entropy is also increasing. And also the differential entropy is increased when the sample points are increased. The randomness associated with the hash value is also increases the security. When adding additional bits of key, it will increase the security. The generated hash function together with the generated will improve the security of the stored template.

VIII.RESULTS

The training datasets for a face template has 10 input images each with the size of 180 X 200. The images are then reshaped and then normalized. Eigen faces are obtained from those images and then sketch is generated from the given images.

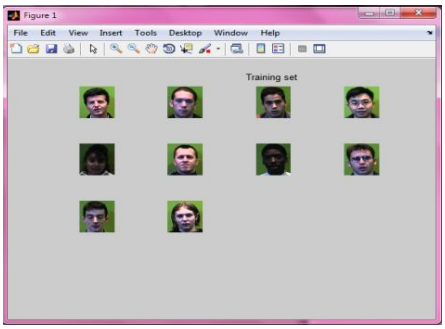

Fig. 4 Trained datasets

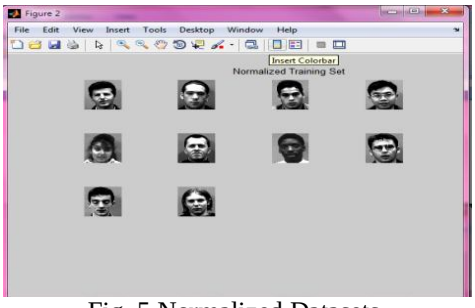

Fig. 5 Normalized Datasets

The images are then normalized. In the input database, each image is converted from RGB to Gray scale image has the Matrix size of [200 180] row and column respectively. Unit8 image is converted to double. The mean and Standard Deviation of each image is obtained. The mean image has the size <36000 X 1 double>. The Standard deviation of each image is 59.5700. Each image is normalized using mean and standard deviation.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

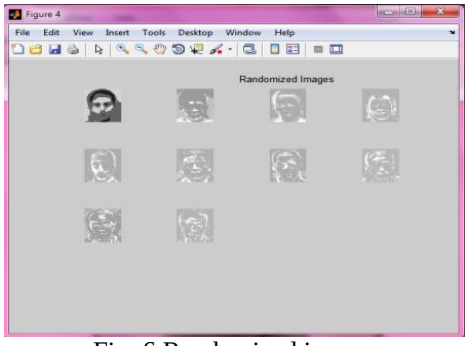

Fig. 6 Randomized image

Code words and Sketches are generated as a matrix. Codebook consists of several code words which correspond to each image.

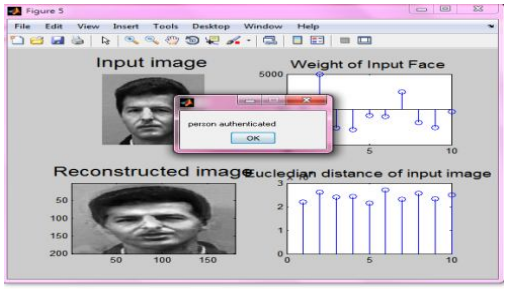

Fig. 7 Image Authentication

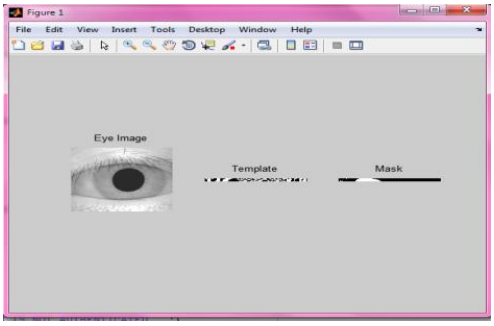

Fig. 9 Iris feature Extraction

Authentication of image is done by using Hamming Distance. Iris images are taken from CASIA datasets. Gabor filter is used for feature extraction.

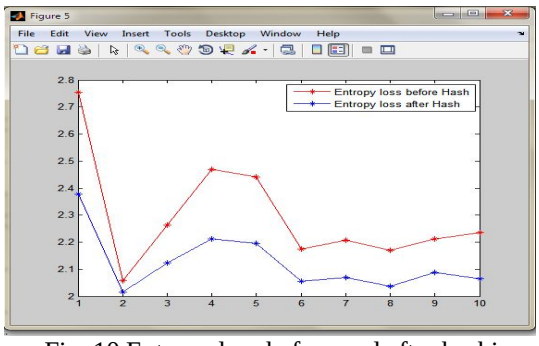

Fig. 10 Entropy loss before and after hashing

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

Entropy loss is calculated before applying secure sketch and after applying secure sketch. When combining both secure sketch and robust hashing it will minimize the entropy loss. When the Entropy loss is minimized key strength is improved.

VIII.CONCLUSION

In this work, a substantial construction of Secure Sketch for face, iris and voice are obtained. This work is done to protect the stored databases to ensure security. The key entropy is measured to determine the key strength in secure sketch. The Key Entropy is not alone the sufficient parameter to measure the security. For that, FAR and FRR measurements are also taken into consideration. FAR measures the number of falsely accepted unauthorized users and, FRR measures the number of falsely rejected legitimate user. When using a single Biometric template, finding a general and accurate way to compute the min-entropy of biometric data is a challenging open problem along with determining the exact information leakage of the sketches. For that, multi-biometric system that combines many sources are considered, which can improve the security. To improve the security further robust hashing applied after applying secure sketch. This hybrid approach improves the security. The security is measured in terms of differential entropy. This work enhances the security by increasing the key strength.

REFERENCES

[1] Andy Adler, Richard Youmaran, Sergey Loyka, "Towards a Measure of Biometric Feature Information", IEEE Xplore, Electrical and computer Engineering, 2006.
[2] Arun Ross and Anil K. Jain, "Multimodal Biometrics: An Overview" Appeared in Proc. of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp. 1221-1224, September 2004.
[3] AshwinSwaminathan, Yinian Mao, "Robust and Secure Image hashing", IEEE Transactions on Information Forensics and security, 2006.
[4] Christian Rathgeb and Christoph Busch, "Multi-Biometric Template Protection: Issues and Challenges", New Trends and Developments in Biometrics, ISBN 978- 953-51-0859-7, November 28,2012.
[5] Dolly Choudhary, ShamikTiwari, Ajay Kumar Singh, "A Survey: Feature Extraction Methods for Iris Recognition", International Journal of Electronics Communication and Computer Technology (IJECCT) Volume 2 Issue 6 (November 2012).
[6] Eugen LUPU, Petre G. POP, "Multimodal Biometric Systems Overview", ACTA TECHNICA NAPOCENSI, Electronics and Telecommunications, Volume 49, Number 3, 2008.
[7] Frank Y. Shih, Shouxian Cheng, Chao-Fa Chuang, Patrick S. P. Wang, "Extracting Faces and Facial Features from Color Images". IEEE Xplore, Automatic Face and Gesture Recognition, Oct 1996.
[8] Julien Bringer, HervéChabanne, Bruno Kindarji, "The best of both worlds: Applying Secure sketches to cancelable biometrics", Science of Computer Programming 74 (2008) 43_51.
[9] K.Sasidhar, Vijaya L Kakulapati, Kolikipogu Ramakrishna &K.KailasaRao, "Multimodal Biometric Systems –Study to Improve Accuracy and Performance", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.
[10] Marina Blanton and MehrdadAliasgari, "On The (Non-) Reusability of Fuzzy Sketches and Extractors and Security in the Computational Setting",Air Force Officeof Scientific Research,GRANT FA9550-09-1-0223.
[11] Vijay M. Mane, Dattatray V. Jadhav, "Review of Multimodal Biometrics: Applications, challenges and Research Areas", International Journal of Biometrics and Bioinformatics (IJBB), Volume 3, Issue 5.
[12] Xavier Boyen, YevgeniyDodis, Jonathan Katz, RafailOstrovsky,and Adam Smith, "Secure Remote Authentication Using Biometric Data". R.Cramer (Ed.): EUROCRYPT 2005, LNCS 3494, pp. 147 -163, 2005.
[13] YagizSutcu, HusrevTahaSencar, NasirMemon, "A Secure Biometric Authentication Scheme Based on Robust Hashing", MM&sec Proceedings of the 7th workshop on multimedia and security.
[14] YagizSutcu, Qiming Li, and NasirMemon, "Protecting Biometric Templates with Sketch: Theory and Practice", IEEE Transactions on Information Forensics and Security, Vol. 2, No. 3, September 2007.