IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-8 E-ISSN: 2347-2693

# A Multimodal Biometric Authentication Technique using Fused Features of Finger, Palm and Speech

**T. Srinivasa Rao[1*], E. Srinivasa Reddy[2]**

[1*]Dept. of Computer Science and Engineering, Acharya Nagarjuna University, Guntur, India
[2]Dept. of Computer Science and Engineering, Acharya Nagarjuna University, Guntur, India

[*]*Corresponding Author: tsr3333@gmail.com, Tel.: +91-9885143309*

**Available online at: www.ijcseonline.org**

Received: 16/Jul/2017, Revised: 24/Jul/2017, Accepted: 19/Aug/2017, Published: 30/Aug/2017

***Abstract*—** Biometric verification is a reliable approach that can be used to authenticate a person. Biometric authentication systems depend on unique human characteristics such as face, iris, fingerprint, gait, voice etc. to authenticate persons automatically. Biometrics varies from person to person and this is very sensitive data. This information should be kept safe, if not, severe security and privacy risks may occur. Biometric systems face some challenges like noise and non-universality in the process of establishing identity by using a single biometric trait. The noise in the data sensed from sensors may increase False Acceptance Rate (FAR) of the system where as non-universality may reduce Genuine Acceptance Rate (GAR). Because of this reason biometric systems that use single biometric trait provide less benefits in affording security. In this article, we device a Fused Multimodal system, which uses many biometric traits such as fingerprint, palmprint and voice etc. such that it may provide many advantages over uni-biometric systems such as, greater verification accuracy, larger feature space to accommodate more subjects and more security against spoofing. The newly proposed multimodal authentication system is primarily based on feature extraction using fingerprint, palm print, voice and key generation using RSA. MATLAB tool is used to carry out the experimentation. The performance of multimodal biometrics with RSA has significant improvement which has a GAR of 98% and FAR of 2%.

***Keywords*—**Multi-Modal Biometrics, Biometric Fusion, Fingerprint, Palmprint, Speech.

## I. INTRODUCTION

Person authentication has become of utmost importance. Traditional technologies authenticate persons using PINs or passwords but they are not more reliable. So that biometrics are using by the latest authenticating technologies as an automatic and reliable alternative to the traditional technologies. Biometric systems consider behavioral or physiological characteristics of the subjects as their identification. Among other advantages, biometric traits (e.g. face, speech, iris or fingerprint) cannot be lost or forgotten. Biometric authentication systems use unique human characteristics such as face, iris, fingerprint, gait, voice etc. to authenticate certain individuals automatically. All the modalities have their inherent advantages and shortcomings, but undoubtedly face detection is the most addressed and applied technique.

Biometrics [1] are basically based on the expansion of pattern recognition systems. Now a days, a person's unique characters like images, recordings or measurements can be acquired by electronic or optical sensors like cameras and scanning devices. Biometric systems are widely used in applications such as customs, security, prevention of cybercrime, and border control, healthcare, public aid/social benefits, passport, identity verification, immigration as well as commercial enterprises use. Biometric systems face some challenges like noise and non-universality in the process of establishing identity by using a single biometric trait. The noise in the data sensed from sensors may increase False Acceptance Rate (FAR) of the system where as non-universality may reduce Genuine Acceptance Rate (GAR). Because of this reason biometric systems that use single biometric trait provide less benefits in affording security. In this article, we device a Fused Multimodal system, which uses many biometric traits such as fingerprint, palmprint and voice etc. such that it may provide many advantages over uni-biometric systems such as, greater verification accuracy, larger feature space to accommodate more subjects and provide more security against spoofing. The newly proposed multimodal authentication system is primarily based on feature extraction using fingerprint, palm print, voice and key generation using RSA.

There are diverse biometric traits such as fingerprint, iris, Voice recognition, retina, finger vein and DNA etc., to recognize the identity of a person. If only one trait was taken

© 2017, IJCSE All Rights Reserved 

at a time it can be treated as uni-biometric [2] system. Uni-biometric systems has few drawbacks such as unpredictable biometric due to sensor, less quality of a biometric trait of the authentic user. In addition to that, large scale civilian recognition systems and high security applications require the perfect accuracy in analyzing the identities but uni-biometric systems may fail sometimes to meet that accuracy. So to fulfill the requirements of such applications, uni-biometric systems that are based on a single source of biometric information alone are not enough. Systems that combine the information from various biometric sources are to be considered for recognition. The consolidated information from these multiple sources can meet the required accuracy to determine or certificate an individual person. Hence the evolution of biometric systems that takes the information from multiple biometric [3] sources are emerged. These systems are to be considered as multibiometric systems which are expected to perform more accurately compared to uni-biometric systems that is based on the assertion of the particular segment of biometric trait.

Multibiometric systems can enhance the accuracy by using two steps. Firstly, effective fusion [4] of multiple biometric sources should be done. This will increases the dimensionality of the feature space and reduces the overlap between the feature distributions of dissimilar individuals. The fusion of multiple biometrics will give more exclusive identity to an individual than using a single biometric trait. In addition to accuracy, in muti-biometric systems, the noise, imprecision, or inherent drift (caused by factors like ageing) that are presented in a subset of one biometric sources can be covered by the undivided information provided by the remaining sources. Multi-modal biometric systems may also overcome some disadvantages of uni-biometric systems. Multi-modal biometric systems can solve the non-universality problem and may reduce the failure to enroll errors, make the search of a large biometric database in a computationally efficient manner and will increase the resistance to spoofing attacks, provides a degree of flexibility in user authentication. Multimodal biometric is nothing but the fusion of uni-biometric. Fusion level [5] has different techniques such as sensor level, feature level, score level, decision level, and rank level. In proposed system feature level fusion was used. Biometric traits like fingerprint, palm print and speech are considered in the proposed method are were combined [6-19,21-23] with asymmetric cryptographic algorithm RSA [20]. This biometric template was stored in the database which can increase the GAR and FAR. This article is organized into 6 sections. The first section is the introduction of various multimodal biometric traits. The second section discusses the fusion of multimodal biometric traits. The third section deals with the feature level fusion. The fourth section discusses about modified RSA algorithm. The fifth section results and discussions. The sixth and last section is conclusion.

## II. FUSION BASED MULTIMODAL BIOMETRIC SYSTEM

There are two modules in fusion multimodal biometric system. One is Enrollment module and the other one is Verification module which is shown below in Fig.1. Enrollment module contain an interface through some electronic equipment like the biometric sensor or reader to measure or record the raw biometric data from the user. From the taken biometric traits such as finger-print, palm-print, and speech, the required features will be extracted. In feature level fusion, the extracted features of all these biometric traits are to be fused and then by using RSA encryption technique, the fused features are be encrypted and to be stored as a template in a database. That template can be used later for desired authentication and verification that undergo in the verification module. In the verification module the user can claim for uniqueness of the biometric traits. The verification module verifies whether the claim is genuine or imposter.

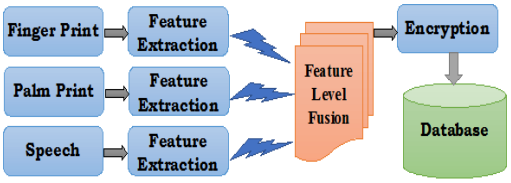


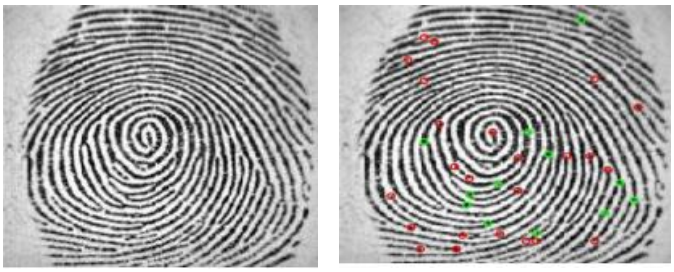

Figure.1 architecture of the proposed system

The captured biometric traits of a new individual through the Enrollment module interface are compared against the stored data only after the encrypted template in the verification module was decrypted. After comparison, the newly captured biometric traits of the individual are used to determine the identity of the user.

### *A. Fingerprint Feature Extraction*

Fingerprint which contain the impressions with the distinct ridges on the finger tips can be extracted by using the Finger print recognition technology. Finger-prints can be either rolled or flat. A rolled print captures ridge on both sides of the finger whereas flat print covers only an impression of the central area between the fingertip and the first knuckle. We only utilize the rolled print in our biometric system. Optical scanners are used to capture an image of the fingerprint. This finger-print was then enhanced, and converted into a template as shown in Fig.2 (b). There are some interesting points called minutiae which are by the corners or forking of the abrasion skin ridges on every finger. These minutiae points makes an individual's fingerprint unique by mainly focusing on location, orientation of ridge flow and its type (i.e. Ridge ending or bifurcation). The patterns can also be formed by the flow of friction skin ridges like the arch, whorl and loop of each finger. In this paper, Minutiae extraction is done based on bifurcation (with the point at which a single ridge splits into two ridges) and termination (immediate ending of a ridge).

© 2017, IJCSE All Rights Reserved 



(a) (b)

Figure.2 (a) Original image (b) Extracted minutiae points

*B. Palm-print feature extraction by texture analysis*

The palm-print feature extraction method includes two steps: filtering and matching. We first discuss about the Gabor filter which is the motivation for our palm print research.

*1. Gabor function*

Gabor-filter, Gabor-filter bank, Gabor-wavelet and Gabor-transform which use Gabor function can be widely applied to pattern recognition, image processing and other computer vision areas. Precise time frequency location can be given by the Gabor function which can be governed by the "Uncertainty Principle". The general form [8, 9] of a circular 2-D Gabor filter in the spatial domain is

$$G(x,y,\theta,u,\sigma) = \frac{1}{2\pi\sigma^2} exp\left(-\frac{x^2+y^2}{2\sigma^2}\right) \times exp\{2\pi i(ux\cos\theta + uy\sin\theta)\}$$

where i =√−1; $\theta$ controls the orientation of the function; σ is the standard deviation of the Gaussian envelope and $u$ is the frequency of the sinusoidal wave. In large number of applications Gabor filters are being widely used. Gabor functions has the ability to provide robustness against different brightness and contrast of images in addition to precise time-frequency location. Furthermore, the filters can model the receptive fields of a simple cell in the primary visual cortex. In this paper, we tried to apply the Gabor filter for the authentication of palm print based on all these properties of Gabor functions.

*2. Filtering and feature extraction*

We can generally observe the principal lines and wrinkles in our captured palm print images (see Fig. 3(a)). Stack filter is used to find the principal lines. But these principle lines may not always give high accuracy because there may be similarity amongst different palms. This can be seen in Fig. 3 which shows that there are similar principle lines in six palm print images. Instead of the principle lines, wrinkles can be used for palm print authentication because they can result in high accuracy in authentication. But accurately extracting the wrinkles is still a difficult task. So that we applied texture analysis for palm print authentication.

Table 1 The List of Parameters for the 12 filters

| Levels | No | Sizes | $\theta$ | U | σ |
|---|---|---|---|---|---|
| 1 | 1 | 9 x 9 | 0 | 0.3666 | 1.4045 |
| | 2 | 9 x 9 | 45 | 0.3666 | 1.4045 |
| | 3 | 9 x 9 | 90 | 0.3666 | 1.4045 |
| | 4 | 9 x 9 | 135 | 0.3666 | 1.4045 |
| 2 | 5 | 17 x 17 | 0 | 0.1833 | 2.8090 |
| | 6 | 17 x 17 | 45 | 0.1833 | 2.8090 |
| | 7 | 17 x 17 | 90 | 0.1833 | 2.8090 |
| | 8 | 17 x 17 | 135 | 0.1833 | 2.8090 |
| 3 | 9 | 35 x 35 | 0 | 0.0916 | 5.6179 |
| | 10 | 35 x 35 | 45 | 0.0916 | 5.6179 |
| | 11 | 35 x 35 | 90 | 0.0916 | 5.6179 |
| | 12 | 35 x 35 | 135 | 0.0916 | 5.6179 |

A Gabor function, G(x, y, Θ, u, σ) with a special set of parameters (σ, Θ, u), is changed into a discrete Gabor filter, G[x, y, Θ, u, σ]. Table 1 is the list of 12 sets of parameters that are based on experimental results that in the next section. The parameters for the discrete Gabor function are chosen from this Table. To achieve good robustness to brightness, the Gabor filter is converted to zero DC (direct current) by use of the following formula:

$$\tilde{G}[x,y,\theta,u,\sigma] = G[x,y,\theta,u,\sigma] - \frac{\sum_{i=-n}^{n}\sum_{j=-n}^{n} G[i,j,\theta,u,\sigma]}{(2n+1)^2}$$

where $(2n+1)^2$ is the size of the filter. As the Gabor filter has odd symmetry, automatically the illusionary part of the Gabor filter contain zero DC. This Gabor filter adjustment was perverted with a sub-image which was defined in section 2. By using the following inequalities, we can code the sample point in the filtered image to two bits as, ($b_r$, $b_i$)

$$b_r = 1 \quad \text{if} \quad \mathrm{Re}[\tilde{G}[x,y,\theta,u,\sigma] * I] \geq 0$$

$$b_r = 0 \quad \text{if} \quad \mathrm{Re}[\tilde{G}[x,y,\theta,u,\sigma] * I] < 0$$

$$b_i = 1 \quad \text{if} \quad \mathrm{Im}[\tilde{G}[x,y,\theta,u,\sigma] * I] \geq 0$$

$$b_i = 0 \quad \text{if} \quad \mathrm{Im}[\tilde{G}[x,y,\theta,u,\sigma] * I] < 0$$

where *I* is the sub-image of a palm print. The coding method is used only to store the phase information in palm print images in the feature vector. The feature size is 256 bytes. The features that are generated by the 12 filters listed in Table 1 are shown in Fig.3. Iris recognition can also be done by using this texture feature extraction method.

© 2017, IJCSE All Rights Reserved 

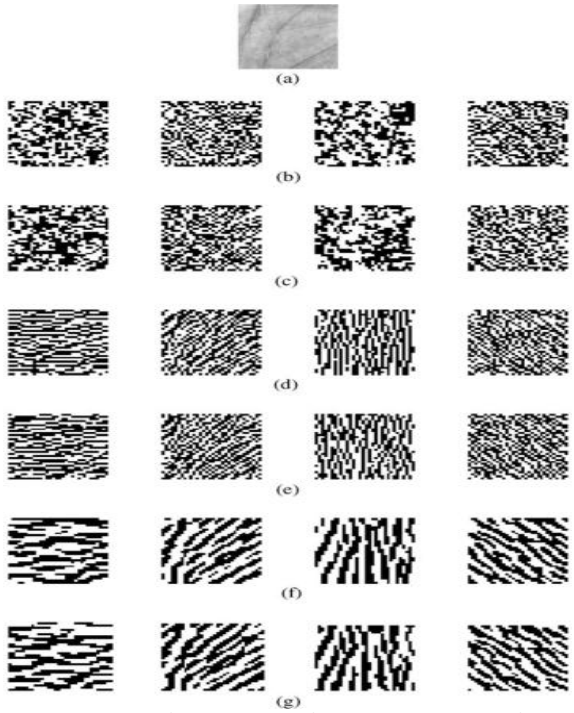



Fig. 3. Original image of palm and their features obtained by 12 filters listed in the Table: (a) original image, (b), (d) and (f) real parts of features from Levels 1–3 filters, respectively, (c), (e) and (g) imaginary parts of from Levels 1–3 filters, respectively.

### *C. Speech feature extraction using Mel Frequency Cepstrum Coefficients (MFCC)*

Speech recognition can be done by observing the given speech signal. The compact representation of the speech signal is provided by the feature vectors. By computing the sequence of these feature vectors, features extraction can be done in Automatic Speech Recognition. Computation of the sequence of the feature vectors can be performed in three main stages. In first stage, speech signal under goes for spectra-temporal analysis to generate raw features that are describing the envelope of the power spectrum for short speech intervals. This process is called the speech analysis or the acoustic front-end. The extended feature vector formed by the two types of features that are static and dynamic, are gathered in second stage. In the final stage, the extended feature vectors are transformed into more compact and robust vectors. Then finally those vectors are fed to the recognizer.

MFCC is the most famous and reliable feature extraction technique for speech recognition. The frequency bands are stored as logarithmic values in MFCC. So that it can estimate the human system response more relatively than any other system. The frequency bands in Mel - frequency cepstrum are spread evenly on the Mel scale and MFCC can be obtained from Mel - frequency cepstrum. MFCC vector can be calculated from each frame and this is based on the short term analysis. The following formula is used to calculate MFCC

$$\text{Mel}(f) = 2595 * \log_{10}(1 + f/700)$$

The steps involved in MFCC feature extraction are as shown in the following figure.

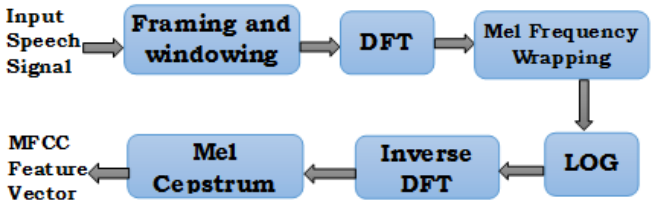



Figure.4 MFCC Feature extraction stages

## III. FEATURE LEVEL FUSION

In Feature level fusion, different feature sets that are extracted from multiple biometric are fused. If the feature sets are distinct (e.g., the feature are extracted from different biometric modalities like fingerprint, palm print and speech) combine them to form a single feature set. Or if feature sets that contain different samples which are extracted by using the same feature extraction algorithm and from the same biometric trait, then it can be defined as a template update or template improvement. It increases the correctness of the feature recognition compared to the other fusion technique. In this research, the stored template was converted in to the fused matrix. In that fused matrix, Feature level fusion technique was implemented. Later it was compared with the fused matrix of the present query.

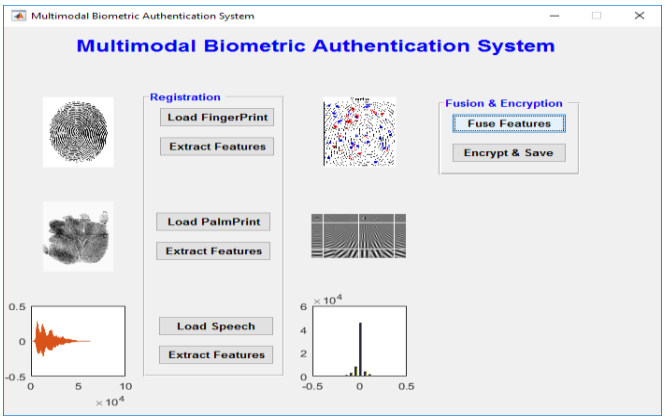



Fig. 5 Steps of Feature Level Fusion

## IV. MODIFIED DRSA (MDRSA)

The multimodal biometric system means an individual information was extracted from the multiple traits. As the information was taking from different sources, it is needed to keep the template secure from the database. So, to secure the template, RSA public key cryptographic algorithm is used to encrypt the template in the proposed system. When compared with the prevailing RSA method, to achieve acceptable reputation of the decrypted image, by using the symmetry properties of the algorithm, the adjustments had done in the decryption stage of RSA. The following steps

© 2017, IJCSE All Rights Reserved 

explain about the MDRSA (Modified Decrypted Rivest, Shamir and Adleman):

*A. Key Generation:*

1. Choose two different prime numbers p and q.
2. Calculate n such that n = p*q. (n is used as the modulus for both the public and private keys).
3. Calculate the quotient of n, Φ (n) Where, Φ (n) = (p-1) (q-1).
4. Calculate an e such that 1 < e < Φ(n), and such that e and Φ(n). (e and Φ(n) are relatively prime). Where 'e' is kept as the public key exponent.
5. Calculate (using modular arithmetic) which satisfies the congruence relation. d= 1 (mod Φ (n)).

This is commonly computed using the Extended Euclidean Algorithm. e and Φ(n) are relatively prime and d is to be the modular multiplicative inverse of 'e'.

The public key has modulus n and the public (or encryption) exponent. The private key has a modulus 'n' and the private (or decryption) exponent 'd', which is kept secret.

*B. Encryption:*

1. Person "A" transmits his/her public key (modulus n and exponent e) to Person B, keeping his/her private key secret.
2. When Person" B" wishes to send the message "M" to Person A, he first converts M to an integer such that 0 < m < n by using agreed upon reversible protocol known as a padding scheme.
3. Person B computes, with Person A's public key information, the cipher text c corresponding C ≡ me (mod n)
4. Person B now sends message "M" in cipher text, or C, to Person A.

*C. Decryption:*

1. Person A recovers m from c by using his/her private key exponent, d, by the computation $m \equiv C^d \pmod n$.
2. Given m, Person A can recover the original message "M" by reversing the padding scheme.
   a. $C \equiv m^e \pmod n$,
   b. $C^d \equiv (m^e)^d \pmod n$
   c. $C^d \equiv m^{de} \pmod n$.
3. By the symmetry property,
   a. $m^{de} \equiv m^{de} \pmod n$.
   b. Since de = 1 + kΦ (n), we can write
   c. $m^{de} \equiv m^{1 + k\Phi(n)} \pmod n$,
   d. $m^{de} \equiv m(m^k)^{\Phi(n)} \pmod n$
   e. $m^{de} \equiv m \pmod n$

From Euler's Theorem, we can show that this is true for all 'm' and the original message

$C^d = m \pmod n$, is obtained.

## V. SIMULATION RESULTS

The GUI in MATLAB is used to design the security level of the proposed multimodal biometric system. At first, three biometric traits fingerprint, palm print and speech are considered for multimodal fusion. The feature extractions of fingerprint, palm print and speech are done using different techniques like minutia extraction, Gabor feature extraction and MFCC method respectively and then they are fused using feature level fusion. The combined features are then encrypted using RSA encryption algorithm. The steps involving in this process are shown in Fig. 6.

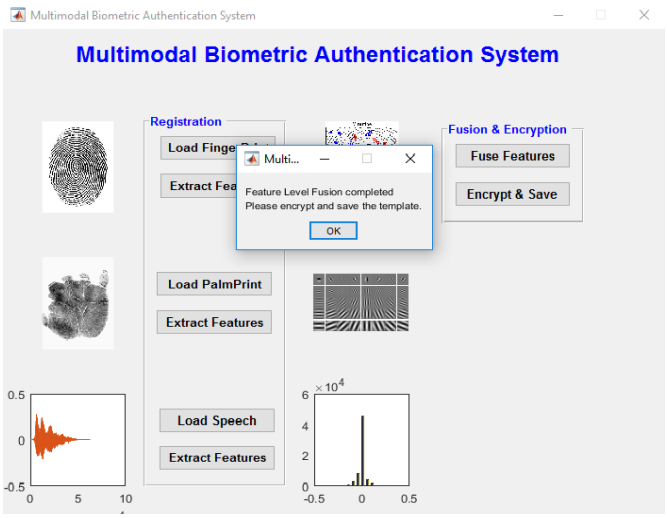



Figure. 6 Encryption of Fused Biometric

Then the encrypted feature extractions are stored in the database and then the decrypted image is coordinated with the current query. The simulation model is developed after each biometric trait such as fingerprint, palm print and speech are trained with unimodal identity.

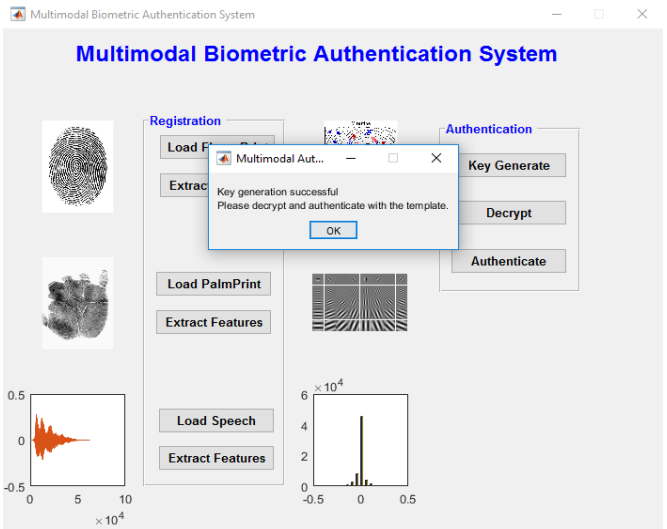



Fig. 7 process of Key generation

© 2017, IJCSE All Rights Reserved 

For both unimodal and multimodal biometric systems, and using RSA and without using RSA, False Acceptance Rate (FAR) and Genuine Acceptance Rate (GAR) are computed depending upon the matching performance. The system has to yield keys for query user when the verification is essential for the system. This was shown in Fig. 7.

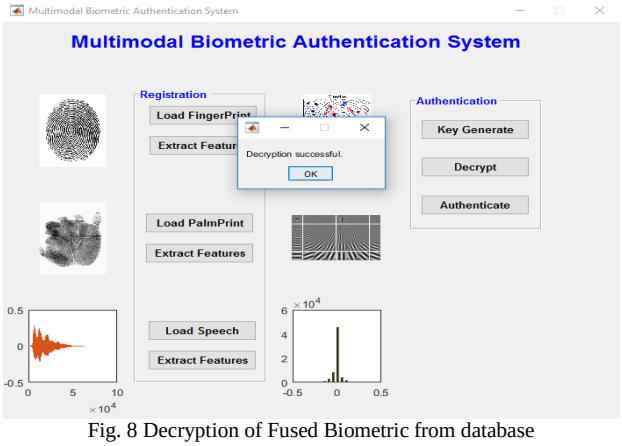



Fig. 8 Decryption of Fused Biometric from database

The produced key is used to decrypt the template after it was searched in the database for matching. The decrypted template is used to match with current query where the current query is a fusion of three biometric traits fingerprint, palm print and speech based on fused matrix values using correlation as in Fig.8 and Fig.9.

When the query template is compared with the stored template, if they are not matched, system reject the request of user to access the database as shown in Fig. 10. To analyze the performance of identifying an individual's authorization of the proposed system, the performance of the enrollment module and that of the verification module for the current query template are compared.

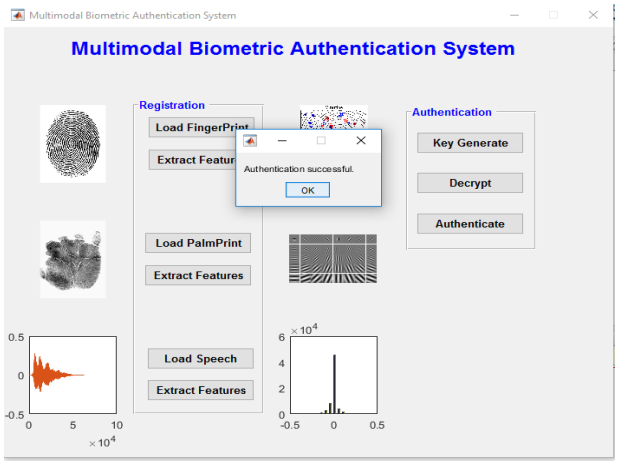



Figure. 9 Process of Matching and Verification

False acceptance rate and genuine acceptance rate are computed depending upon the genuine and fraud authentication during a verification module. The false acceptance rate defines about the fraud user allowance in authentication and it should be low. Whereas genuine acceptance rate defines about the genuine user allowance and it should be high. The performance of multi-modal was compared with uni-modal and then a plot was drawn on ROC curve FAR versus GAR.

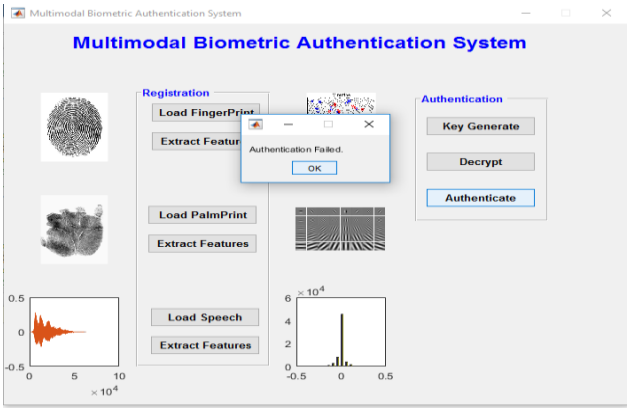



Figure. 10 Access Denied by the system

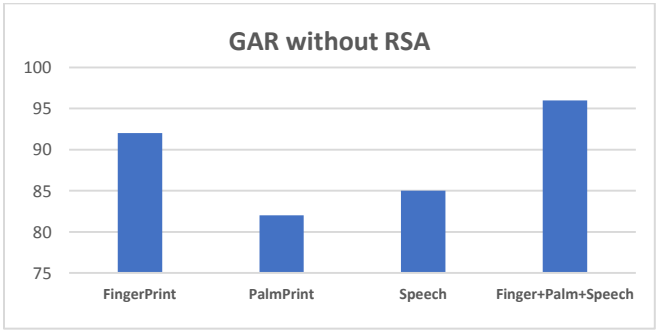



Fig.11 GAR without RSA

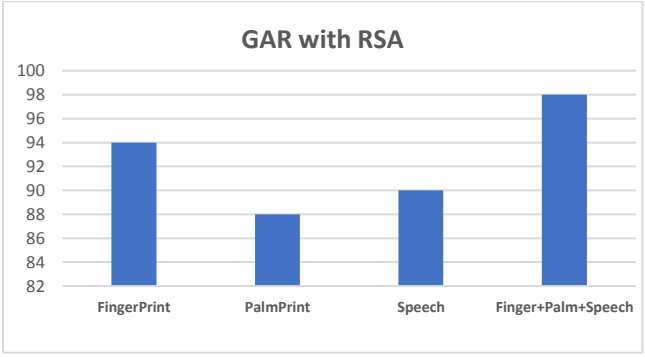



Fig. 12 GAR with RSA

The samples of unimodal biometric traits such as fingerprint, palm print and speech are trained without RSA and then multimodal biometric trait such as fingerprint, palm print and speech was also implemented using feature level fusion techniques without RSA. The fingerprint was trained and performance was calculated based on matching minutiae points with current query for an identity using FAR and

© 2017, IJCSE All Rights Reserved 

GAR. GAR of 92% and FAR of 8% for fingerprint. Similarly, the palm print was and its GAR of 82% and FAR of 18%. The speech was trained and its GAR of 85% and FAR of 15%. The multimodal biometric was trained based on fused matrix values using correlation and its GAR of 96% and FAR of 4%. Figure 11 depicts the GAR performance without RSA in the graphical format and figure 13 depicts FAR performance without RSA.

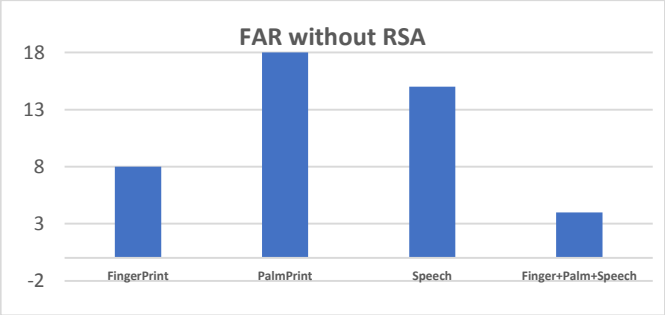



Figure. 13 FAR without RSA

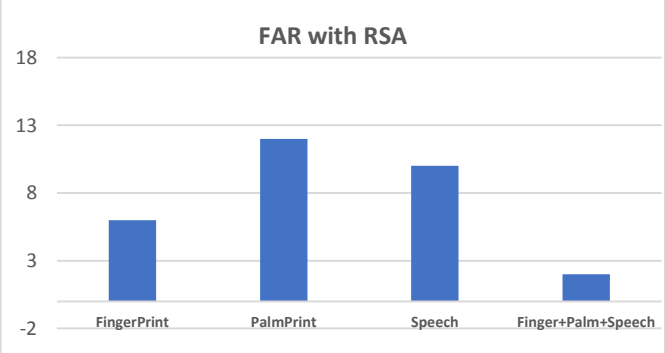



Figure. 14 FAR with RSA

The samples of unimodal biometric traits such as fingerprint, palm print and speech are trained with RSA and then multimodal biometric trait such as fingerprint, palm print and speech was also implemented using feature level fusion techniques with RSA. The fingerprint was trained and performance was calculated based on matching minutiae points with current query for an identity using FAR and GAR. GAR of 96% and FAR of 4% for fingerprint. Similarly, the palm print was and its GAR of 88% and FAR of 12%. The speech was trained and its GAR of 90% and FAR of 10%. The multimodal biometric was trained based on fused matrix values using correlation and its GAR of 98% and FAR of 2%. Figure 12 depicts the GAR performance with RS in the graphical format and figure 14 depicts the FAR performance with RSA.

We can clearly observe from figures 11, 12, 13 and 14, there is a clear improvement in the GAR using RSA than GAR without RSA. There is a reduction in FAR using RSA than FAR without RSA. The performance of finger print using RSA has a GAR of 94% and FAR of 6%, whereas without RSA, GAR was 92% and FAR was 8%. The comparative curves were shown in Fig.12. The performance of multimodal biometric (fusion of fingerprint, palm print and speech) based on fused matrix values using RSA has a GAR of 96% and FAR of 4% whereas without RSA, GAR was 92% and FAR was 8%. The comparative curves were shown in Fig.14. However, in order to increase the accuracy of multimodal biometric as a whole, fusion at feature level fusion, and encrypting using security algorithm has been performed.

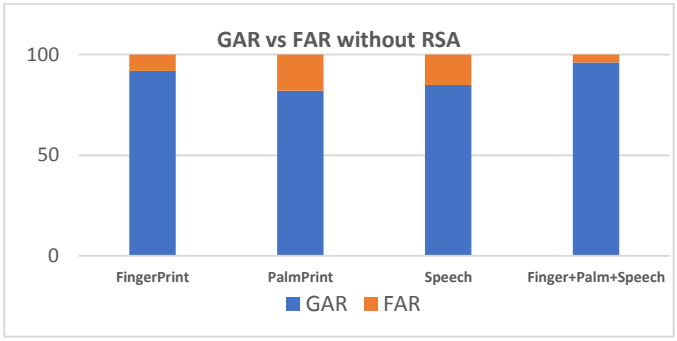



Figure. 15 GAR vs FAR without RSA

The overall performance of multi-modal system has reduced FAR of 2% and increases GAR of 2%, respectively, and its performance compared to unimodal biometric systems such as fingerprint, palmprint and speech with RSA. The performance of multimodal biometric based on fused matrix values using RSA have GAR of 98% and FAR of 2%, RSA with fingerprint have GAR of 94% and FAR of 6%, RSA with palm print have GAR of 88% and FAR of 12%, RSA with speech have GAR of 90% and FAR of 10%. Figure 15 and 16 clearly depicts the GAR versus FAR without and with RSA applied. It is clear that multimodal biometric traits such as fingerprint, palmprint and speech using RSA, has increased the GAR performance and reduced the FAR.

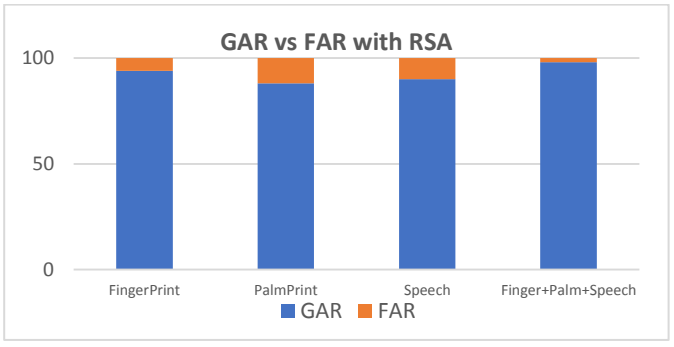



Figure. 16 GAR vs FAR with RSA

## VI. CONCLUSION

The feature level fusion technique is used for the design of multimodal biometric traits such as fingerprint, palm print and speech, which protects the multiple templates using RSA has been implemented using MATLAB. A realistic security

© 2017, IJCSE All Rights Reserved 

analysis of the multimodal biometric cryptosystem has also been conducted using fingerprint, palm print and speech, which provide a remarkable improvement performance in a multimodal biometric cryptosystem using RSA. The overall performance of multimodal system has increased with GAR by 98% and reduced with FAR of 2%, which is compared to unimodal biometric using RSA.

## REFERENCES


[1] Nirmala Saini, Aloka Sinha, "*Face and palmprint multimodal biometric systems using Gabor–Wigner transform as feature extraction*", Pattern Analysis Applications, Vol.18, pp 921–932, 2015.

[2] Mohsen Tabejamaat, "*Selective Algorithm Outline (SAO); An Alternative Approach for Fusing Different Palm-Print Recognition Algorithms*", Neural Process Letters, vol 43, pp 709–726. 2016.

[3] Nadia Nedjah1·Rafae, Soares Wyant, Luiza de Macedo Mourelle, "*Efficient biometric palm-print matching on smart-cards for high security and privacy*", Multimed Tools Applications, December 2016.

[4] Samik Chakraborty, Madhuchhanda Mitra, Saurabh Pal, "*Biometric analysis using fused feature set from side face texture and electrocardiogram*", IET Science, Measurement & Technology, Vol.11 Issue.2, pp. 226-233, 2017.

[5] Edlira Martiri, Marta Gomez-Barrero, Bian Yang, Christoph Busch, "*Biometric template protection based on Bloom filters and honey templates*", IET Biometrics, Vol. 6 Iss. 1, pp. 19-26, 2017.

[6] Panagiotis Moutafis, Ioannis A. Kakadiaris, "*Can We Do Better in Unimodal Biometric Systems? A Rank-Based Score Normalization Framework*", IEEE Transactions On Cybernetics, Vol. 45, No. 12, pp 2654-2668, December 2015.

[7] Yunlian Sun, Kamal Nasrollahi, Zhenan Sun, Tieniu Tan, "*Complementary Cohort Strategy for Multimodal Face Pair Matching*", IEEE Transactions On Information Forensics And Security, Vol. 11, No. 5, pp 937-951, May 2016.

[8] Mohammad Haghighat, Mohamed Abdel-Mottaleb, Wadee Alhalabi, "*Discriminant Correlation Analysis: Real-Time Feature Level Fusion for Multimodal Biometric Recognition*", IEEE Transactions On Information Forensics And Security, Vol. 11, No. 9, pp 1984-1997, September 2016.

[9] L. Mezai and F. Hachouf, "*Score-Level Fusion of Face and Voice Using Particle Swarm Optimization and Belief Functions*", IEEE Transactions On Human-machine Systems, Vol. 45, No. 6, pp 761-773, December 2015.

[10] Kien Nguyen, Simon Denman, Sridha Sridharan, Clinton Fookes,"*Score-Level Multibiometric Fusion Based on Dempster–Shafer Theory Incorporating Uncertainty Factors*", Ieee Transactions On Human-machine Systems, Vol. 45, No. 1, pp 132-141, February 2015.

[11] Muhtahir O. Oloyede, Gerhard P. Hancke, "*Unimodal and Multimodal Biometric Sensing Systems: A Review*", IEEE Access, pp 7532-7555, November 2016.

[12] K. G. Srinivasa, Soumya Gosukonda, "*Continuous multimodal user authentication: coupling hardand soft biometrics with support vector machines to attenuate noise*", CSIT, CSI Publications, pp 129-140, September 2014.

[13] Hataichanok Saevanee, Nathan L. Clarke, and Steven M. Furnell,"*Multi-modal Behavioural Biometric Authentication for Mobile Devices*", IFIP International Federation for Information Processing, pp 465-474, 2012.

[14] Manjunathswamy B E, Appaji M Abhishek, Thriveni J, Venugopal K R, L M Patnaik, "*Multimodal Biometric Authentication using ECG and Fingerprint*", International Journal of Computer Applications, Volume 111 – No 13, pp 33-40, February 2015.

[15] M. Indovina, U. Uludag, R. Snelick, A. Mink, A. Jain, "*Multimodal Biometric Authentication Methods: A COTS Approach*", International Journal of Computer Science and Network Security, pp 1-7, March 2009.

[16] Anushri Chourasiya, Rakesh Pandey, "*A Review on Touch-less Biometric Fingerprint Authentication*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.7, pp.88-91, 2017.

[17] A. Annis Fathima, S.Vasuhi, N.T.Naresh Babu, V.Vaidehi, Teena Mary Treesa,*"Fusion Framework for Multimodal Biometric Person Authentication System*", International Journal of Computer Science, February 2014.

[18] Mohamed Soltane and Mimen Bakhti, "*Multi-Modal Biometric Authentications: Concept Issues and Applications Strategies*", International Journal of Advanced Science and Technology Vol. 48, pp 23-60, November, 2012.

[19] M. Yadav, A. Aalam, "*Five Stage Dynamic Time Warping Algorithm for Speaker Dependent Isolated Word Recognition in Speech*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.10, pp.112-115, 2016.

[20] S. Mewada, P. Sharma, and S. S. Gautam, "*Investigation of Efficient Cryptic Algorithm for Text using SM Crypter*," International Journal of Information Science and Computing, vol. 3, no. 2, p. 99, 2016.

[21] Namrata Dave, "*Feature Extraction Methods LPC, PLP and MFCC In Speech Recognition*", International Journal For Advance Research In Engineering And Technology, Volume 1, Issue VI, pp 1-5, July 2013.

[22] Nadira T., Rehna K., Fepslin Athish Mon, "*A Study and Analysis on Feature Extraction in Content-Based Image Retrieval*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.6, pp.305-307, 2017.

[23] Wai Kin Kong, David Zhang, Wenxin Li, "*Palmprint feature extraction using 2-D Gabor filters*", Pattern Recognition, V.l 36, pp 2339–2347, 2003.


### Authors Profile

**T. Srinivasa Rao**, Professor & TPO in Vasireddy Venkatadri Institute of Technology and Research scholar of Acharya Nagarjuna University, Guntur. He did his Master of Technology in Computer Science Engineering. He also did Mater of Science (Tech)in Mathematics from JNTU, Hyderabad. His research areas of interest are in various domains including Digital Image Processing.

**Dr. E. Srinivasa Reddy**, Professor & Dean R&D in University Engineering College of Acharya Nagarjuna University. He did Master of Technology in Computer Science Engineering from sir Mokhsagundam Visweswariah University, Bangalore. He also did Mater of Science from Birla Institute of Technological Sciences, Pilani. He did Philosophical Doctorate in Computer Science Engineering from Acharya Nagarjuna University, Guntur. Prof.E.S.Reddy, guided successfully more than twenty research scholars for PhD degree. His research areas of interest are in various domains including Digital Image Processing.

© 2017, IJCSE All Rights Reserved 