RSA Algorithm Based On Fingerprint Traits

[1]Sona K.H.
[1]Computer science and Engineering,
[1]Vidya Academy of Science and Technology ,Thrissur,India

***Abstract*—The Fingerprint RSA system deals with modern computing systems securityissues, focusing on biometric based asymmetric keys generation process. ConventionalPKI systems are based on private/public keys generated through RSA orsimilar algorithms. Fingerprint trait (Minutiae points and Core and Delta points),one of the most selective physiological feature has been integrated in the RSAalgorithm for biometric based public/private keys generation. In addition the correspondingprivate key depends on physical or biometric features and it can begenerated when it is needed.Afterthe acquisition of fingerprint, the biometric identifieris extracted, and the keys are generated. Biometric information is then usedfor user authentication and for public/private keys generation. The asymmetrickeys generation distinctive power depends on biometric authentication accuracy,assuring unique asymmetric keys for each authenticated user.**

***Index Terms*— Fingerprint RSA system, PKI systems, Fingerprint trait, Biometric.**

I. INTRODUCTION

Cloud computing, large scale systems, Ambient Intelligence(a vision on the futureof consumer electronics, telecommunication and computing) are based on opensystems and platforms designed for deliver services addressing user needs andwants. These systems/platforms and their applications require high levels of security,such as user authentication, user action monitoring, secure communication,and environment protection. Cryptography and biometrics play a key role in securityapplications. Biometric Cryptosystems (BCSs) indicates systems designedto securely bind a digital key to user biometric information or generate a digitalkey from a biometric trait.

The RSA cryptography is one of the well known public-key cryptosystem that offers both encryption and digital signatures (authentication). The RSA cryptosystem is the de facto standard for public-key encryption and signature worldwide. It is implemented in the most popular security products and protocols in use today, and can be seen as one of the basis for secure communication in the Internet.

Among all the biometric techniques, today fingerprints are the most widely usedbiometric features for personal identification because of their high acceptability,Immutability and individuality. The general shape of the finger print is generally used to pre-process the images. The first scientific study of figure print was made by Galton who divided thefigure print into 3 classes.ie Loop, whorl and arch. Here fingerprint is used as a biometric parameter for generation of encryptionkey. Fingerprints have been used for over a century and are the most widely usedform of biometric identification. The fingerprint of an individual is unique andremains unchanged over an individual's lifetime. A fingerprint is formed from an
impression of the pattern of ridges on a finger. A ridge is curved line on the fingerprint. Valley is the regionbetween two adjacent ridges. The set of minutiae types are restricted into onlytwo types, ridge endings and bifurcations, Ridge endings are the points where theridge curve terminates, and bifurcations are where a ridge splits from a single pathto two paths at a Y-junction.

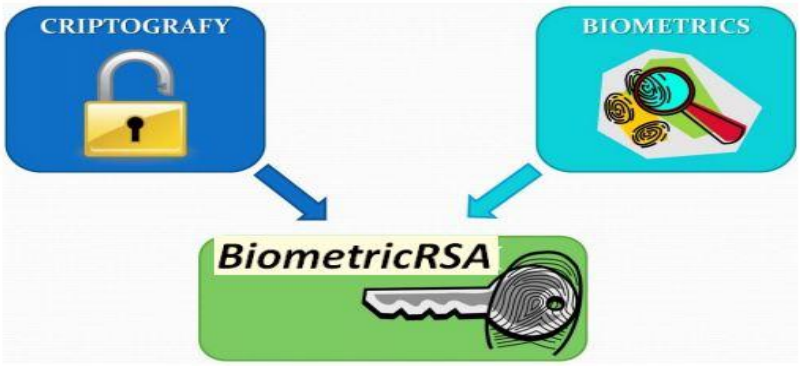


Fig 1.Fingerprint RSA System

II. SYSTEM ARCHITECTURE

The Fingerprint RSA system is applied in such a way that the enhanced fingerprint is given as input to the Minutiae Extractor or Core and Delta point Extractor. Output of Extractor is the list of Minutiae Co-coordinators or Core and Delta point Co-coordinators, which is given as input to the RSA Algorithm. It generates the Fingerprint based key. The Fingerprint RSA system contains secure communication between selected two users before examinining valid users by fingerprint matching through minutiae points plus core and delta points and core and delta points individually.The user send his public key to another user for starting communication. Then user is encrypting message using public key and decrypted by private key. At the end of communication they are exited from stage, and the private key is destroyed after communication.Fig 2 shows System Architecture.

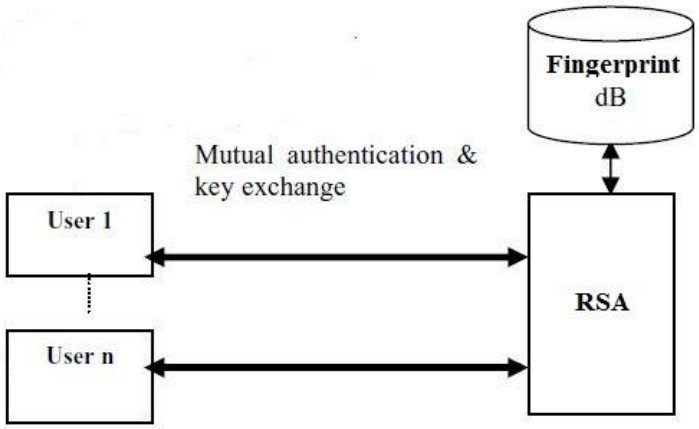


Fig 2. System Architecture

The Fingerprint RSA system is composed of two main modules: the fingerprintauthentication module and the asymmetric cryptography module. Thefingerprint authentication module is based on unimodal approach using Core andDelta points plus Minutiae points and their frequency encoding. The asymmetric cryptography moduleimplements the well-known RSA algorithm. The first module deals with biometricidentifier extraction and user authentication. The second module deals withthe public/private pair generation integrating the extracted biometric identifier.

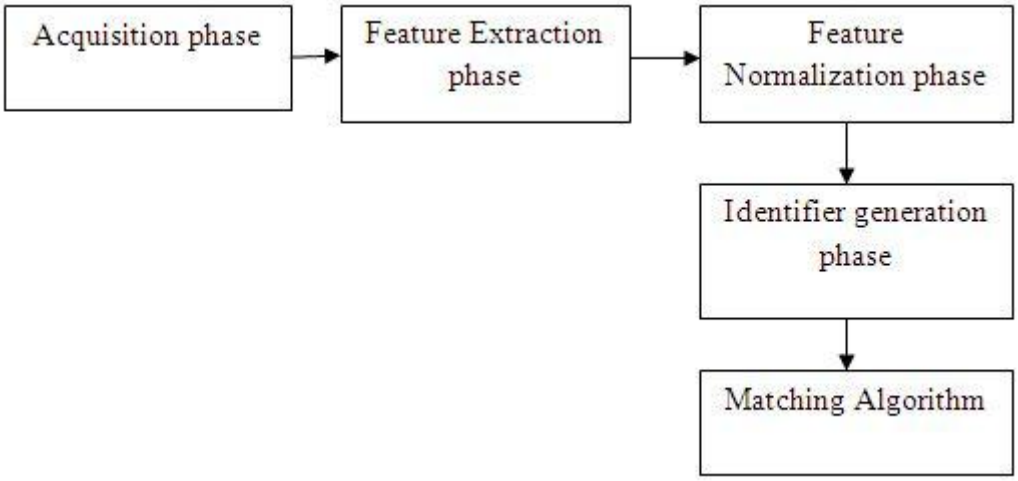


Fig 3.Fingerprint Authentication Module

Fingerprint Authentication Module

The first module deals with biometric identifier extraction and user authentication as shown in Fig 3.

A. Acquisition phase

The acquisition phase deals with fingerprint image acquisition, while the remaining phases deal fingerprint processing and matching.

B. Feature Extraction phase

Among the variety of minutia types reported in literature, two are mostly significant and in heavy usage: one is called termination, which is the immediate ending of a ridge; the other is called bifurcation, which is the point on the ridge from which two branches derive.

After a fingerprint image has been enhanced, the next step is to extract the minutiaefrom the enhanced image. The most commonly employed method of minutiaeextraction is the Crossing Number (CN) concept. Two fingerprints are superimposedand correlation between corresponding pixels is computed for differentalignments.

The core point is the center of a circular edge patternon a fingerprint image, and the delta point is the center of a triangular edge pattern. Core and Delta extraction phase is performed by checking the Poincare indexes associated with the fingerprint direction

matrix. The singularity points with a Poincare index equal to 180, 180, 360 are associated with the Core, the Delta and the double Core, respectively.

C. Feature Normalisation phase

Since the fingerprints of different people may have different sizes, a normalizationoperation must be performed after extraction phase.

D.Identifier Generation phase

After fingerprint regions normalized phase, they are codified using the Log-Gabor approach. This filter, an alternative more performance respect to Gabor filter, can be designed with arbitrary bandwidth and it represents a Gabor filter constructed as a Gaussian on a logarithmic scale.

E.Matching

The matching score is calculated through the Hamming distance calculation betweentwo final identifiers. The template obtained in the identifier generationprocess will need a corresponding matching metric that provides a measure of thesimilarity degree between the two identifiers.

Asymmetric cryptography module

The secondmodule deals with the public/private pair generation integrating the extracted biometricidentifier.In the RSA encryption algorithm, p and q, necessary for the public and privatekeys calculation, are obtained from a random fixed length numbers algorithm.Forlarge prime number lookup table generation any kind of random number generationmethod can be used. Matlab Contains an inbuilt function called primes usedto generate prime number within a limit. For making it into random order sort itaccording to a random index.The index for selecting p and q from Look up tableis obtained from identifier generation phase.It is done in two manners as shown in Fig 4 and Fig 5.

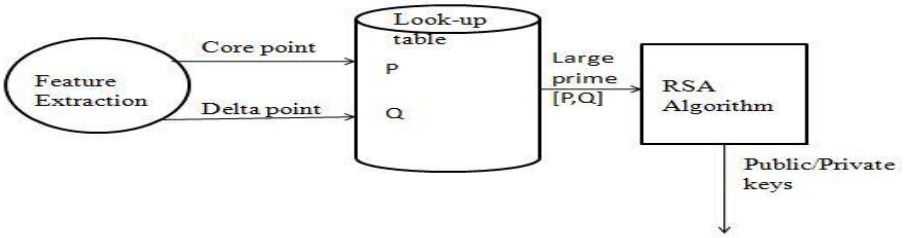


Fig 4.The private/public keys pair generation using Core and Delta point.

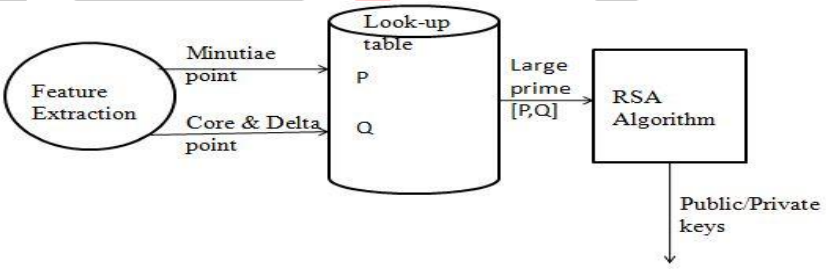


Fig 5.The private/public keys pair generation using Minutiae plus Core and Delta points.

III. SIMULATION AND RESULT

A. Performance metrics

Confusion matrix for VAT with Kmeans algorithm

Predicted Classes	Actual Classes 0	Actual Classes 1
1	87.0	19.0
2	12.0	82.0

	Actual Classes 0	Actual Classes 1
True Positive	87.00	82.00
False Positive	19.00	12.00
False Negative	12.00	19.00
True Negative	82.00	87.00
Precision	0.82	0.87
Recall or Sensitivity	0.88	0.81
Specificity	0.81	0.88

Model Accuracy is 0.84

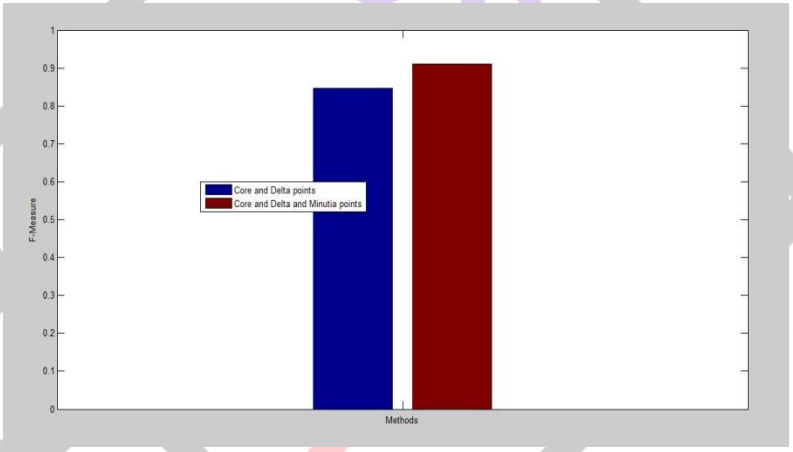
Confusion matrix for SpecVAT with Kmeans algorithm

Predicted Classes	Actual Classes 0	Actual Classes 1
1	89.0	8.0
2	10.0	93.0

	Actual Classes 0	Actual Classes 1
True Positive	89.00	93.00
False Positive	8.00	10.00
False Negative	10.00	8.00
True Negative	93.00	89.00
Precision	0.92	0.90
Recall or Sensitivity	0.90	0.92
Specificity	0.92	0.90

Model Accuracy is 0.91

B. Performance graph



The experimental trials have been conducted on o Database containing169 fingerprints .A confusion matrix (Kohavi and Provost, 1998) contains informationabout actual and predicted classifications done by a classification system.Performance of such systems is commonly evaluated using the data in the matrix.The fingerprint authentication performance has been evaluated using actual valuewith predicted value obtained from algorithm. Actual classes are obtained from itand model accuracy is calculated.

IV.CONCLUSION

The Biometric Authentication and key exchange system together with itspractical applications offers many appealing performance features. The salientfeatures of system make it a suitable candidate for number of practical applicationslike Biometric ATMs and in future, Biometric online web applications etc.Compared with previous solutions, Fingerprint RSA system possesses many advantages,such as the secure against dictionary attack, avoidance of PKI, and highefficiency in terms of both computation and communications.In the system, fingerprint traits have been integrated in the RSA algorithm todevelop a new asymmetric cipher system. Unlike conventional PKI systems, thesystem allows private/public keys generation in different time.

V.FUTURESCOPE

Future works are aimed at increase the number of users and extend the system to several distinctive biometric traits.

Acknowledgement

First of all, I am grateful to The Almighty God for establishing me to complete this project.I am especially thankful to my guide Assistant. ProfessorMrs.AyanaAjith.,M.Tech.,and all other faculty members from the Department of Computer Science and

Engineering, for giving me their sole co-operation and encouragement and criticalinputs in the preparation of this report.Finally I express my heartfelt thanks to our Lab Instructors, colleagues, friendsand my dear Parents for giving me valuable advice and support throughout myproject work.

REFERENCES

[1] Christian Rathgeb, Andreas Uh, A survey on biometric cryptosystems andcancelable biometrics, EURASIP Journal on Information Security 2011,2011:3, http://jis.eurasipjournals.com/content/2011/1/3
[2] Kai Xi, Jiankun Hu, Bio-Cryptography, Handbook of Information and Communication,Peter Stavroulakis,Mark Stamp (Eds.) Security, pp. 129-157,Springer 2010
[3] FengHao, Ross Anderson, John Daugman, Combining cryptography withbiometrics effectively, Technical Report No. 640, 2005, UCAM-CL-TR-640, ISSN 1476-2986
[4] SP.Venkatachalam, P.MuthuKannan, V.Palanisamy, Combining Cryptographywith Biometrics for Enhanced Security, International Conference onControl, Automation, Communication and Energy Conservation, INCACEC2009, pp. 1-6, ISBN: 978-1-4244-4789-3
[5] A. Jagadeesan, T. Thillaikkarasi, K. Duraiswamy, Cryptographic Key Generationfrom Multiple Biometric Modalities: Fusing Minutiae with Iris Feature,International Journal of Computer Applications (0975 8887) Vol. 2No.6, pp. 16-26, June 2010
[6] C. Militello, V. Conti, S. Vitabile and F. Sorbello, ”Embedded Access Pointsfor Trusted Data and Resources Access in HPC Systems”, The Journal ofSupercomputing - An international journal of High- Performance ComputerDesign, Analysis and Use, Springer Netherlands Publisher, 2010,ISSN 0920-8542, Vol. 55, N 1, pp. 4 - 27, (ISSN Online 1573-0484), doi:10.1007/s11227-009-0379-1
[7] V. Conti, C. Militello, S. Vitabile and F. Sorbello, ”A Multimodal Techniquefor an Embedded Fingerprint Recognizer in Mobile Payment Systems”, International Journal on Mobile Information Systems - Vol. 5, No. 2, 2009, pp.105-124, IOS Press Ed., ISSN: 1574-017X, doi:10.3233/MIS-2009-0076