A New Palm Print Based Fuzzy Vault System for Securing Cryptographic Key

Om Prakash Verma and Devesh Bharathan

Abstract—**Biometric unique authentication approach on encrypted message provides a totally secured information delivery without any need to hide any password or secret key. We present the usage of biometrics technique in asymmetric cryptographic domain where we protect secret key involved in cryptographic with the help of fuzzy vault created by randomizing the palm print feature with the secret key. This paper therefore uses the polynomial construction on the secret key using appropriate mapping function and taking the projection of palm print feature on the polynomial constructed which together makes the fuzzy vault. Vault can be unlocked with authentication and polynomial is reconstructed using Lagrange's interpolation. Secret key is retrieved from reconstructed polynomial and corrected with Reed & Solomon (RS) codes. The results shows that 309-bit RSA keys can be secured with palm print based fuzzy vault using the proposed system.**

Index Terms— **RSA; Lagrange's interpolation; RS codes; Galois field; PCA technique; Eigen values.**

I. Introduction

Today information security is very sensitive area of research. Cryptography is one of the most effective ways to enhance the security of the information system via its encryption and decryption modules. A secure encryption key can be associated with a biometric signature to ensure the integrity and confidentiality of communication in distributed systems. Many of the limitations of the password and PIN based encryption schemes can be alleviated by using biometric features, which are unique and can be conveniently extracted from every user. The biometric-based encryption requires physical presence of persons to be authenticated and is therefore reliable, convenient and efficient [1]**.** The motivation to protect secret key involved in cryptographic modules using biometric based fuzzy vault is came from the idea that current cryptographic algorithms e.g., Advanced Encryption Standard (AES) [2], Data Encryption Standard (DES) and RSA [3] have a very high proven security but they suffer from the key management problem as all these algorithms fully depend on the assumption that the keys will be kept in absolute secrecy. If the secret key is compromised, the security provided by them immediately falls apart. Another limitation of the these algorithms is that they require the keys to be very long and random for higher security, e.g., 128 bits for AES, which makes it impossible for users to memorize the keys. As a result, the cryptographic keys are stored securely (e.g., in a computer or on a smart card) and released based on some alternative authentication mechanism. If this authentication succeeds, keys can be used in encryption/decryption procedures. The most popular authentication mechanism used for key release is based on passwords. Thus, the plain text protected by a cryptographic algorithm is only as secure as the password (weakest link) that releases the correct decrypting keys. Simple passwords compromise security, but complex passwords are difficult to remember and expensive to maintain. Further, passwords are unable to provide non repudiation; a subject may deny releasing the key using password authentication.

The most remarkable work in this area is to provide cryptography based security at different stages of biometric authentication via fuzzy vault scheme [4]. This vault is a form of error-tolerant cryptographic algorithm and proved very useful in many circumstances, such as fuzzy human factor based authentication systems, where exactness of the unlock key is usually unavailable. It is inherently more reliable than password-based authentication as biometric characteristics cannot be lost or forgotten. Further, biometric characteristics are difficult to copy, share and distribute and require the person being authenticated to be present at the time and point of authentication. Hence, biometrics-based authentication is a potential candidate to replace password-based authentication, either for providing complete authentication mechanism or for securing the traditional cryptographic keys claiming that his/her password was stolen. Many of these limitations of password-based key release can be eliminated by incorporating biometric authentication.

II. Prior Work

Fuzzy vault for information security is not very new concept. It has been used for the number of years by various scientists in research work. Jules and Sudan [5] have proposed the generation of a secure vault using an un-ordered set, to lock any secret inside and referred it as fuzzy vault. The concept of fuzzy vault has been further explored by Uludag *et al*. [1] where they used fingerprint templates as an unordered set to create the vault around the secret. They further utilizes error correcting codes, such as Reed and Solomon code to produce some error tolerance in the input biometric templates, while decrypting the module. Their contribution is to hide any secret in fuzzy vault using polynomial construction under un-ordered set. The secret can

Manuscript received January 25 2012; revised March 8, 2012. This work was supported in part by the Biometric Lab, Indian Institute of Technology Delhi, Summer Internship Program.

Om Prakash Verma is with the Department of Information Technology, Delhi College of Engineering, Delhi, India (e-mail: opverma.dce@gmail.com).

Devesh Bharathan is with the Department of Information Technology, Delhi College of Engineering, Delhi, India (e-mail: devesh.bharathan@gmail.com).

be retrieved back by polynomial reconstruction, if certain points of the unordered set are known at receiving end. The security of the scheme mainly depends upon polynomial construction and reconstruction problem. They have combined the concept of fuzzy vault with biometrics (fingerprint) by using biometric template as an un-ordered set. Uludag and Jain [4] proposed the minutiae based features from the fingerprints for locking and unlocking the vault. They attempted to secure the secret key of any cryptosystem using fuzzy vault. Vault is created by taking projections on fingerprint minutiae features and Cyclic Redundancy Codes (CRC) technique is used for error correction. However, this approach is limited to its usage due to its inability to eliminate the inherent variability in minutiae feature. Nanda kumar *et al.* [6] have attempted to eliminate such variability using helper data and illustrated promising results. Feng Hao *et al*. [7] use iris biometric for generating cryptographic keys and a combination of Reed and Solomon error correcting theories for error tolerance. Clancy et *al*. [8] proposed a smart card based fuzzy vault that employed fingerprints for locking and unlocking. The presumption that acquired fingerprint images are pre-aligned is not realistic and could be the possible reason for high false rejection rate (up to 30.0%) reported in the paper. Lin and Lia [9] have done remarkable work in order to prevent repudiation but their work still required smart card and password for better implementation and hence reduces its usability. Recently, a modified fuzzy vault scheme is proposed by Feng Hao *et al*. [7] using asymmetric cryptosystem. Having generated RSA public and private keys, authors have used Reed and Solomon coding to convert the keys in to codes. Further they used two grids, one for codes and other for biometric features. The elements in the corresponding grids are in same positions. The unlocking of vault only requires the knowledge of the correct positions of the numbers in any of the grids.

Our scheme is inspired from work Fuzzy Vault for Fingerprints in [1] with a number of modifications. The fingerprint features are very difficult to extract from the elderly, laborer, and handicapped users. In compare, we explored the usage of palm print biometric to create fuzzy vault. Having a large surface area palm images are less affected with skin attributes like, amount of grease and dust on the hand of laborers, elderly people and handicapped users as lack of palm is less likely than thumb. A mapping function is suggested to map the secret data (Secret Key of RSA system) to the coefficients of polynomial. PCA technique is used to get most randomized palm feature and projections are taken on this to create the vault. During unlocking, polynomial is reconstructed with Lagrange's interpolation and polynomial coefficients are finally mapped to secret data. In our current encoding implementation, the data is encrypted by RSA cryptosystem, which is represented in Galois Field. And for error correction we have followed RS coding (Reed and Solomon) on these field elements. Firstly, the secret key is mapped to decimal values to form polynomial coefficients. Thereafter the polynomial generated is used for taking projection on the elements of images obtained by PCA technique. Thus the elements and its projection together make the vault.

Decoding implementation is done by comparing elements of another image of user with the vault generated for that user. With the matched values the reverse of encoding methodology is followed with reconstruction of polynomial being done by Lagrange's polynomial reconstruction. And hence the secret key is generated.

III. Proposed Fuzzy Vault System

Fuzzy vault scheme is a simple and novel cryptographic construction. Suppose we have a secret, which we want to share with some specific persons, but do not want to post it indiscriminately, such as a public website. One approach is to compile a set of elements *A* with the secret and publish it in an encrypted form. To extract the secret information, one needs to have an unlocked set *B,* which is close to *A,* to unlock the vault. We have suggested an alternative way of creating a Fuzzy Vault around the secret key of asymmetric cryptosystem. Secret key is mapped to decimal values (with mapping function) to form polynomial coefficients as follows;

$$K = SECRET\ KEY$$
$$X = MAP\ [K]$$

where X is the formed polynomial. Most randomized Palm features data is obtained by PCA technique as follows;

$$P = PALM\ FEATURE$$
$$Q = PCA\ [P]$$

where Q contains most randomized palm features. Projections of Q are taken over X and vault is made up of Q, R and some chaff points (not lying on polynomial X) given as

$$R = EVALUTE[X, Q]$$
$$VAULT = [Q, R] + CHAFF\ POINT$$

For unlocking, the user features are randomized and vault is unlocked with matching them with Q of vault. Polynomial is reconstructed and its coefficients are mapped back to secret key as

$$G = USER\ PALM$$
$$H = PCA\ [G]$$
$$[I, J] = UNLOCK\ [H]$$
$$L = INTERPOLATE\ [I, J]$$
$$SECRET\ KEY = M = INVERSEMAP\ [L]$$

A. Mapping Function

Any generalized injective (one to one) function can be used for mapping since its inverse give unique value. So a better option is to use logarithmic function. Therefore for each 15 characters of secret key, take decimal equivalent of these values and then take log at base 2 to get constant value. Repeat it for entire length of the key and get the polynomial coefficients as follow;

$$K = SECRET\ KEY$$
$$L = GROUP\ [K] \quad (FORM\ THE\ GROUP\ OF\ EACH\ 15\ CHRACTERS\ TO\ DECIMAL\ EQUIVALENT)$$
$$M = LOG\ [L] \quad (TAKE\ THE\ LOG\ AT\ BASE\ 2\ OF\ EACH\ VALUE)$$

where *M* is the constructed polynomial.

B. PCA Mapping

Fuzzy Vault consist the projection of most randomized Palm-Features over the polynomial. The Palm print recognition is done by principal component analysis (PCA) technique to generate most randomized Palm-Feature [10]. Constructed polynomial is evaluated on randomize palm feature which is obtain as follows

P = PALMFEATURE MATRIX (SIZE = 720 X 300)
(DATABASE OF 100 PERSONS)
B = P X P' (SIZE = 720 X 720)
C = EIG (B) (SIZE = 720 X 100) (TAKE 100 EIGEN VECTORS OF B)
Q = C' X P (SIZE = 100 X 300)

P' & *C'* are transpose vectors of *P* & *C* respectively.

where *Q* is the randomized palm feature.

IV. Proposed Algorithm

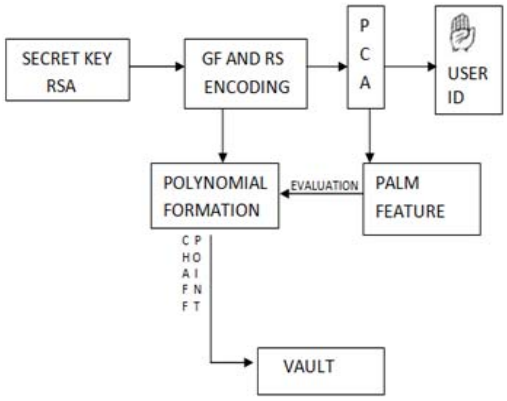

Fig. 1. Block diagram of encoding phase.

A. Locking the Vault (Encoding Phase)

Let *S* be the secret key which is generated using RSA algorithm on the given message. Suppose that *S* be the secret key of 309 characters (i.e. for strength of 512 characters), which is converted in the array format *R*. For the simplicity of our further computation, *R* is padded with some extra redundant number, so that it is of 324 lengths. Now *R* is converted to a two dimensional array *R1* of size "18x18"(square matrix). In the current encoding implementation, the array elements are represented as Galois Field [11], in order to insure that elements are taken in quantized range, so for error correction Reed and Solomon codes are applied. The Galois Field of size (2^5) and the key size is set to 18 (i.e. n = 22, k = 18, m = 5). Now RS coding is performed on Galois Field element to convert it into a two dimensional array *R2* having size (18 x 22). *R2* is converted to a one dimensional double array *A* having 396 (18 x 22) elements and also some redundant elements are padded to *A*. For polynomial formation, considering it to be of degree 26, elements of *A* is divided into groups of 15. As said earlier the mapping logarithmic function is used, therefore $\log_2$ of the decimal value of each of the 27 groups is computed and stored into an array *P1*. These groups are the coefficients of polynomial of order 26.

As discussed earlier, the PCA technique is applied to convert the given data into a (100 x 300) matrix. Using the elements of single image of each user, the projections of each value of x using the polynomial is computed. Now the x values are stored in an array *X1* and the corresponding projection is stored in another array *Y1*. Some randomly generated chaff values are added to *X1* and *Y1*, assuming genuine and chaff points are uniformly distributed. Hence *X1* and *Y1* together makes the vault locked. The scheme for the encoding phase is represented in Fig. 1.

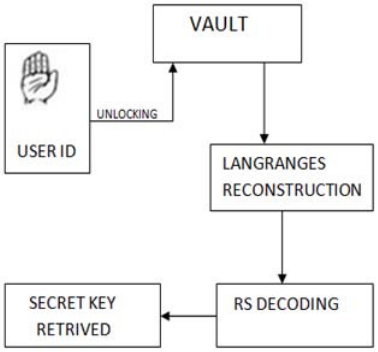

Fig. 2. Block diagram of decoding phase.

B. Unlocking the Vault (Decoding Phase):

The idea for unlocking the vault is conveniently taken by comparing the elements of second image of the user with the vault generated for that user. Now the matched values are stored in an array *W* and the corresponding projection are stored in array in an array *L*. Exactly 27 pairs is formed from *W, L* and the inverse of whole encoding procedure is followed. The Lagrange's reconstruction [12] is followed for polynomial reconstruction. Using the 27 coefficients of this polynomial, all 405 values are recomputed by first finding the anti-log of each coefficient and then getting 15 values each for a coefficient (27 x 15 = 405). These 405 values are stored in array *B1*. The inverse RS decoding is followed on the first 396 values of array *B1* taken in two dimensional array *B2* of size (18 x 22). An array *B3* of size (18 x 18) is generated with the help of RS decoding. Afterwards the secret key *S'* is retrieved from *B3* with length 309. The scheme for the encoding phase is represented in Fig. 2.

V. Experimental Results

The computation requires 37 seconds for a system with a 2.10 GHz dual processor. Further, the system is implemented in Matlab, contributing to high computational times.

The analysis of results (see Table 1) based on the Eigen values shows that false accept rate (FAR) is negligible at lower Eigen values but some significant value at higher Eigen values which can be reduce by taking more samples per user. The results obtained using the proposed method as compared to fingerprint based fuzzy vault is appreciable since we achieved 65% successful unlocking rate for a second image of user from 10 different users while Yang & Verbauwhede *et al*. [13] has given result for fingerprint with 83% successful unlocking rate for 10 prints per finger from 10 different fingers, forming a total 100 fingerprint images.

TABLE I: EXPERIMENTAL RESULTS

S:No	Test performed for Ten user's image:		
	NUMBER OF EIGEN VECTORS TAKEN	***PERCENTAGE OF VAULT UNLOCKED BY IMAGE 2 OF USER***	***PERCENTAGE OF VAULT UNLOCKED FROM IMAGE OF OTHER USER***
1.	50	20%	0%
2.	100	20%	0%
3.	300	30%	10%
4.	600	65%	20%

VI. CONCLUSION

Introduction of biometrics in cryptography domain is really a better option to make system more secure. Thus a secure encryption key can be associated with a biometric signature to ensure the integrity and confidentiality of communication in distributed systems. Many of the limitations of the password and PIN based encryption schemes can be alleviated by using biometric features, which are unique and can be conveniently extracted from every user.

We have shown that performance and security of a palm print based fuzzy vault is better option in comparable to fingerprint fuzzy vault. The experimental results from the proposed approach on the palm print images suggest its possible usage in an automated palm print based key generation system. The proposed method has inherent biometric limitations like adaptation of biometrics is not easily applicable. The proposed system is very critical in terms of precision required for proper implementation. Reconstruction of polynomial of high power with at most accuracy is somewhat very tedious job and method really lags in this phase. Therefore better polynomial formation and precision is challenge in this work.

REFERENCES

[1] U. Uludag1, S. Pankanti, and A. K. Jain1," Fuzzy Vault for Fingerprints," *Springer Berlin/Heidelberg*, vol. 3546, pp. 310-319, 2005.

[2] National Institute of Standards and Technology, *Advanced Encryption Standard(AES),* Federal Information Processing Standards Publication 197, November 26, 2001.[Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[3] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 3. Ed., Prentice Hall.,2002,ch. 1.

[4] U. Uludag and A. K. Jain, "Fuzzy fingerprint vault," in *Proc. Workshop: Biometrics: Challenges Arising from Theory to Practice*, pp. 13-16, Cambridge, UK, Aug. 2004.

[5] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," in Proc. *IEEE Int'l. Symp. Information Theory*, Lausanne, pp. 408, 2002.

[6] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and Performance," *IEEE Trans. Info. Forensics & Security*, vol. 2, no. 4, pp. 744-757, Dec. 2007.

[7] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics efficiently," *IEEE Trans. Computers*, vol. 55, pp. 1081-1088, Sep. 2006.

[8] T. C. Calancy, N. Kiyavash, and D.J . Lin, "Secure Smartcard-based Fingerprint Authentication," *ACM SIGMM , Multimedia Workshop on Biometrics Methods and Applications*, pp. 45-52, 2003.

[9] C. H. Lin and Y. Y. Lai, "A flexible biometrics remote user authentication scheme," *Computer Standards & Interfaces*, vol. 27, no. 1, pp. 19-23, Nov. 2004.

[10] A. Murat and E. Murat, "Kernel Principal Component Analysis of Gabor Features for Palmprint Recognition," *Springer Berlin / Heidelberg*, vol. 5558, 2009.

[11] Great Galois field array−MATLAB. [Online]. Availble: http://www.mathworks.in/help/toolbox/comm/ref/gf.html .

[12] H. Jeffreys and B. S. Jeffreys "Lagrange's Interpolation Formula." Methods of Mathematical Physics, 3rd ed. Cambridge, England: Cambridge University Press, p. 260, 1988.

[13] S. Yang and I. M. Verbauwhede, "Secure fuzzy vault based fingerprint verification system," *IEEE Conference, Signals, Systems and Computer*, vol. 1, pp. 577 – 581, 7-10 Nov. 2004.

[14] A. Kumar and A. Kumar," Development of a New Cryptographic Construct Using Palmprint Based Fuzzy Vault," *EURASIP Journal on Advances in Signal Processing*, 2009.

[15] W. Diffie and M. Hellman, "Multi-user cryptographic techniques," *AFIPS Proceedings* 45, pp 109–112, June 8, 1976.

[16] B. Archer, E. W. Weisstein, Lagrange interpolating polynomial, *MathWorld – A Wolfram Web Resource.*[Online]. Available: http://mathworld.wolfram.com/LagrangeInterpolatingPolynomial.html

Om Prakash Verma received his B.E. degree in Electronics and Communication Engineering from Malaviya National Institute of Technology, Jaipur, India, M.Tech. degree in Communication and Radar Engineering from Indian Institute of Technology (IIT), Delhi, India, and Ph.D. from University of Delhi, Delhi, India. From 1992 to 1998 he was assistant professor in Department of Electronics & Communication Engineering, at Malaviya National Institute of Technology, Jaipur, India. He joined Department of Electronics & Communication Engineering, Delhi College of Engineering (now Delhi Technological University) Delhi, India, as Associate Professor in 1998. Since 2007, he is head of department of Information Technology at Delhi Technological University, Delhi. He is also the author of more than 25 publications in both international journal and conference proceedings. He has guided more than 20 M.Tech. students for their theses. He has authored a book on Digital Signal Processing in 2003. He is a Principal investigator of an Information Security Education Awareness project, sponsored by Department of Information Technology, Government of India. His research interests include image processing, application of fuzzy logic in image processing, application of evolutionary algorithm in signal and image processing. (email:opverma.dce@gmail.com)

Devesh Bharathan was born in Varanasi,India, on January 11, 1989.He received B.E in Information Technology from Delhi College of Engineering (now Delhi Technological University),Delhi,India,in 2011.His reaserch interest are in Information Security and Image Processing.Presently he is working as Software Engineer in Oracle India Pvt Ltd Bangalore. (email:deveshbharathan@gmail.com)