A Palmprint Based Cryptosystem using Double Encryption

Amioy Kumar, Ajay Kumar
Biometrics Research Laboratory
Department of Electrical Engineering, Indian Institute of Technology Delhi
Hauz Khas, New Delhi 110 016, INDIA

Abstract

The combination of cryptology and biometrics has emerged as promising component of information security. Despite the current popularity of palmprint biometric, there has not been any attempt to investigate its usage for the fuzzy vault. This paper therefore investigates the possible usage of palmprints in fuzzy vault to develop a user friendly and reliable crypto system. We suggest the use of both symmetric and asymmetric approach for the encryptions. The cipher text of any document is generated by symmetric cryptosystem; the symmetric key is then encrypted by asymmetric approach. Reed and Solomon codes are then used on the generated asymmetric key to provide some error tolerance while decryption. The experimental results from the proposed approach on the real palmprint images suggest its possible usage in an automated palmprint based key generation system.

1. Introduction

Biometric-based authentication system should be designed to withstand attacks when deployed in security critical applications such as e-commerce and accesses to restricted data/buildings. The biometric-based encryption requires physical presence of persons to be authenticated and is therefore reliable, convenient and efficient. The encryption keys in are generated using low-level combination of biometric features and cryptology. The work detailed in this paper incorporates both symmetric and asymmetric cryptographic approach into the fuzzy vault to ensure higher security and utilize the advantages of both systems in a common domain. Fingerprint identification is widely accepted in most of the cases for personal identification. However, it also has difficulties regarding feature extraction. The fingerprint features are very difficult to extract in the case of elderly peoples, laborers, and handicapped peoples. As a result, other biometric characteristics are receiving increasing attention. Moreover, additional biometric features, such as palmprints, hand geometry can be easily integrated with the existing authentication system to provide enhanced level of confidence in personal authentication.

2. Prior Work

In the fuzzy vault literature, Juels and Sudan [8] have presented a promising model which was an improvement on the prior study by Juels and Wattenberg in [9]. The security of the scheme mainly depends upon polynomial construction and reconstruction problem. Clancy *et al*. [10] 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 (30.0%) reported in the paper. Uludag and Jain [11] proposed to use minutiae based features from the fingerprints for locking and unlocking the vault. However, this approach is limited to its usage due to its inability to eliminate the inherent variability in minutiae feature. Nandakumar *et al.* [2] in their forthcoming paper have attempted to eliminate such variability using *helper data* and illustrated promising results. Lin *et al*. [12] 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. Goh and Ngo [14] use similar technique by extracting Eigen-projections from the face image, as a feature for biometric locking. However for experimental evaluation they have taken images form continuous video source creating doubts about real evaluation. Feng *et al*. [15] use iris biometric for generating cryptographic keys and a combination of RS and Hadamard error correction for error tolerance. Recently, a modified fuzzy vault scheme is proposed in [16] using asymmetric cryptosystem. Having generated RSA public and private keys, they have used Reed and Solomon coding system 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. However, this approach utilizes the asymmetric cryptosystem and has all the problems associated with such systems. Moreover, the database used for the experimental evaluation is too small (9 users) to generate any reliable conclusion on the performance. In summary, different range of biometrics has been used for fuzzy vaults in literature. However, with few notable exceptions, *e.g*. [15], with small false rejection rates, the average FAR of 15% has been cited.

The main contributions of this paper can be summarized as follows. Firstly this paper investigates a new approach for fuzzy vault using palmprint biometric. Secondly, unlike prior work in the literature, this paper proposes a combined cryptosystem which successfully exhibits the advantage of both symmetric and asymmetric cryptography. It may be noted that the asymmetric approach (RSA) for encryption has been estimated to be very slow as compared to tradition asymmetric approach (AES) [5]. Therefore the proposed approach is to use symmetric cryptography to encrypt the entire

document and then we encrypted symmetric key using asymmetric (RSA) approach. The palmprint based fuzzy vault is then constructed around decryption key. Finally, we investigate the performance of the palmprint based cryptosystem on a large dataset and achieve promising results.

3. Proposed System

The objective of this work is to incorporate both symmetric and asymmetric cryptographic approaches into the fuzzy vault in order to ensure higher security and utilize the advantages of both systems in a common domain. We denote it as double encryption. The approach is to use symmetric key approach (DES) for encrypting the secret document and the generated symmetric key is again encrypted by asymmetric approach (RSA). In the next subsections we review the RSA cryptosystem and discuss the proposed approach utilizing the combination of two approaches.

3.1.5. RSA Cryptosystem

A traditional RSA algorithm [21] requires two randomly generated prime numbers [20]. For the security of RSA algorithm, the prime numbers should be bigger (512 bit in our case) and randomly chosen. The algorithm can be briefly summarized as follows:

1. Firstly two large primes k and l are computed such that their product is equal to the required bit size of the key;
2. The products $m = k*l$ and $si = (k\text{-}1)*(l\text{-}1)$ are computed;
3. An integer n, $1 < n < si$ could be chosen such that $\gcd(n, si) = 1$, where gcd represents the greatest common divisor;
4. The secret key sc can be generated by satisfying the modulo

   $n*sc \equiv 1 \pmod{si}$ such that $1 < sc < si$;
5. The public key is (m, n) is made publically available and the private key is (m, sc) kept private. The values of k, l and si are also be kept secret.

Any secret encrypted using public key can only be decrypted by using private key. The main points involved in encryption and decryption are:

Lucie does the following:-

1. Obtains the recipient Bryan's public key (m, n).
2. Represents the plaintext message as a positive integer pt.
3. Computes the ciphertext $ct = pt^{\wedge n} \bmod m$.

4. Sends the ciphertext *ct* to Bryan.

Recipient Bryan does the following:-

1. Uses his private key (*n*, *d*) to compute $pt = ct^{\wedge sc} \bmod m$.
2. Extracts the plaintext from the integer representative *pt*.

Using RSA algorithm, asymmetric cryptosystem can be able to solve a number of problems regarding symmetric cryptographic approach.

3.1.6. The Problems behind RSA

The asymmetric approaches like RSA, DSA, *etc*. are generally known to be slower (about 100 times slower) [5] than symmetric approaches like DES, AES, *etc*. As a conclusion one can argue that the symmetric cryptography is highly suitable for encrypting and decrypting the bulk of messages on data lines. However, the associated problem of providing all the recipients with an advanced copy of secret key can be expensive and hazardous. The insecurity associated with the distribution of all the necessary secret keys to all the recipients on a regular basis is very high. In summary, working with RSA cryptosystem can certainly eliminate several drawbacks associated with symmetric approaches. However, this cryptosystem still has some problems regarding complexity of algorithm as it works very slowly (whenever a bulk data encryption is required) due to the fact that it is mathematically intensive and requires extra management for public keys.

3.1.7. Double Encryption

The solution is to encrypt a mmessage with a fast symmetric algorithm, then encrypt the secret key using asymmetric cryptography and then send it to the recipient. Asymmetric cryptography is slow, but not too slow to encrypt such a small file as a symmetric encryption key. Upon receipt, the recipient can easily use his/her private asymmetric key to decrypt the symmetric key. Further that symmetric key can be used to quickly decrypt the message file. Let *X* denote the dummy message to be encrypted and K_{sim} be the symmetric key, used to encrypt the document. Then

$$Y=K_{sim}(X), T=K_{pub}(Y), Y=K_{pri}(T), X=K_{sim}(Y) \quad (1)$$

For encrypting this message the symmetric key can be generated using DES algorithm. Let the symmetric key is denoted by K_{sim}. Now the generated symmetric key again encrypted by asymmetric approach using RSA algorithm. Let the public and private key associated with the RSA cryptosystem be denoted as K_{pub} and K_{pri}. We will use this generated public key K_{pub} for encryption and the

generated private key K_{pri} for decryption. The equation (1) summarizes the complete procedure. The figure 1 illustrates the complete block diagram and includes key steps in double encryption algorithm. For the traditional RSA cryptosystem, the public key has made publically available while private key has kept private. The cipher text has generated with encryption key publically available while decrypted with private key kept private. The security of system depends upon secrecy of private key.

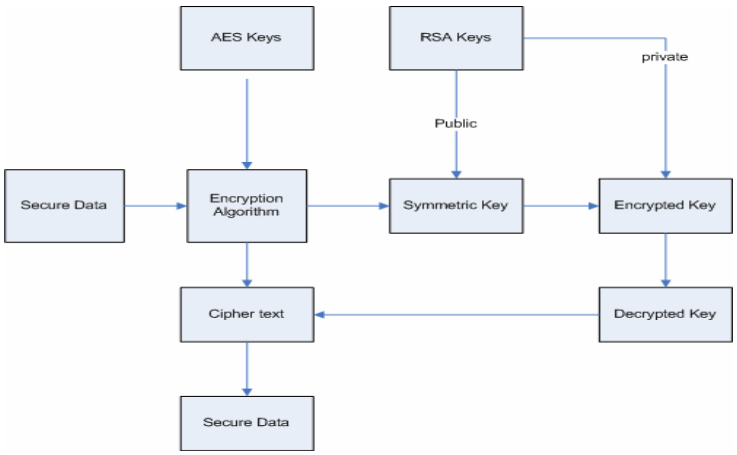


Figure 1: Block diagram for the double encryption

3.2. Palmprint based Fuzzy Vault

One of the key objectives of this work is to investigate the usage of palmprint biometric in the development of a cryptographic construct. The palmprint based cryptosystem can have higher user acceptance and performance. Despite the recent popularity of palmprint based systems [6], [7], [24], there has been not any attempt to investigate its usage for the fuzzy vault. The palmprint literature has cited number of advantages of palmprint biometric; (i) due to large surface area, the region of interest for palmprint is larger as compared to fingerprint and hence more features can be extracted, (ii) the chances of damaged hand are less than damage fingerprint for a person, (iii) even the presence of very less amount of dirt or grease can affect the performance of fingerprint verification, but having little effect in case of palmprint, and importantly (iv) higher user acceptance for palmprint mainly due to the stigma of fingerprints being associated with criminal investigations.

The double encryption method incorporates both the ideas of symmetric and asymmetric cryptosystem efficiently and minimizes most of the shortcomings associated with both the approaches. The other important concern of the system is the management of private key, as at the end of double encryption

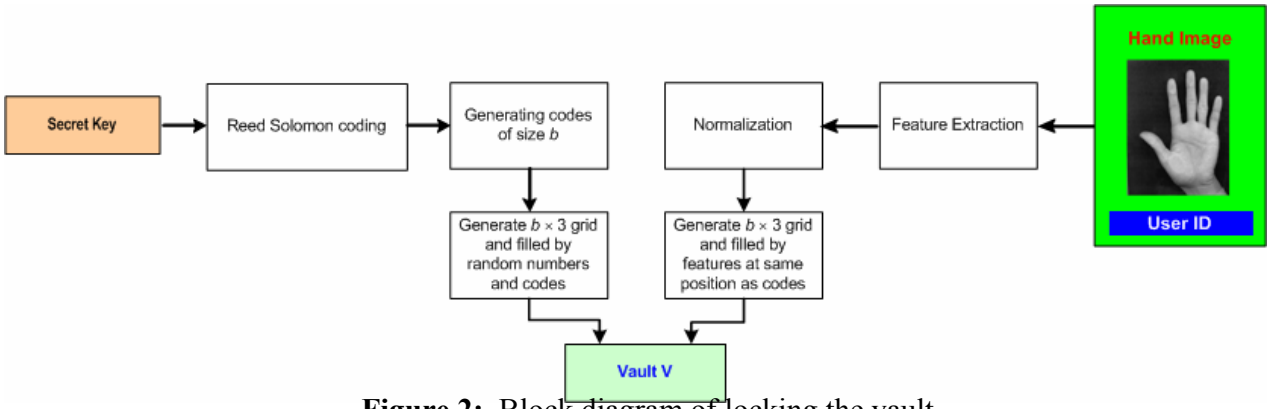


Figure 2: Block diagram of locking the vault

security of the entire system depends upon the security of private decryption key. The security to private key can be ensured by the use of well known concept fuzzy vault detailed in [1]. The combination of cryptographic keys with biometric offers several advantages including the fact that this removes the extra key management for a user by ensuring that it is non-transferable. This method of protecting the private key not only makes the usage of smart cards redundant but also made the user self dependent for its key. The difficulties lies in the fact that the cryptographic algorithm expected the keys should be highly similar within every use, but clearly not the case with typical biometric. The key is to use suitable coding theory scheme which can tolerate resulting errors .We have used Reed and Solomon (RS) coding scheme for providing some error tolerance while decryption. This error tolerance is essentially required to handle inherent variations in palmprint (biometric) features from the same user during decryption. These variations can be attributed to the scale, orientation and translational variations in the user palmprints due to peg-free imaging. The RS coding scheme have error correcting capacity of $(n\text{-}k)/2$, where n is the length of code and k is the length of message, and used to encode decryption key K_{pri}.

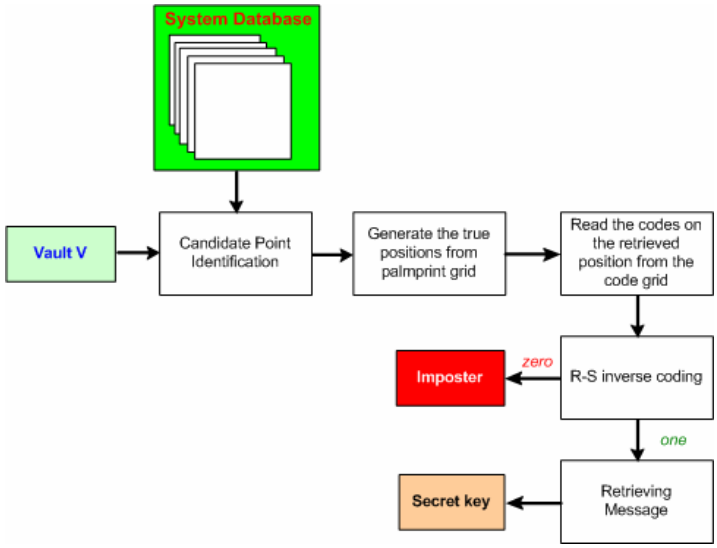


Figure 3: Block diagram for unlocking the vault.

We can easily vary (k, n) during the training stage/phase and achieve the best possible combination for minimum false acceptance and rejection rates. The proposed design of palmprint vault is quite similar as for the fingerprint [16]. Let the codes generated by R-S coding theory is of size b. Then generate a grid of size $b \times 3$ such that i^{th} row of grid contains i^{th} place. The rest two places are filled by random numbers generated during encoding. We designate this grid as grid F. Further, a grid of same size is generated and the biometric features are placed at the same position as in the case of RS codes. The rest two places are filled with number such that each row is maintained in arithmetic progression. Let us designate these numbers as *tolerance value*. These points are actually the chaff points making the grid fuzzy. We called this grid as grid G. To unlock the vault we only need to know the correct positions of the elements in grid G, which can be achieved by comparing the input palmprint features with all the number in the corresponding row. Taking the minimum in distance we can easily locate the positions of actual biometrics from grid F and hence the corresponding positions for the codes in grid G. The inverse RS codes are used to decode the codes. One can select the suitable values for n and k to control the error occurred due to the variability in palmprint features. ***The motivation behind choosing the tolerance for the palmprint features is to make them fuzzy such that an imposter is not able to predict the feature vector just at random***. The block diagram for locking and unlocking the vault using palmprint features is shown in figure 2 and 3 respectively. Once the procedure for the locking and unlocking of vault is determined, we fix the criteria for genuine to successfully open the vault while rejecting the imposter attempts. Finally, this decryption key should successfully decrypt the secret private RSA key.

3.3. Feature Extraction and Normalization

The palmprint features employed in this work were extracted from the palmprint images acquired from the digital camera using unconstrained peg-free setup in indoor environment. The extraction of region of interest, *i.e*. palmprint, from the acquired images is similar as detailed in [4]. The Discrete Cosine Transform (DCT) is used for the characterization of unique palmprint texture. DCT is highly computationally efficient[1] and therefore suitable for any online cryptosystem. As illustrated in figure 4, each of the 300 × 300 pixels palmprint image is divided into 24 × 24 pixels overlapping blocks. The extent of this overlapping has been empirically selected as 6 pixels. Thus we obtain 144 separate

[1] DCT is basis of JPEG and several other standards (MPEG-1, MPEG-2 for TV/video, and H.263 for video-phones).

blocks from each palmprint image. The DCT coefficients from each of these N square block pixels, *i.e.* $f(x,y)$, is obtained as follows:

$$C(u,v) = \varepsilon(u)\varepsilon(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi.u}{2.N}(2x+1)\right]\cos\left[\frac{\pi.v}{2.N}(2y+1)\right] \quad (2)$$

where $u, v = 0, 1. 2, \ldots, N-1$ and $\varepsilon(u) = \varepsilon(v) = \begin{cases} \sqrt{\frac{2}{N}} & \text{for} \quad u \neq 0 \\ \sqrt{\frac{1}{N}} & \text{for} \quad u = 0 \end{cases}$

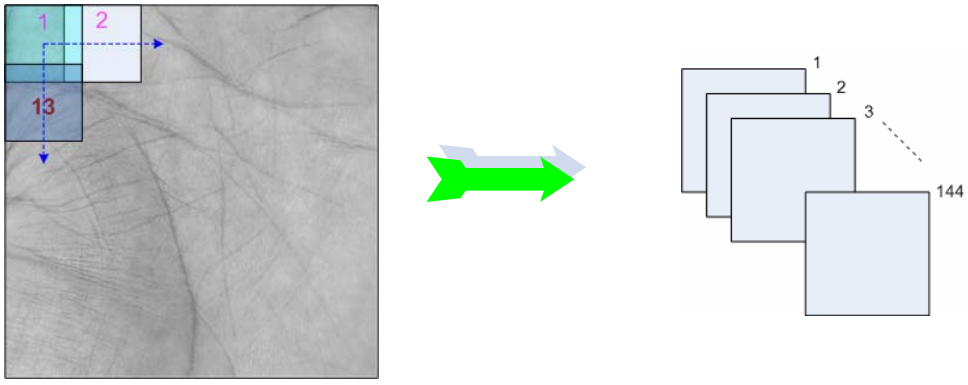


Figure 4: Localization of 144 overlapping palmprint image sub blocks for feature extraction

The standard deviation of DCT coefficients, obtained from each of the overlapping blocks, is used to characterize the region. Thus we obtain a feature vector of 144 values. High degree of intra-class variability in the palmprint features, mainly due to peg-free imaging, poses serious problems in the unlocking of the constructed vault by the genuine. Corresponding to each feature vector, the training images are normalized and then their mean and standard deviations are used for feature normalization in the test phase. This normalization reduces the features less variability and very much helpful in fixing tolerance for fuzzy vault.

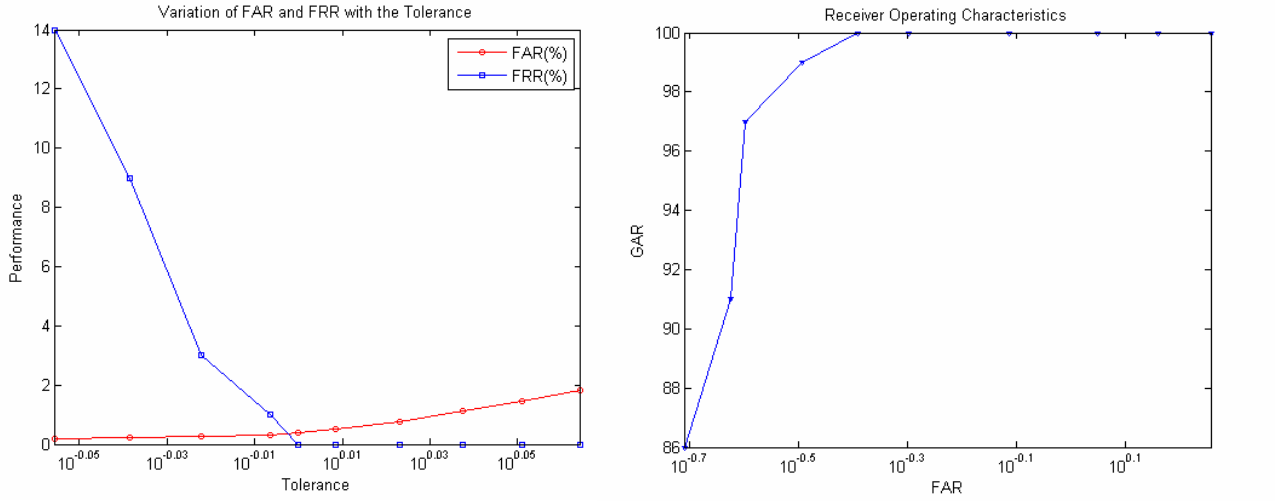
4. Experimental Results

The implementation of the system consists of generation of RSA cryptosystem. A dummy document is then double encrypted using symmetric and asymmetric keys. After double encryption, fuzzy vault has created around private key by generating grids using R-S codes and palmprint features. The evaluation was based on varying tolerance value over a range and the corresponding FAR and FRR is then calculated. The palmprint database consisted of the left hand images from the 85 users and two images from each of the users were employed. The first enrolled palmprint image from each of the users was employed to lock the vault. The successful opening with the second enrolled palmprint

image of the same user was considered as genuine match while opening with all the other enrolled test images from other enrolled users (*i.e.* 84 users) were considered as imposter matches. Thus our false acceptance rate (FAR) and false rejection rate (FRR) estimation is based on 84 × 85 imposter and 85 genuine respective attempts. The decisions for FAR and FRR depends upon choice of tolerance. We performed several experiments to select the best value of this tolerance. Figure 5 illustrates the performance of the proposed palmprint based vault. Figure 5(a) illustrates the variation of FRR and FRR scores with the tolerance while figure 5(b) illustrates the receiver operating characteristics (ROC). RSA cryptosystem used in our program has some variations in key length [23]. Table 1 illustrates the variation in experimental results (equal error rate) with the key length and the corresponding tolerance value.

Table 1: Summary of experimental results

Key Length	EER	Tolerance
306	0.905	1.060
307	0.375	0.995
308	0.752	1.065
309	2.134	1.118



(a) (b)

Figure 5: (a) The variations of the FAR and FRR characteristics with the tolerance for the palmprint based cryptosystem, (b) corresponding receiver operating characteristics.

5. Discussion

While the idea of incorporating biometrics within cryptographic constructs has shown promising results than password-based authentication, the system still has open issues. The biometric modalities investigated for the experimental evaluation has been quite limited and as most of the prior work is

Table 2: Comparative summary of prior work.

Biometric	Feature	Error Correction Code	FRR (%)	FAR (%)	Reference	Database Size
fingerprint	Minutiae points	RS Code	5	0	[17]	9 Users
Voice	Cepstrum coefficient	Discretization	20	NA*	[19]	10 Users
Signature	Dynamic time wrapping	Feature coding	28	1.2	[3]	25 Users
Iris	Gabor Feature	RS code and Hadamard codes	0.47	0	[15]	70 Users
Fingerprint	Fourier transform	Majority code	12	35	[14]	20 Users
Fingerprint	Minutiae point	RS code	30	NA	[11]	NA*
Fingerprint	Minutiae points and helper data	RS code	3	0.24	[2]	100 Users (*FVC'02*)
Palmprint	**DCT features**	**RS code**	**0**	**0.4**	**-**	**85**

*NA – Not Available

focused on fingerprint. Recently, iris [15], face [14], signature [3] have also been investigated and yielded promising results. However, comparative summary of prior work presented in table 2 suggests that that much of the work has been simulated on a small dataset, such as [16] has used 9 users, [18] has used 10 users, [13] has used 20 users, which is quite small to generate a reliable conclusion on performance.

Despite the current popularity of palmprint biometric, there has not been any attempt to investigate its usage for the fuzzy vault. This paper therefore investigated the possible usage of palmprints in fuzzy vault to develop a user friendly and reliable crypto system. The image dataset used for the experiments (85 users) was acquired from unconstrained peg-free setup as such images are more realistic and expected to show large variations. We propose mixed cryptosystem which has advantage over both symmetric and asymmetric cryptography. The advantage of the proposed system is that it not only attempts to alleviate the shortcomings of symmetric key based cryptosystem, but also solves the problems involve in asymmetric key based approach. As the asymmetric approach for the encryption is quite slow in bulk data encryption, we encrypt the entire document with symmetric key approach (since this approach is quite fast in bulk data encryption, compared to asymmetric approach). On the other hand to minimize the shortcomings associated with symmetric key approach, we again encrypt the symmetric key using asymmetric approach. The palmprint based fuzzy vault is then constructed using the decryption key which is private. The experimental results on the performance are ascertained using the FRR and FAR scores.

Performance of the proposed system depends upon choice of tolerance chosen for grid of palmprint features. The increase in tolerance could lead to wrong positions in grid and hence even the genuine user cannot open the vault, which can result in unacceptably high false rejection rate. The low tolerance value could diminish the fuzziness of grid which can cause the imposters to be accepted and hence increase in false acceptance rate. The optimal range for tolerance value is dependent on the range of palmprint features.

The main consideration is on the construction of palmprint based fuzzy vault around private key. The private and public keys are generated on publicly available RSA toolbox [23]. The bit length of modulus m=*k*l*, where m *K* and *l* are prime numbers (section 3.1.5) is chosen as 1024 bits and length of encryption exponent *n* is 64 bit. The two large primes chosen to be 512 bits, so that 1024 bit RSA modulus *m* can be generated. The RSA implementation has utilized the string format to generate the RSA keys and its length varies from 306 to 309 which is equivalent to 1015 to 1024 in binary bits. For the used RSA cryptosystem, the private key *sc* should be chosen such that it should satisfy the equation:

$$n*sc \equiv 1 \pmod{si}, \quad \text{where } 1 < sc < si \tag{3}$$

It can be observed from above equation that more than one value of *n* can satisfy the congruence and hence the length of generated string (key) can vary. The prime numbers are randomly chosen and so the values of *si* and *n* are, so that the variations in length of keys are not controlled. In our experiments we have observed and accounted for this variation. Our implementation stores the fixed length key and loads it at the time of generating grids to construct the vault. Therefore the table 1 illustrated all the possible variations in key length and the corresponding equal error rates with the tolerance value. We can see as the key length varies (in the range 306 to 309) the system has different equal error rate at different tolerance. The minimum equal error rate is on key length 307.

5. Conclusions

This paper has investigated a new approach to construct the cryptographic vault using palmprint features. In order to combine cryptography with palmprints we have also suggested the implementation of double encryption. This can efficiently reduce the possibility of hacking within a cryptosystem. The experimental results presented in section 4 illustrate that the palmprint based cryptosystem can operate at low EER (0.375%). The comparative summary of this work with the prior work, presented in table 2, suggest that the palmprint can be used as a promising biometric in

the construction of a cryptosystem. The cryptosystem investigated in this paper employed localized spectral features from the palmprints. The multiple feature representation, such as detailed in [6], can offer more reliable characterization of features and therefore cryptosystem based on multiple-palmprint representation is can be considered for the extension of this work.

5. References

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

[2] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and Performance," to appear in *IEEE Trans. Info. Forensics & Security*, available online from Aug. 2007

[3] F. Hao, and C.W. Chan, "Private key generation from on-line handwritten signatures," *Information Management & Computer Security*, Issue 10, No. 2, pp. 159–164, 2002.

[4] A. Kumar, D. C. M. Wong, Helen C. Shen, and A. K. Jain, "Personal authentication using hand images", *Pattern Recognition Letters*, vol. 27, pp. 1478-1486, Oct. 2006.

[5] W Stallings, *Cryptology and Network Security: Principles and Practices*, 3rd Ed., Prentice Hall, 2003.

[6] A. Kumar and D. Zhang, "Palmprint authentication using multiple representation," *Pattern Recognition*, vol. 38, pp. 1695-1704, Oct. 2005.

[7] Z. Sun, T. Tan, Y. Wang, S. Z. L, "Ordinal palmprint representation for personal identification," *Proc. CVPR 2005*, pp. 279-284, 2005.

[8] A. Juel and M. Sudan, "A Fuzzy Vault Scheme", *Proc. IEEE Int'l. Symp. Information Theory*, A. Lapidoth and E. Teletar (*Eds.*), pp. 408-412, 2002.

[9] A. Juel and M. Wttenberg, "A Fuzzy Vault Commitment Scheme", *Sixth ACM Conf. Computer and Comm. Security*, G. Tsudik (*Ed.*), pp. 408-412, 2002.

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

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

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

[13] C. Sautar, D. Roberge, A. Stoianov R. Gilroy and B.V.K. Vijaya Kumar, "Biometric Encryption" *Information Management and Computer Security*, vol. 9, no 5, pp. 205-212, 2001.

[14] A. Goh, and D.C.L. Ngo, "Computation of Cryptographic keys from face biometrics," *International Federation for Information Processing*, LNCS 2828, Springer-Verlag, pp. 1-13, 2003.

[15] H. Feng, A. Ross, and J. Daughman, "Combining crypto with biometrics efficiently", *IEE Trans. Computers*, pp. 1-17, Sep. 2006.

[16] A. Nager and S. Chaudhury, "Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme," *Proc. ICPR 2006,* pp 537-540, Hong Kong, Aug. 2006.

[17] F. Monrose, M. K. Reiter and R. Wetzel, "Password hardening based on keystroke dynamics," *Proc. 6th ACM Conf. Computer & Comm.*, pp. 69-83, CCCS, 1999.

[18] F. Monrose, M.K. Reiter, Q. Li and S. Wetzel, "Cryptographic key generation from voice," *Proc. IEEE Symposium Security & Privacy*, pp. 1-12, May 2001.

[19] F. Hao, and C. W. Chan, "Private key generation from on-line handwritten signatures," *Information Management & Computer Security*, Issue 10, no. 2, pp. 159–164, 2002.

[20] http://pajhome.org.uk/crypt/rsa/maths.html.

[21] RSA algorithm, http://www.di-mgt.com.au/rsa_alg.html.

[23] http://islab.oregonstate.edu/koc/ece575/02Project/Kie+Raj/

[24] D. Zhang, W.K. Kong, J. You, and M. Wong, "On-line palmprint identification," *IEEE Trans. Patt. Anal. Machine Intell.*, vol. 25, pp. 1041-1050, Sep. 2003..