Hindawi Publishing Corporation
EURASIP Journal on Advances in Signal Processing
Volume 2009, Article ID 967046, 11 pages
doi:10.1155/2009/967046

Research Article

Development of a New Cryptographic Construct Using Palmprint-Based Fuzzy Vault

Amioy Kumar[1] and Ajay Kumar[1,2]

[1] *Biometrics Research Laboratory, Department of Electrical Engineering, Indian Institute of Technology Delhi, Hauz Khas, New Delhi 110 016, India*
[2] *Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong*

Correspondence should be addressed to Ajay Kumar, ajaykr@ieee.org

Received 7 October 2008; Accepted 16 July 2009

Recommended by Stephanie Schuckers

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 palmprint in fuzzy vault to develop a user friendly and reliable crypto system. We suggest the use of both symmetric and asymmetric approach for the encryption. The ciphertext of any document is generated by symmetric cryptosystem; the symmetric key is then encrypted by asymmetric approach. Further, Reed and Solomon codes are used on the generated asymmetric key to provide some error tolerance while decryption. The experimental results from the proposed approach on the palmprint images suggest its possible usage in an automated palmprint-based key generation system.

1. Introduction

Hacking of the information is widely considered as one of the potential attacks on any secure system. Authentication systems should be designed to withstand such attacks when deployed for critical security applications such as e-commerce and accesses to restricted data/buildings. Biometric-based authentication is considered as one of the most secured systems whenever high privacy is demanded. However, such authentication systems itself follow stepwise procedural algorithms, like feature extraction, matching, classification, and so forth, for authentication/verification purposes [1]. As biometric templates are required at each step, it increases the possibilities of intrusion at every step and requires additional security management [2]. For instance, even a most secure authentication system is not reliable if it cannot defy the attacks on the stored database, or if an intruder can intercept the template features generated from the biometric traits. Recent research efforts have developed some promising ideas to resist attacks on biometric authentication system. One of such proposed solutions is to cancel the tainted biometric features and regenerate the new one for authentication purposes (also known as cancelable biometric [3]). BioHashing technique is frequently used to transform (noninvertible) biometric template into some other representations using one-way hash functions. This reissuance of the biometric templates can withstand the attacks on stored templates and widely accepted as a solution to the intrusion in extracted features. The most acknowledgeable work in this area is to provide cryptography-based security at different stages of biometric authentication. Cryptography is one of the most effective ways to enhance the security of the information system via its encryption and decryption modules [4]. Even so, the weakest link of cryptography-based security systems is the associated secret key. While the simple memorized key can be easily intercepted, a long and complex key needs extra storage management like tokens, smart cards, and so forth. Consequently, the smart card-based solutions came in existence. To provide an aid to security, the cryptographic keys are now stored somewhere (e.g., in a computer or on a smart card) and released based on some alternative authentication mechanism. The most popular mechanism used for this purpose is password-based security [5], which

is again a long string and difficult to make secure, as now the whole security depends upon the password given, used for authentication.

As a solution, 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. The encryption keys can be generated using low-level combination of biometric features and cryptology. Jules and Sudan [6] have proposed the generation of a secure vault using an unordered 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. [7], 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 decryption module.

However, the motivation to protect secret key involved in cryptographic modules using biometric based fuzzy vault can have several drawbacks due to different cryptographic approaches. While the symmetric cryptographic approaches suffered authentication problems, asymmetric approaches are computationally intensive (as further discussed in Section 3). We, therefore, proposed the combination of both symmetric and asymmetric cryptographic approaches (which is referred to as double encryption in this paper) into the fuzzy vault to meet high-security standard and utilize the advantages of both approaches in a common domain. In the recent years, biometric features such as face, iris, fingerprint, hand geometry, palmprint, and signature have been suggested for the security in access control. Most of the current research in biometrics has been focused on fingerprint and face. The recent research on face recognition has shown some thorny problems regarding pose, lighting, orientation, and gesture which made it less reliable as compared to other biometrics. Fingerprint identification has successfully implemented and widely accepted in most of the cases for recognition purposes. However, it also has difficulties regarding feature extraction. The fingerprint features are very difficult to extract from the elderly, laborer, and handicapped users. As a result, other biometric characteristics are receiving increasing attention. Moreover, additional biometric features, such as palmprint and hand geometry, can be easily integrated with the existing authentication system to provide enhanced level of confidence in personal authentication. We explored the usage of palmprint biometric to create fuzzy vault. The prior works in this area is summarized in Section 2, while the detail of the earlier cryptographic approaches is presented in Section 3. Double encryption is explored in Section 4. The proposed system is discussed in Section 5. The experimental results from the performed approach are summarized in Section 6. This section also includes a summary of related prior work. Finally, the main conclusions from this paper are summarized in Section 7.

2. Prior Work

The issue of nonrevocable biometric has been investigated by Ratha et al. [3] by introducing the concept of cancelable biometrics. Davida et al. [8] proposed majority decoding and error correcting codes-based technique to generate the cancelable biometric features. The approach is further utilized using optical computation techniques in [9] and using keystroke dynamics in [10]. Sautar et al. [9] were the first to commercialize the concept in to their product *bioscrypt*. They applied Fourier transform and majority coding to reduce the feature variation. A predefined random key is locked by biometric sample using phase angle product, and this product can be further unlocked by other genuine biometrics. The performance analysis is however not reported. Connie et al. [11] used the concept of BioHashing by calculating fisherprojections. However, the results shown by them are based on the assumption that the generated token or keys will be never stolen or shared. This is quite unrealistic and creates doubts about real evaluation. The study of such unrealistic evaluation has been presented by Kong et al. in [12]. One of the innovative works proposed in this area is by [2], where the authors utilized random orientation field into the feature extractor to generate cancelable competitive codes. The authors further considered all the three attacks possible (template reissuance, replay attacks, and database attacks) to provide a complete secure system. To protect the generated cancelable competitive codes (replay attacks) [2], the idea of one-time pad (OTP) ciphers is explored. The OTP [13] is a symmetric cipher (same key is used for both encryption and decryption) generated by applying XOR between the randomly generated key and the plaintext. The decryption can be done using the matched OTP and the key (used for encryption). The advantage with OTP is that each encryption is independent to the next encryption, and random key can be used only once for encryption. Hence, theoretically there is no way to break such encryption just by analyzing a sequence of message. Although OTP encryption has advantages over other encryption algorithms, still it has some open issues like (i) the key involved for decryption should be identical to encryption once and hence required safe communication of key to the decrypting party [13]; (ii) the number of bits in the key is same as in the plaintext which makes the algorithm computationally inefficient for encrypting bulk data; (iii) one of the major requirements of the algorithm is that not part or bit of the key should be ever reused in any other encryption; otherwise it is easy to break it [14]. (Synchronized OTP generator can be employed to counter such problems.) Authors in [15] proposed a new cryptosystem by generating 1024 bits binary string, extracted from the differential operations. The string is then mapped to 128 bits encryption key using a Hash function. The approach is novel and secure in many respects but still has issues to resist against attack on generated encrypting key using Hash function, as raised by Kong et al. in [12].

In most of the works proposed in literature of cancelable biometrics, security of system depends upon the generated unique code from a particular one-way hash functions. Thus the system is secure till the unique code is not compromised

and hence requires extra security management. Juels and Sudan [6] have presented a promising model which was an improvement on the prior study by Juel and Wttenberg in [16]. They have produced a significant improvement by modifying the Scheme of Davida et al. (in using error correcting code size) [8] by introducing Reed and Solomon error correcting coding theory in their fuzzy vault. Their contribution is to hide any secret in fuzzy vault using polynomial construction under unordered set. The secret can be retrieved back by polynomial reconstruction, if certain points of the unordered set can be known at receiving end. The security of the scheme mainly depends upon polynomial construction and reconstruction problem. Uludag et al. [7] have combined the concept of fuzzy vault with biometrics (fingerprint) by using biometric template as an unordered set. Uludag and Jain [17] 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. [18] have attempted to eliminate such variability using *helper data* and illustrated promising results. Hao et al. [19] use iris biometric for generating cryptographic keys and a combination of Reed and Solomon and Hadamard error correcting theories for error tolerance. Calancy et al. [20] proposed a smart card-based fuzzy vault that employed fingerprints for locking and unlocking. The presumption that acquired fingerprint images are prealigned is not realistic and could be the possible reason for high false rejection rate (30.0%) reported in the paper. Lin and Lai [21] 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 in [19] using asymmetric cryptosystem. Having generated RSA public and private keys, authors have used Reed-Solomon coding to convert the keys in to codes. Further they used two grids, one for codes and the 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, a different range of biometrics has been used for fuzzy vaults in literature. However, with few notable exceptions, for example, [15, 19], with small false rejection rates, the average FAR of 15% has been cited.

In contrast to prior work in this area, we proposed [22] fuzzy vault-based security to withstand the attacks on secret key employing palmprint. The secret document/information can be first encrypted using double encryption. The symmetric key approach can be easily employed to encrypt bulk data. The attacks on security of symmetric key (secure communication, authentication, as detailed in Sections 3.1.1 and 3.1.2 in this paper) are reduced by encrypting it again using asymmetric cryptographic approach. Finally, the private key of asymmetric approach (at the end of double encryption) is protected by creating fuzzy vault around it. The approach is to firstly employ double encryption to strengthen the security system and reduce the shortcomings associated with both symmetric and asymmetric cryptographic approaches and finally to utilize the palmprint features to create fuzzy vault around the key at the end of double encryption.

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 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, named as initials of Ron Rivest, Adi Shamir, and Leonard Adleman) for encryption has been estimated to be very slow as compared to traditional symmetric approach (Data Encryption Standard, abbreviated as DES) [4]. 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. Cryptographic Approaches

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. This is referred to 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, both symmetric and asymmetric approaches are briefly introduced, and then the proposed approach utilizing the combination of both approaches is discussed.

3.1. The Symmetric Cryptosystem. The symmetric approach is most commonly used cryptosystem, as the system is easy to implement and more importantly it has very fast encryption speed [4]. Symmetric algorithms, such as, DES, Triple DES, and Rijndael [4], provide efficient and powerful cryptographic solutions, especially for encrypting bulk data. Let $X = [x_1, x_2, x_3, \ldots, x_m]$ be the secret message required to be hidden by source A (Lucie). The m letters of message are alphabets. The message is intended to B (Bryan). Lucie generates its symmetric key, say K_{Sim}, and uses this key to lock secret message X:

$$Y = K_{Sim}(X). \tag{1}$$

She then sends the encrypted (locked) message and the respective symmetric key (K_{Sim}) to B (Bryan). Receiver B (Bryan) used the symmetric key to decrypt the message:

$$X = K_{sim}(Y). \tag{2}$$

In the presented work we have used advance encryption standard (AES) as a symmetric cryptosystem, which is advanced version of data encryption standard (DES). The AES is symmetric key-based cryptosystem which is based on the principle of block and substitution cipher. The AES algorithm uses substitution boxes, polynomial matrices, and symmetric key to convert a plain text to cipher text. These are the parameter for AES cryptosystem and required to be generated first before the encryption module [4]. Although symmetric key algorithm is very fast and efficient in bulk data encryption, it can sometimes fail to ensure high-security requirements. There are few shortcomings with the usage of symmetric key cryptography. We now detail the problems associated with symmetric key algorithms.

3.1.1. The Problems behind Authentication. Ensuring the integrity of received data and verifying the identity of the source of that data is of major concern to ensure the security in data communication. A symmetric key can be used to check the identity of the individual, as it requires the presence of symmetric key, but this authentication scheme can have some problems involving trust. The problem is that this scheme cannot discriminate between the two individuals who know the shared key. For example, any person having control on Lucie's private particulars can make any fraud message to her pals by pretending himself as Lucie. This not only allows intruder to do any unauthorized work in place of Lucie but also creates problems for other related persons. This uncertainty with symmetric approaches made them useless whenever high confidentiality required in the communication system. The above discussed issues can lead to the position where there is no stand to deny if the disputes were to arise. The relevant example is of repudiation when Lucie's friend renews the contract signed by Lucie without telling her and repudiates from the fact by claiming that someone else might have stolen the key from Lucie to sign the contract. This concludes the key point that the communication system must present nonrepudiation between communicating parties. The major weakness with symmetric approach is that they sometimes fail to authenticate persons in communication.

3.1.2. The Problems behind Security of Key. The other problem associated with this system is to ensure the security of the involved symmetric key and how to exchange it safely. The security of a signed document depends upon the secret key involved as only secret key can ensure the decryption of this document. Thus for a secure communication system the secret key should be exchanged safely. One of the shortcomings of the cryptographic approaches is that they do not emphasize on key exchange problems. The asymmetric approaches such as RSA, DSA, and ECC are very good substitution of symmetric approach as it eliminates many of its shortcomings. Both of the above discussed problems can be alleviate by using asymmetric approach.

3.2. The Asymmetric Cryptosystem. The conventional symmetric cryptosystem is similar to a lockbox with a combination lock. This combination lock opens and closes with one and the single combination, that is, the key that can be used for both opening and closing the box. However, the asymmetric approach uses a single lock that has two distinct combinations, one for opening and one for losing. This approach allows effective control over who can place or remove the contents in lockbox by assigning one of the combinations as the secret and the other one as public. This added flexibility offers two distinct advantages: confidentiality without prior key exchange and the enforcement of data integrity. Now for this approach, B generates a related pair of keys: a public key K_{pub} and a private key K_{pri}. The K_{pri} is known only to B, whereas K_{pub} is publicly available to everyone and therefore accessible by A also. With the message X and the encryption key K_{pub} as input, A forms the cipher text, denoted as Y, as follows:

$$\begin{aligned} Y &= K_{pub}(X), \\ Y &= [y_1, y_2, y_3, \ldots, y_m]. \end{aligned} \tag{3}$$

The intended receiver in the position to matching is able to invert above using the following transformation:

$$X = K_{pri}(Y). \tag{4}$$

In this work, we have used RSA cryptosystem which is the most commonly used asymmetric approach. A traditional RSA algorithm [23] requires two randomly generated prime numbers [24]. For the security of RSA algorithm, the prime numbers should be bigger (512 bit in our case) and randomly chosen. Any secret encrypted using public key can only be decrypted by using private key and vice versa. The main points involved in encryption and decryption are as follows.

Lucie does the following:

(1) obtains the recipient Bryan's public key,

(2) represents the plaintext message as a positive integer,

(3) computes the ciphertext,

(4) sends the ciphertext to Bryan.

Recipient Bryan does the following:

(1) uses his private key to compute positive integer,

(2) extracts the plaintext from the integer representative.

Using RSA algorithm, asymmetric cryptosystem can be employed to solve a number of problems regarding symmetric cryptographic approach. But as compared to symmetric approach, asymmetric approach also has few drawbacks.

3.2.1. The Problems behind RSA. The private and public key approach of RSA cryptosystem can be substitute of the key exchange problem involved with symmetric approaches, but the major problem regarding this approach is the distribution of public keys. Having signed the secret document with Bryan's secret key, Alice must ensure that the public key available is really Bryan's key but not of intruder Carol. The management and security of private key is also a major concern. The other important problem with asymmetric cryptography is that the processing requires intense use of

the central processing unit as it is computationally intensive and requires a lot of mathematical computations. This may be a real problem when several simultaneous sessions are required. The asymmetric approaches like RSA, DSA, and so forth are generally known to be slower (about 100 times slower) [4] than symmetric approaches like DES, AES, and so forth. 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.

4. Double Encryption

One way to alleviate above discussed problems associated with the symmetric and asymmetric cryptographic approaches is to use double encryption. A secret message is encrypted using fast symmetric algorithm; the secret key is then encrypted using asymmetric cryptography; the Ciphertext (encrypted message) and the encrypted keys are finally sent to the recipient. Asymmetric cryptography is slow (computationally intensive), but not too slow to encrypt such a small (as compared to secret message) bits 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. This idea not only resolves the problem using both approaches but is also more computationally sound.

4.1. Why Double Encryption? Most of the problems regarding symmetric/asymmetric approaches can be remedied using double encryption. The advantages of the symmetric approaches are utilized to encrypt bulk of the data, while asymmetric approaches are used to provide authentication/verification to secure communication (as discussed in Sections 3.1.1 and 3.1.2 symmetric approaches are sometimes fail in authentication purposes). Using double encryption, a message (may be bulk data) can be encrypted by symmetric key approach, while the key is again encrypted by public/private keys of asymmetric approach. Once the message is encrypted by public key of recipients, it can only be decrypted by its private key. This ensures a safe communication between the source and the verified/authenticated recipient. On the other hand, if the message is encrypted by private key of the recipient, it can only be decrypted by corresponding public key (which is publicly available). This process authenticates the source of encryption and therefore prevents any possible repudiation or denial from the message generator.

4.2. Prior Work in Double Encryption. The concept of double encryption is not new in cryptographic literature [25–27]. However, most of the related work is centered on the implementation of cryptographic encryption and decryption modules [28–30]. Some of these notable efforts can now be outlined. Nishimura et al. [25] in their recent European patent have detailed the concept of encrypting symmetric key with public and private keys of asymmetric approach. Their developed approach ensures that when a doubly-encrypted message is received, it is sent by a particular/authenticated user; also the recipient of this message is a specific/verified user(s). Doh et al. [31] have presented double encryption-based optical security system. They have utilized the facial images by using random-phase patterns in the spatial plane and the Fourier plane and a personal information image consisting of a personal identification number (PIN). With the recognition of PIN, the authentication of the encrypted personal identification card has done by primary classification and recognition of the PIN with the proposed multiplexed MACE phase-encrypted filter. In this technique, the possibility of spoofing is significantly decreased using the double-identification process. Z. Liu and S. Liu [32] proposed Double image encryption based on iterative fractional Fourier transform. They used to encrypt two different images into a single one simultaneously by their amplitudes of fractional Fourier transform with different orders.

In contrast to proposed double encryption schemes, we explored this concept for fuzzy vault. The combination of cryptographic algorithms with biometrics has been presented in several prior publications, for example, [2, 15, 17–19]. Some of these attempts have been focused to hide the secret information in biometric-based fuzzy vault [17, 18] while others used to generate cryptographic keys using biometrics ([15, 19]) to hide the secret information. *Our contribution to literature is that we attempt* to hide secret information using double encryption (via symmetric and asymmetric cryptographic approaches). In order to strengthen the cryptographic approaches, we closed the asymmetric key (at the end of double encryption) by creating palmprint-based fuzzy vault around it. *Our scheme is quite unique in the sense that, it overcomes any dependency on generated secret key (like [11, 33]) in cryptographic approaches and utilized the unique palmprint features to create the fuzzy vault.*

4.3. Motivation to Fuzzy Vault. One of the most important applications of double encryption is that it can overcome many of the problems associated with the symmetric key approach (as the symmetric key is again encrypted by asymmetric approach). In addition, the level of security offered by the resulting asymmetric key, at the end of double encryption, is very high and desired to secure the entire system. *In the cryptographic literature, security of asymmetric key (at the end of double encryption) is generally questioned as the main/key weakness of the double encryption [28].* In the proposed approach, we have utilized the concept of fuzzy vault to overcome this shortcoming of double encryption by locking the private key in the vault. This combination of double encryption with biometrics (fuzzy vault) can

overcome most of the weaknesses regarding symmetric and asymmetric cryptographic approaches.

5. Proposed System

Let X denote the dummy message to be encrypted and let K_{sim} be the symmetric key, used to encrypt the document. In order to encrypt the message X, the symmetric key can be generated using AES algorithm. Let the symmetric key be denoted by K_{sim}. Now for making system more secure and overcome the difficulties of symmetric key approach, (key exchange problem, confidentiality, etc.) the generated symmetric key again is encrypted by asymmetric approach using RSA algorithm. Let the public and private keys associated with the RSA cryptosystem are denoted by 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. Equation (5) summarize the complete procedure:

$$\begin{aligned} Y &= K_{sim}(X), \\ T &= K_{pub}(Y), \\ Y &= K_{pri}(T), \\ X &= K_{sim}(Y). \end{aligned} \tag{5}$$

Figure 1 illustrates the complete block diagram and includes all the key steps in the double encryption algorithm. For the traditional RSA cryptosystem, the public key has made publicly available while private key has kept private. The cipher text has been generated with the publicly available encryption key while it is decrypted with the private key kept private. The security of the system depends upon the secrecy of private key.

5.1. 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 [34–36], there has not been 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 is associated with criminal investigations.

The double encryption method detailed in previous section incorporates both the ideas of symmetric and asymmetric cryptosystem efficiently and minimizes most of the shortcomings associated with both approaches. The other important concern of the system is the management of private key, as at the end of double encryption 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 [6]. Using the concept of fuzzy vault, our main goal is to hide this decryption key using biometric features to provide some security to the decryption key and make the whole system tailored for its practical usage. The combination of cryptographic keys with biometric offers several advantages including the fact that this removes the extra key management efforts required by the user and ensures that it is nontransferable. This method of protecting the private key not only makes the usage of smart cards redundant but also makes the user self dependent for its key. The difficulties lie in the fact that the cryptographic algorithm expects that the keys should be highly similar for every attempt for successful access, but it is clearly not the case with a typical biometric. The key is to use suitable coding theory scheme which can tolerate 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 palmprint due to peg-free imaging. The RS coding scheme has error correcting capacity of $(n - k)/2$, where n is the length of code and k is the length of message, and used to encode decryption key K_{pri}.

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 [37]. Let the codes generated by R-S coding theory be of size b. Then we generate a grid of size $b \times 3$ such that ith row of grid contains ith 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 of the two places are filled with numbers such that each row is maintained in the 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 numbers in the corresponding row. Taking minimum of the distance, we can conveniently locate the positions of actual biometrics from grid F and hence the corresponding positions for the codes in grid G. The idea of generating such random numbers to combine with biometric templates is somewhat similar to as discussed in [2]. However, in contrast to [2], our approach is to add the tolerance value to the feature vectors. Out of the three places on the grid G, only one place is filled by original feature, and the rest two places are filled by original features added with tolerance value. The work presented in [2] has been motivated from the random orientation field, which is inserted into the feature extractor to generate noise-like feature codes. The inverse Reed and Solomon codes are used to decode the codes. One

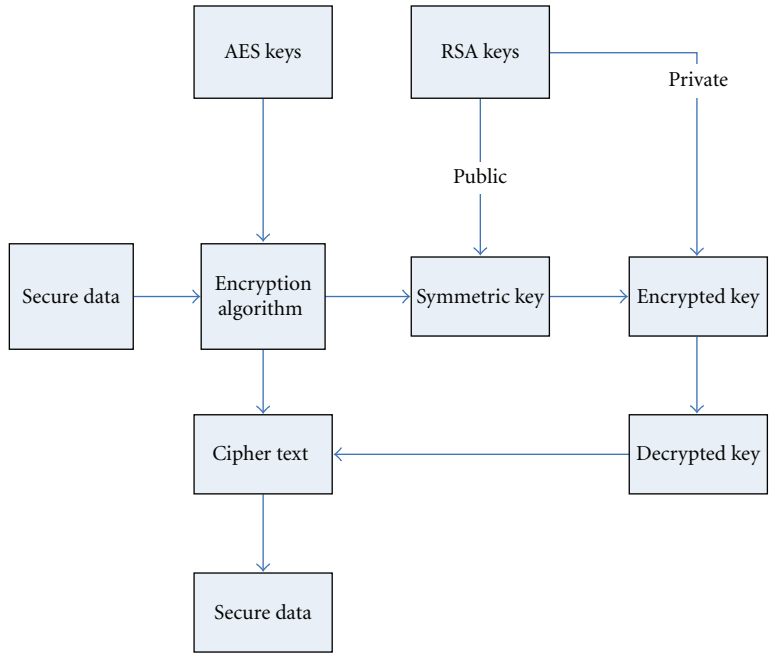

Figure 1: Block diagram for the double encryption.

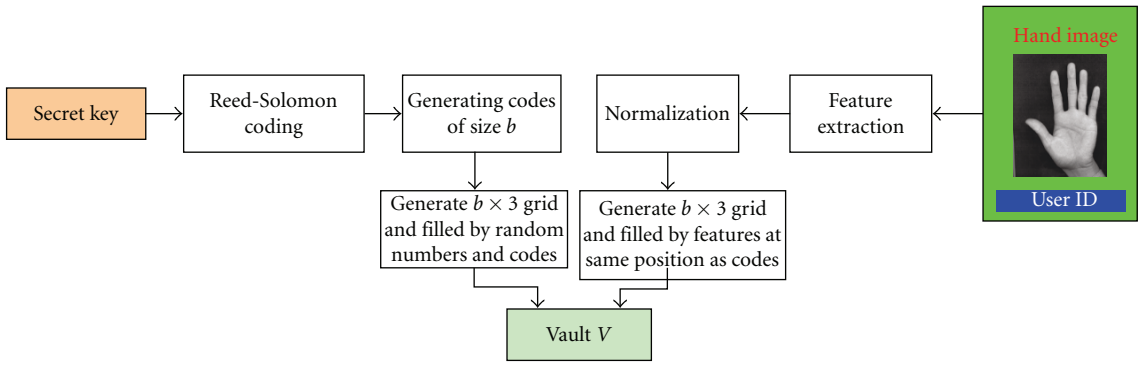

Figure 2: Block diagram for locking of the vault.

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 the vault using palmprint features is shown in Figure 2. The corresponding unlocking mechanism is illustrated in Figure 3. Once the procedure for the locking and unlocking of vault is determined, we fix the criteria for the genuine users to successfully open the vault while rejecting the imposter attempts. The vault is said to open successfully, if the codes retrieved from grid F (created by R-S codes) using the query palmprint features will be identically equal to the codes used at the time of locking. The inverse R-S codes can be applied to the retrieved codes to get back the original symmetric decryption key. Finally, this decryption key should successfully decrypt the secret private RSA key.

5.2. 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, that is, palmprint, from the acquired images is similar as detailed in [38]. The Discrete Cosine Transform (DCT) is used for the characterization of unique palmprint texture. The DCT is highly computationally efficient and therefore suitable for any online cryptosystem. (DCT is the basis of JPEG and several other standards (MPEG-1, MPEG-2 for TV/video, and H-263 for video-phones).) 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 blocks from each palmprint image. The DCT coefficients from each of these N square block pixels, that is, $f(x, y)$, are

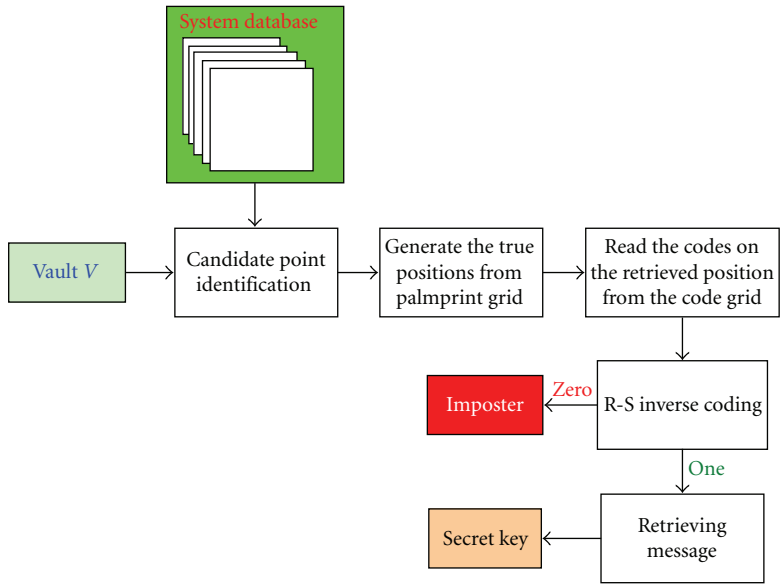

Figure 3: Block diagram for unlocking of the vault.

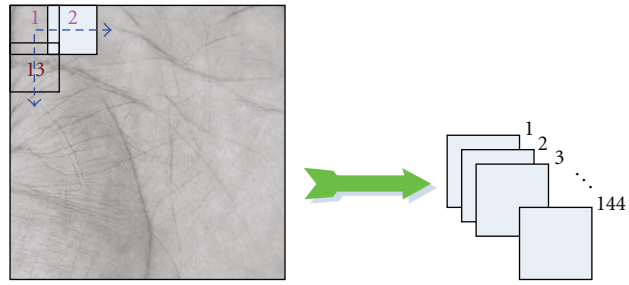

Figure 4: Localization of 144 overlapping palmprint image subblocks for feature extraction.

obtained as follows:

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

$$\varepsilon(u) = \varepsilon(v) = \begin{cases} \sqrt{\frac{2}{N}} & \text{for } u \neq 0, \\ \sqrt{\frac{1}{N}} & \text{for } u = 0. \end{cases} \tag{6}$$

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 intraclass variability in the palmprint features, mainly due to peg-free imaging, poses serious problems in the unlocking of the constructed vault by the genuine. The variability in feature vectors has been reduced with the help of Z-rule normalization. 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 interclass variability of the extracted features and very much helpful in fixing the tolerance for fuzzy vault.

6. 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 is created around the private key by generating grids using R-S codes and palmprint features. The evaluation is based on varying tolerance value over the range, and the corresponding false acceptance rate (FAR) and false rejection rate (FRR) are then computed. The palmprint database consisted of the left-hand images from the 85 users, and two images from each of the users are 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

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

users (i.e., 84 users) was considered as imposter matches. Thus our performance estimation, that is, FAR and FRR, is based on 84×85 imposter and 85 respective genuine attempts. The decisions from the FAR and FRR depend 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 FAR and FRR scores with the tolerance while Figure 5(b) illustrates the receiver operating characteristics (ROC). The RSA cryptosystem used in our program has some variations in key length [39]. The RSA implementation has utilized the string format to generate the RSA keys, and its length varies from 306 to 309 (detailed in Section 6.1) [26]. As cryptographic keys are supposed to be same at each application, authentication rates can vary with each length size of the generated key. Table 1 illustrates the variation in experimental results (equal error rate) with the key length and the corresponding tolerance value.

6.1. 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 most of the prior work is focused on fingerprint. Recently, iris [19], face [33], and signature [40] have also been investigated and yielded promising results. However, summary of prior work presented in Table 2 suggests that much of the work has been simulated on a small dataset, such as [37] has used 9 users, [41] has used 10 users, and [9] 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 [22] therefore investigated the possible usage of palmprint 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.

Our experimental results illustrated the EER up to about 0.3% while achieving the FRR of 0% at 0.35% FAR. However, these results may be less convincing as other approaches [2, 15]; our system is more reliable and robust, as far as attacks on secret key are concerned. The experimental results in BioHashing are dependent upon security of tokenized (pseudo)random number, as reported in [12] and have to put additional efforts to secure these numbers. In contrast, our emphasis is to strengthen the cryptographic approaches for

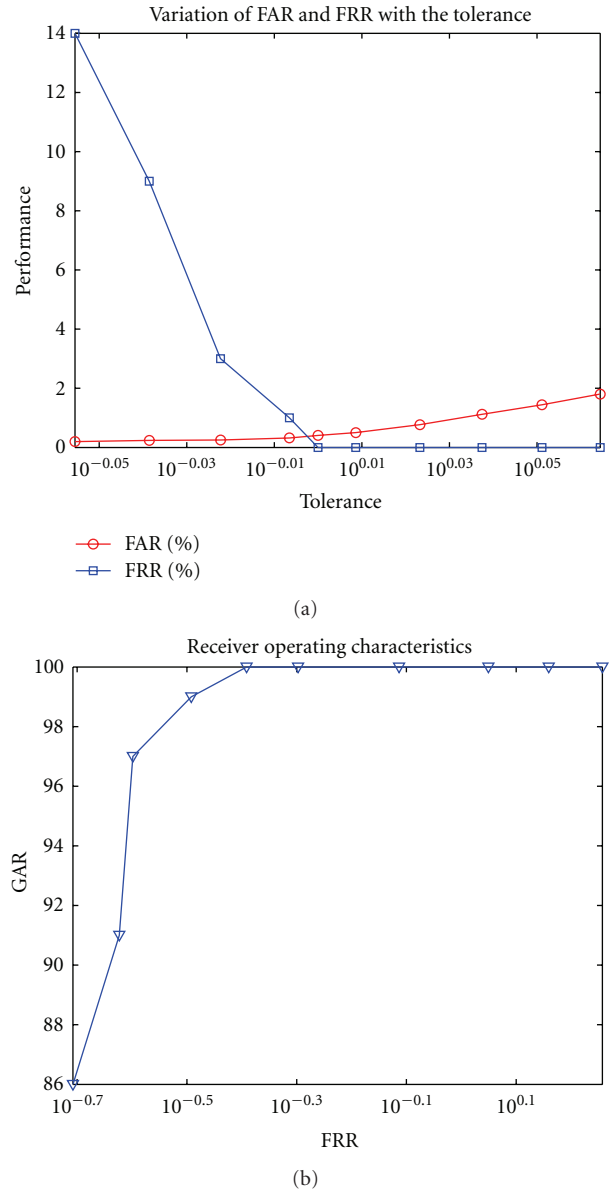

Figure 5: (a) The variations of the FAR and FRR characteristics with the tolerance for the palmprint-based cryptosystem, and (b) corresponding receiver operating characteristics.

encryption (the problems with symmetric and asymmetric approach have been discussed earlier in Sections 3.1.1-3.1.2) and withstand the attacks on secret key. Any secret document/information (of any length) can be encrypted by symmetric cryptographic approach (as symmetric approaches such as, DES, and AES are very efficient for the encryption of bulk data) and the secret symmetric key is again encrypted using asymmetric approach (to overcome dependency on secret symmetric key). Finally, the palmprint-based fuzzy vault is created around the private asymmetric key to prevent unauthorized disclosure of the key. At the decryption end, if the input palmprint template is able to open the vault (using matching criteria), the access to private key is granted. The rest is the conventional cryptographic mechanism as the

Table 2: Summary of related prior work.

Biometric	Feature	Error Correction Code	FRR (%)	FAR (%)	Reference	Database Size
fingerprint	Minutiae Points	RS Code	5	0	[42]	9 Users
Voice	Cepstrum coefficient	Discretization	20	NA*	[41]	10 Users
Signature	Dynamic time wrapping	Feature coding	28	1.2	[40]	25 Users
Iris	Gabor Feature	RS code and Hadamard Codes	0.47	0	[19]	70 Users
Fingerprint	Fourier transform	Majority code	12	35	[33]	20 Users
Fingerprint	Minutiae point	RS code	30	NA	[17]	NA*
Fingerprint	Minutiae points and helper data	RS code	3	0.24	[18]	100 Users (*FVC '02*)
Palmprint	DCT features	RS code	0	0.4	—	85

*NA—Not Available.

private key is used to decrypt symmetric key and finally the secret document. In fact, we propose a mixed cryptosystem which has advantage over both symmetric and asymmetric cryptography. The advantage of the proposed system lies in that it not only attempts to alleviate the shortcomings of symmetric key-based cryptosystem but also solves the problems involved in asymmetric key-based approach. The approach minifies dependency on secret key involved and alternatively investigates a more secure and promising system, as compared to BioHashing-based techniques.

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 the private key. The private and public keys are generated on publicly available RSA toolbox [26]. 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 the encryption exponent n is 64 bit. The two large primes are 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 satisfies the following equation:

$$n * sc \equiv 1 \pmod{si}, \quad \text{where } 1 < sc < si. \tag{7}$$

It can be observed from the above equation that more than one value of n can satisfy the congruence, and hence the length of the generated string (key) can vary. The prime numbers are randomly chosen and so are the values of si and n, and therefore 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 Table 1 illustrated all the possible variations in key length and the corresponding performance (EER) with the tolerance value. It can be observed from this table that as the key length varies (in the range 306 to 309), the system has different equal error rates at different tolerances. The minimum equal error rate is achieved when the key length is 307.

7. Conclusions

This paper has investigated a new approach to construct the cryptographic vault using palmprint features. In order to combine cryptography with palmprint features we have also incorporated the implementation of double encryption. This can efficiently reduce the possibility of hacking within a cryptosystem. The experimental results presented in Section 6 illustrate that the palmprint-based cryptosystem can operate at low EER (0.375%). The summary of the prior work, presented in Table 2, suggests that the palmprint can be used as a promising biometric in the construction of a cryptosystem. However, the work presented in Table 2 is not directly comparable; our motivation is to mere outline the effectiveness of the proposed work. The cryptosystem investigated in this paper employed localized spectral features from the palmprint. The multiple feature representation, such as detailed in [34], can offer more reliable characterization of features, and therefore cryptosystem based on multiple-palmprint representation can be considered for the extension of this work.

Acknowledgment

This work was partially supported by the research Grant from the Department of Science and Technology, Government of India (Grant no. 100/IFD/1275/2006-2007).

References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[2] A. Kong, D. Zhang, and M. Kamel, "Three measures for secure palmprint identification," *Pattern Recognition*, vol. 41, no. 4, pp. 1329–1337, 2008.

[3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[4] W. Stallings, *Cryptology and Network Security: Principles and Practices*, Prentice Hall, Upper Saddle River, NJ, USA, 3rd edition, 2003.

[5] J. Nam, Y. Lee, S. Kim, and D. Won, "Security weakness in a three-party pairing-based protocol for password authenticated key exchange," *Information Sciences*, vol. 177, no. 6, pp. 1364–1375, 2007.

[6] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proceedings of the IEEE International Symposium on Information Theory*, p. 408, Lausanne, Switzerland, June-July 2002.

[7] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," in *Proceedings of the 5th Audio- and Video-Based Biometric Person Authentication (AVBPA '05)*, vol. 3546 of *Lecture Notes in Computer Science*, pp. 310–319, Springer, Hilton Rye Town, NY, USA, July 2005.

[8] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 148–157, Oakland, Calif, USA, May 1998.

[9] 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.

[10] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," in *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pp. 73–82, 1999.

[11] T. Connie, A. Teoh, M. Goh, and D. Ngo, "PalmHashing: a novel approach for cancelable biometrics," *Information Processing Letters*, vol. 93, no. 1, pp. 1–5, 2005.

[12] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of BioHashing and its variants," *Pattern Recognition*, vol. 39, no. 7, pp. 1359–1368, 2006.

[13] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213673,00.html.

[14] http://world.std.com/~franl/crypto/one-time-pad.html.

[15] X. Wu, D. Zhang, and K. Wang, "A palmprint cryptosystem," in *Proceedings of IAPR/IEEE International Conference on Biometrics (ICB '07)*, vol. 4642 of *Lecture Notes in Computer Science*, pp. 1035–1042, August 2007.

[16] A. Juel and M. Wttenberg, "A fuzzy vault commitment scheme," in *Proceedings of the 6th ACM Conference on Computer and Communications Security*, G. Tsudik, Ed., pp. 408–412, 2002.

[17] U. Uludag and A. K. Jain, "Fuzzy fingerprint vault," in *Proceedings of Biometrics: Challenges Arising from Theory and Practice*, pp. 13–16, Cambridge, UK, August 2004.

[18] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: implementation and performance," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 744–757, 2007.

[19] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[20] T. C. Calancy, N. Kiyavash, and D. J. Lin, "Secure smartcard-based fingerprint authentication," in *Proceedings of the ACM SIGMM Multimedia Workshop on Biometrics Methods and Applications*, pp. 45–52, Berkeley, Calif, USA, 2003.

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

[22] A. Kumar and A. Kumar, "A palmprint-based cryptosystem using double encryption," in *Biometric Technology for Human Identification V*, vol. 6944 of *Proceedings of SPIE*, pp. 1–9, Orlando, Fla, USA, March 2008.

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

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

[25] K. A. Nishimura, S. J. Wenstrand, and G. Panotopoulos, "Biometric identification device," European patent EP1760667, July 2007.

[26] http://www.wipo.int/pctdb/en/wo.jsp?wo=2001092994&IA;=WO2001092994&DISPLAY;=DESC.

[27] P. W. Dent, "Cryptographic method and system for double encryption of messages," US patent no. 6904150, June 2005.

[28] M. J. Fischer, "Cryptography and computer security," Lecture Note-5 CPSC 467a, Department Of Computer Science, Yale University, http://zoo.cs.yale.edu/classes/cs467/2006f/attach/ln05.html.

[29] H. Ng, "Simple pseudorandom number generator with strengthened double encryption (Cilia)," http://eprint.iacr.org/2005/086.pdf.

[30] G. Immega, T. Vlaar, G. Vanderkooy, and K. Tucker, "Method for biometric encryption of email," European patent no. EP1290534, December 2003.

[31] Y.-H. Doh, J.-S. Yoon, K.-H. Choi, and M. S. Alam, "Optical security system for the protection of personal identification information," *Applied Optics*, vol. 44, no. 5, pp. 742–750, 2005.

[32] Z. Liu and S. Liu, "Double image encryption based on iterative fractional Fourier transform," *Optics Communications*, vol. 275, no. 2, pp. 324–329, 2007.

[33] A. Goh and D. C. L. Ngo, "Computation of cryptographic keys from face biometrics," in *Communications and Multimedia Security*, vol. 2828 of *Lecture Notes in Computer Science*, pp. 1–13, Springer, Berlin, Germany, 2003.

[34] A. Kumar and D. Zhang, "Personal authentication using multiple palmprint representation," *Pattern Recognition*, vol. 38, no. 10, pp. 1695–1704, 2005.

[35] A. Kong and D. Zhang, "Compititive coding scheme for palmprint verification," in *Proceedings of the International Conference on Pattern Recognition (ICPR '04)*, vol. 1, pp. 520–523, August 2004.

[36] A. Kumar, "Incorporating cohort information for reliable palmprint authentication," in *Proceedings of the 6th Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP '08)*, pp. 583–590, Bhubaneswar, India, December 2008.

[37] A. Nagar and S. Chaudhury, "Biometrics based asymmetric cryptosystem design using modified fuzzy vault scheme," in *Proceedings of the 18th International Conference on Pattern Recognition (ICPR '06)*, vol. 4, pp. 537–540, Hong Kong, August 2006.

[38] A. Kumar, D. C. M. Wong, H. C. Shen, and A. K. Jain, "Personal authentication using hand images," *Pattern Recognition Letters*, vol. 27, no. 13, pp. 1478–1486, 2006.

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

[40] H. Feng and C. C. Wah, "Private key generation from on-line handwritten signatures," *Information Management and Computer Security*, vol. 10, no. 4, pp. 159–164, 2002.

[41] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," in *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 202–213, May 2001.

[42] F. Monrose, M. K. Reiter, and R. Wetzel, "Password hardening based on keystroke dynamics," *International Journal of Information and Computer Security*, vol. 1, no. 2, pp. 69–83, 1999.