Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme

Abhishek Nagar
Mathematics Department, IIT Delhi
mau01057@ccsun50.iitd.ac.in

Santanu Chaudhury
Electrical Engg. Department, IIT Delhi
santanuc@ee.iitd.ac.in

Abstract

We propose a novel biometrics cryptosystem where one can send and receive secure information using just the fingerprints. This cryptosystem is a judicious blend of the asymmetric cryptosystem like RSA and the symmetric Fuzzy Vault Scheme having the advantages of both the aforementioned cryptosystems. We have proposed a modification of the Fuzzy Vault Scheme to make it more robust against variations in the values of biometric features. Finally we propose the use of invariant features as a key to producing a hierarchical security system where the same key (fingerprint) can be used to generate encrypted messages at different levels of security.

1. Introduction

Inconvenience in ensuring the integrity of the key is one of the major problems associated with cryptosystems that require user to carry smart cards or remember passwords. People have tried to design cryptosystems based on biometrics to eliminate some of the problems but have yet not been successful in utilizing the full power of biometrics. C. H. Lin, and Y. Y. Lai [5] developed a server login protocol using biometrics to ensure non-repudiation but it still requires smart card and password, which highly undermines its usability. Another authentication system developed by M. Savvides, B.V.K. Vijaya Kumar, and P.K. Khosla using cancelable biometrics [1] also uses a smart card which contains coded biometric data to be matched with the one extracted in real time from the user for authentication. In our paper the main focus is on designing a biometric cryptosystem to send encrypted messages to the receivers without the use of any smart card or remembering any password and at the same time ensuring optimum security.

In spite of having advantages like non-repudiation and convenience of usage etc., biometrics has certain issues [4] that restrict its use as a key to a cryptosystem. One of the problems with biometrics is that the number of biometrics that can be obtained from a person is limited and their compromise would mean that that particular biometric is rendered useless forever. To eliminate this problem cancelable biometrics [1] has been proposed in literature. A cancelable biometric is a transformed biometric such that a number of keys can be obtained from a single biometric using different transformations. Another major problem with using biometrics is their nonrepeatability i.e. each time one gets a biometric from a person its value is not the same as that of one taken previously. To alleviate this problem Juels and Sudan have proposed a Fuzzy Vault Scheme [2] which utilizes the error-correcting codes such as the Reed-Solomon codes to produce a symmetric cryptosystem that can tolerate some differences in the values of the encryption and decryption keys. But being symmetric, the usage of Fuzzy Vault Scheme is highly restricted in secure message sending protocols as the receiver has the encryption key and hence is able to generate fake messages. Through this project we have tried to incorporate the asymmetric RSA cryptosystem into the Fuzzy Vault Scheme in order to utilize the advantages of biometrics in the domain of asymmetric cryptosystems. In addition we have incorporated a hierarchy of security levels into our cryptosystem using the invariant properties of permutation group. This is highly desirable for information exchange in an organizational setup.

We have used fingerprint features as proposed by Anil. K. Jain et al. [3] for our system but this approach is not limited to fingerprints, in fact other biometrics like iris data, face features etc can also be used with minor calibrations.

2. Modified Fuzzy Vault Scheme

0-7695-2521-0/06/$20.00 (c) 2006 IEEE

The Fuzzy Vault Scheme has some drawbacks in regards to its efficiency in generating a cryptosystem as this scheme does not utilize the order of the feature elements of the biometrics used. The locking set is generated by evaluating the key polynomial at the values present in the biometric feature vector. Now if two elements have nearly the same value in the feature vector, they are taken as the same element thereby decreasing the number of elements on which the polynomial is to be evaluated. Hence the security level is decreased.

In our proposed Modified Fuzzy Vault Algorithm, we have tried to utilize the order of the feature vector to create a more stable and secure cryptosystem. In this new scheme we evaluate the polynomial on all the points in the domain but we hide the evaluations under the legitimate points of the vault. Since now the order is also taken into account, so we have devised a new and efficient scheme to sieve out the legitimate points to open the vault.

2.1. Design of the Modified Fuzzy Vault

The construction of the modified Fuzzy Vault is described as a sequence of sequence of steps as follows:

1. Encode the message using the Reed-Solomon codes to get the code C of length n.
2. Each element of the code C is placed on a grid of size nx3 such that ith row of the grid contains ith code element placed randomly in one of the 3 places. Call this gridC.
3. Place the biometric template of length n on a similar grid such that its position and order coincides with that of the code C in code grid. Call this gridB.
4. Fill rest of the elements of gridC with random numbers in the appropriate range.
5. Fill the elements of the gridB in such a way that each row becomes an arithmetic progression of distance equal to the tolerance value, FV tolerance.

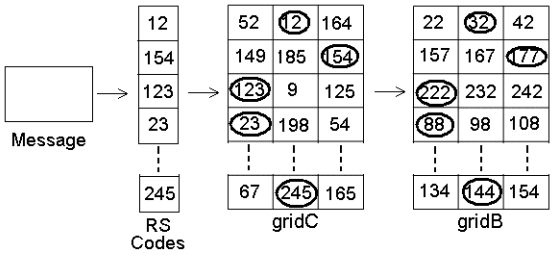

Figure 1. gridB and gridC of the Modified Fuzzy Vault where circles indicate legitimate points

To unlock the Vault we only need to know the correct positions of the legitimate elements in gridC or gridB. The sequence of numbers that we get as the legitimate points of gridC is nothing but the reed-solomon code for the encrypted message. This reed-solomon code can be easily decoded using any of the standard algorithms to get back the desired message.

Once the receiver has the actual biometric feature, the legitimate-point sieving algorithm is just to select one point out of three from each row of gridB which is nearest to the corresponding biometric value. The security of this scheme is of the order of 10^{100} if we take n to be 255 i.e. opening the vault is equivalent to selecting the correct one out of more than 10^{100} choices taking care of the error-correcting capabilities of the RS codes. The reason for choosing the chaff points at a distance of FV_tolerance is that the attacker should not be able to sieve out the chaff points only on the basis of their unexpectedly highly varying values.

Since RS codes have an error correcting capacity of (n-k)/2 where n is length of code and k is length of secret message, we are able to have a control over it by increasing k by appending some random digits to the original message. We refer to this error correcting capacity of the vault as Permissible Error in our paper. Being able to control k is highly desirable as we can calibrate the cryptosystem according to the quality of the biometric being used in the cryptosystem.

3. Secure Transformation for Cancelability

Since the biometric features like fingerprints are easily accessible and hence not secure, so we need to incorporate some secure information into the biometric feature to be able to use these as a key to the cryptosystem. Also since the number of usable biometrics known to date is limited so we cannot afford to compromise these while being used as a key. To overcome these problems, we have followed the approach used in [1], the cancelable biometrics, where the biometric template is convolved with a secret 2D random signal to create a secure biometric.

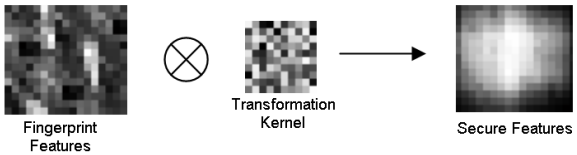

Figure 2. Creating Secure Features

Using this approach both our problems are solved as without knowing the random signal one cannot get the secure biometric and one can easily discard a secure biometric by discarding the corresponding random signal. In this research, we have converted the biometric template of length 255 to a matrix of size 15*17 and convolved with a random kernel of the size 10*10 to get the Secure Features.

4. Hierarchical Security using Invariant Features

Since in an organizational setup it is desirable to have a system of sending secure messages to all the people above a certain rank, we have incorporated a hierarchical group security protocol in our system using transformation invariants. Now instead of Secure Feature we use its certain invariant features as a key to the cryptosystem.

Let us divide the Secure Feature vector into blocks of size 4 and sort each block separately to form the new key for the cryptosystem. The advantage of this new key is that if we have a key generated using block-size 2, we can easily generate key corresponding to block-size 2x for some positive integer 'x' and hence it is called the invariant feature. We have used precisely this scheme to implement hierarchical security where the block-size determines the security level. The bigger the block size, the lesser is the security. The Secure Feature vector is appended with zeros to make its length equal to 2^n for some n and a key corresponding to security level 's' is generated using block-size 2^{i+1}. A vault created at a certain security level 's' is meant to be opened only by people having the keys corresponding to security level at least 's'.

This special permutation is a good choice for the transformation since it does not vary the values of elements of the Secure Feature vector. This is a highly desirable property because biometrics is non-repeatable and we would not like a scheme which blows up the error. The only problem with this approach is that if the error in the re-extracted Secure Feature is substantially high, it can change the order of the elements in their respective blocks. Hence the number of errors will be equal to the number of positions an element has shifted in the sorted order in a particular block. But this error is again not too substantial because of the small block – sizes.

The hierarchical security implementation is not just limited to the aforementioned permutations but any other set of transformations which has the desired hierarchical structure and stability properties.

5. Design of the Complete Cryptosystem

The Fuzzy Vault scheme described previously has a drawback that the receiver is also able to generate the vault pretending to be the actual sender. To alleviate this problem, we add some extra information in the encrypted message which could be easily verified by the receiver but not replicated for creating a fake vault. For this purpose we have used the RSA cryptosystem to design a system as depicted by the figure 3.

The system primarily consists of a number of encryption modules linked to a server for information transfer. Each module has its own RSA security protocol (128 bit) such that the encryption key is secured with the module and the decryption key and the field is made public by sending it to main server. Each module can register a number of users. While registering a user, it generates a secure transformation for that particular user which is kept secure inside the module.

Now we shall list the complete set of steps followed to send a document using this system.

1. System takes the fingerprint of the user and extracts the features from it.
2. Fingerprint Features are transformed to Secure Features using the Secure Transformation registered with the module.
3. An RSA cryptosystem (32 bit) is initialized having Field n, Encryption Key e, and Decryption Key d.

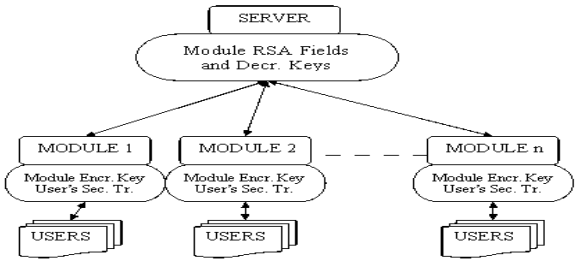

Figure 3. System Design

4. Document is divided into chunks of appropriate length and encrypted using e.
5. Random digits are appended to d, which is to be secured in the fuzzy vault so that the required value of Permissible Error is achieved (10 in our exp.).
6. Invariant Features corresponding to the desired security level are extracted.
7. Modified Fuzzy Vault containing appended d is created over the Invariant Features.
8. The created Vault is encrypted using the module encryption key and is sent to receiver along with the encrypted document and required identifications and values.

The receiver is supplied with the fuzzy vault unlocking key, i.e. the invariant features corresponding to the desired security level, once for all the transactions. To receive the document, the receiver does the following:

1. Decrypt the vault using the publicly available module decryption key.
2. If security level of vault is lesser than security level of receiver, generate the new key corresponding to vault security level.
3. Open vault using the key to get document decryption key, d.

4. Decrypt document using first few desired digits of d.

The encryption using the module encryption key confirms the validity of the message that the message is sent through the encryption module used by a legitimate user and not using the unlocking key available with the receiver as one can not input directly the Secure Features to the encryption module which are actually calculated using the fingerprint. Hence the system develops the required asymmetric nature.

6. Experiments

We have tested our Modified Fuzzy Vault on fingerprint features extracted using the gabor feature based filterbank as proposed by A.K. Jain et al. [3]. For this purpose, we took a set of 29 fingerprint images (size: 256x256) from 9 people. A feature vector of 384 elements is calculated as described in the aforesaid paper. These values are then normalized to a range of 0 to 255 for ease in creating the fuzzy vault and defining the tolerance values. The false acceptance rates (FAR) and false rejection rates (FRR) corresponding to these are shown in the Table 1. The error correcting capacities of the Fuzzy Vault is taken to be 10 and at the second highest security level i.e. block-size 8 where for the highest level, it is 4.

Table 1. FAR and FRR for Modified Fuzzy Vault

FV_tol.	FAR (%)	FRR (%)	**FV_tol.**	FAR (%)	FRR (%)
2	0	5	12	2.78	0
4	0	0	14	9.72	0
6	0	0	16	11.1	0
8	0	0	18	16.7	0
10	2.78	0	20	19.4	0

Table 2. FAR for hierarchical Security

Enc. Sec. Level	**Dec. Sec. Level**	**FAR(%), FV_tol. =**		
		4	**6**	**8**
1	2	0	0	0
1	3	0	0	0
2	3	5	5	0

Further we tested our system for the hierarchical security by calculating the false acceptance rate while trying to decipher a message encoded with higher security using a key with lower security, the results are shown in Table 2.

7. Conclusion

We have presented the design of a novel asymmetric cryptosystem based on biometrics having features like hierarchical group security and which eliminates the use of passwords and smart cards as opposed to earlier cryptosystems like [5,6] though it requires special hardware support which is present with any other biometrics system. This paper presents a new direction of research in the field of asymmetric biometric cryptosystems which is highly desirable in order to get rid of passwords and smart cards completely. Through the experiments we have shown the validity of the proposed Modified Fuzzy Vault Scheme and the hierarchical security structure. .

8. References

[1] M. Savvides, B.V.K. Vijaya Kumar, and P.K. Khosla, "Cancelable biometric filters for face recognition", *ICPR*, 23-26 Aug. 2004, pp. 922-925 Vol.3.

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

[3]A.K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-basedFingerprint Matching", *IEEE Trans. Image Process.*, 2000, 846–859.

[4] U. Uludag, S. Pankanti, S. Prabhakar, and A.K Jain, "Biometric cryptosystems: issues and challenges", *Proceedings of the IEEE*, Volume 92, Issue 6, June 2004, pp. 948 – 960.

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

[6] T.C. Clancy, N. Kiyavash, and D.J. Lin, "Secure smartcard-based fingerprint authentication", *ACM Workshop on Biometrics: Methods and Applications*, Nov. 2003, pp. 45-52.

[7] U. Uludag, A. Jain, "Fuzzy Fingerprint Vault", *Proc. Workshop: Biometrics: Challenges Arising from Theory to Practice*, pp.1316, Aug 2004.