ISSN:0975-9646

High Secure Crypto Biometric Authentication Protocol

K Hemanth, Srinivasulu Asadi, Dabbu Murali, N Karimulla and M Aswin

ABSTRACT: Concerns on widespread use of biometric authentication systems are primarily centered around template security, revocability, and privacy. The use of cryptographic primitives to bolster the authentication process can alleviate some of these concerns as shown by biometric cryptosystems. In this paper, we propose a *provably secure* and *blind* biometric authentication protocol, which addresses the concerns of user's privacy, template protection, and trust issues. The protocol is blind in the sense that it reveals only the identity, and no additional information about the user or the biometric to the authenticating server or vice-versa. As the protocol is based on asymmetric encryption of the biometric data, it captures the advantages of biometric authentication as well as the security of public key cryptography. The authentication protocol can run over public networks and provide nonrepudiable identity verification. The encryption also provides template protection, the ability to revoke enrolled templates, and alleviates the concerns on privacy in widespread use of biometrics. The proposed approach makes no restrictive assumptions on the biometric data and is hence applicable to multiple biometrics. Such a protocol has significant advantages over existing biometric cryptosystems, which use a biometric to secure a secret key, which in turn is used for authentication. We analyze the security of the protocol under various attack scenarios. Experimental results on biometric datasets (finger print) show that carrying out the authentication in the encrypted domain does not affect the accuracy, while the encryption key acts as an additional layer of security.

General Terms: Artificial neural networks, biometrics, cryptosystems, Privacy, public key cryptography, security, support vector machines (SVMs).

Keywords — Cryptography, Authentication, Biometric cryptosystems, Support Vector Machine, Wavelets and Neural networks.

1. INTRODUCTION

Biometric authentication systems are gaining wide-spread popularity in recent years due to the advances in sensor technologies as well as improvements in the matching algorithms that make the systems both secure and cost-effective. They are ideally suited for both high security and remote authentication applications due to the non-repudiable nature and user convenience. Most biometric systems assume that the template in the system is secure due to human supervision (e.g., immigration checks and criminal database search) or physical protection (e.g., laptop locks and door locks). However, a variety of applications of authentication need to work over partially secure or insecure networks such as ATM networks or the Internet. Authentication over insecure public networks or with untrusted servers raises more concerns in privacy and security. The primary concern is related to the security of the plain biometric templates, which cannot be replaced, once they are compromised. The privacy concerns arise from the fact that the biometric samples reveal more information about its owner (medical, food habits, etc.) in addition to the identity. Widespread use of biometric authentication also raises concerns of tracking a person, as every activity that requires authentication can be uniquely assigned to an individual A biometric system that can work securely and reliably under such circumstances can have a multitude of applications varying from accessing remote servers to e-shopping over the Internet. For civilian applications, these concerns are often more serious than the accuracy of the biometric.

The primary problem here is that, for Alice, Bob could either be incompetent to secure her biometric or even curious to try and gain access to her biometric data, while the authentication is going on. So Alice does not want to give her biometric data in plain to Bob. On the other hand, Bob does not trust the client as she could be an impostor. She could also repudiate her access to the service at a later time. For both parties, the network is in-secure. A biometric system that can work securely and reliably under such circumstances can have a multitude of applications varying from accessing remote servers to e-shopping over the Internet. The primary concerns that need to be addressed for widespread adoption of biometrics. For civilian applications, these concerns are often more serious than the accuracy of the biometric.

If the user is able to authenticate himself using a strongly encrypted version of his biometricof the concerns on privacy and security can be addressed. How- ever, this would require the server to carry out all the compu- tations in the encrypted domain itself. Unfortunately, encryption algorithms are designed to remove any similarity that ex- ists within the data to defeat attacks, while pattern classification algorithms require the similarity of data to be preserved to achieve high accuracy. In other words, security/privacy and accuracy seem to be opposing objectives. Different secure authen- tication solutions try to make reasonable trade-offs between the opposing goals of security and accuracy, in addition to making specific assumptions about the representation or biometric being used.

2. RELATED WORK

Existing System and Details: The previous work in the area of encryption-based security of biometric templates tends to model the problem as that of building a classification system that separates the genuine and impostor samples in the encrypted domain. However, a strong encryption mechanism destroys any pattern in the data, which adversely affects the accuracy of verification. Hence, any such matching mechanism necessarily makes a compromise between template security (strong encryption) and accuracy (retaining patterns in the data). The primary difference in our approach is that we are able to design the classifier in the plain feature space, which allows us to maintain the performance of the biometric itself, while carrying out the authentication on data with strong encryption, which provides high security/ privacy. Over the years a number of attempts have been made to address the problem of template protection and privacy concerns and despite all efforts, puts it, “a template protection scheme with provable security and acceptable recognition performance has thus far remained elusive”. In this section, we will look at the existing work in light of this security-accuracy dilemma, and understand how this can be overcome by communication between the authenticating server and the client. Detailed reviews of the work on template protection can be found.

The first class of feature transformation approaches known as Salting offers security using a transformation function seeded by a user specific key. The strength of the approach lies in the strength of the key. A classifier is then designed in the encrypted feature space. Although the standard cryptographic encryption such as AES or RSA offers secure transformation functions, they cannot be used in this case. The inherent property of dissimilarity between two instances of the biometric trait from the same person, leads to large differences in their encrypted versions. This leads to a restriction on the possible functions that can be used and in salting, resulting in a compromise made between security and the performance. Some of the popular salting-based approaches are biohashing and salting for face template protection. Moreover, salting-based solutions are usually specific to a biometric trait, and in general do not offer well-defined security. Kong *et al.* do a detailed anal- ysis of the current biohashing-based biometric approaches. They conclude that the zero equal error rate (EER) reported by many papers is obtained in carefully set experimental conditions and unrealistic under assumptions from a practical view point.

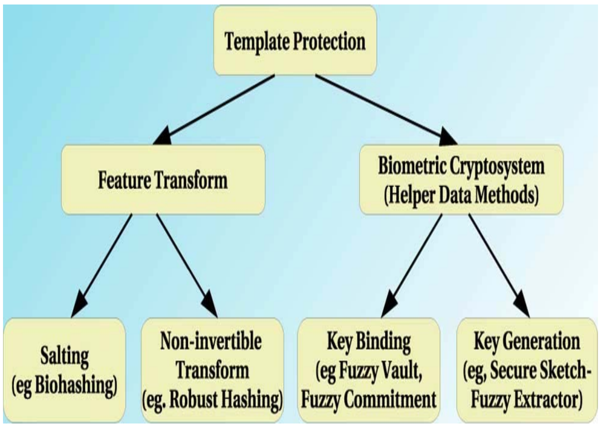

Template Protection
Feature Transform
Biometric Cryptosystem (Helper Data Methods)
Salting (eg Biohashing)
Non-invertible Transform (eg, Robust Hashing)
Key Binding (eg Fuzzy Vault, Fuzzy Commitment
Key Generation (eg, Secure Sketch-Fuzzy Extractor)

Fig. 1 Categorization of Template Protection Schemes

The second category of approaches identified as noninvert- ible transform applies a trait specific noninvertible function on the biometric template so as to secure it. The parameters of the transformation function are defined by a key which must be available at the time of authentication to transform the query feature set. Some of the popular approaches that fall into this category are robust hashing and cancelable templates. Cancelable templates, allows one to replace a leaked template, while reducing the amount of information revealed through the leak, thus addressing some of the privacy concerns. However, such methods are often biometric specific and do not make any guarantees on preservation of privacy, especially when the server is not trusted. Methods to detect tampering of the enrolled templates help in improving the security of the overall system.

The third and fourth classes, shown in Fig., are both variations of Biometric cryptosystems. They try to integrate the ad- vantages of both biometrics and cryptography to enhance the overall security and privacy of an authentication system. Such systems are primarily aimed at using the biometric as a protection for a secret key (key binding approach) or use the bio- metric data to directly generate a secret key (key generation approach). The authentication is done using the key, which is unlocked/generated by the biometric. Such systems can op- erate in two modes in the case of remote authentication. In the first case, the key is unlocked/generated at the client end, which is sent to the server for authentication, which will ensure se- curity of the template, and provide user privacy. However, this would become a key-based authentication scheme and would lose the primary advantage of biometric authentication, which is its nonrepudiable nature. In the second case, the plain biometric needs to be transmitted from the user to the server, both during enrollment and during authentication. This inherently leaks more information about the user than just the identity, and the users need to trust the server to maintain their privacy. Moreover, authenticating over an insecure network makes the plain biometric vulnerable to spoofing attacks.

Blind Authentication addresses all these concerns,

1) The ability to use strong encryption addresses template protection issues as well as privacy concerns.

2) Non-repudiable authentication can be carried out even be-

Tween nontrusting client and server using a trusted third party solution.

3) It provides provable protection against replay and client-side attacks even if the keys of the user are compromised.

4) As the enrolled templates are encrypted using a key, one can replace any compromised template, providing revocability, while allaying concerns of being tracked.

2.1. Demerits of existing system

- Less Privacy.
- Less Security.
- Difficult to perform Verification..

2.2. Proposed System

Blind authentication is able to achieve both strong encryption-based security as well as accuracy of a powerful classifiers such as support vector machines (SVMs) and neural networks. While the proposed approach has similarities to the blind vision scheme for image retrieval, it is far more efficient for the verification task. Blind Authentication addresses all the concerns mentioned

1) The ability to use strong encryption addresses template protection issues as well as privacy concerns.

2) Non-repudiable authentication can be carried out even between nontrusting client and server using a trusted third party solution.

3) It provides provable protection against replay and client side attacks even if the keys of the user are compromised.

4) As the enrolled templates are encrypted using a key, one can replace any compromised template, providing revocability, while allaying concerns of being tracked.

The framework is generic in the sense that it can classify any feature vector, making it applicable to multiple biometrics. Moreover, as the authentication process requires someone to send an encrypted version of the biometric, the nonrepudiable nature of the authentication is fully preserved, assuming that spoof attacks are prevented. The proposed approach does not fall into any of the categories. This work opens a new direction of research to look at privacy preserving biometric authentication.

2.3. Authentication

To perform authentication, the client locks the biometric test sample using her public key and sends the locked ID to the server. The server computes the products of the locked ID with the locked classifier parameters and randomizes the results. These randomized products are sent back to the client. During the second round, the client unlocks the randomized results and computes the sum of the products. The resulting randomized sum is sent to the server. The server derandomizes the sum to obtain the final result, which is compared with a threshold for authentication.

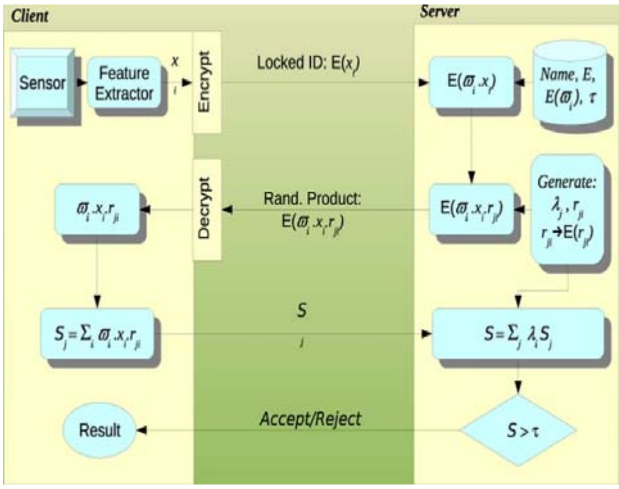

Client
Server
Sensor
Feature Extractor
x_i
Encrypt
Locked ID: $E(x_i)$
$E(\varpi_i . x_i)$
Name, E, $E(\varpi_i)$, τ
Decrypt
$\varpi_i . x_i r_{ji}$
Rand. Product: $E(\varpi_i . x_i r_{ji})$
$E(\varpi_i . x_i r_{ji})$
Generate: λ_j , r_{ji} $r_{ji} \rightarrow E(r_{ji})$
$S_j = \Sigma_i \varpi_i . x_i r_{ji}$
S_j
$S = \Sigma_j \lambda_i S_j$
Result
Accept/Reject
$S > \tau$

Fig. 2 Blind Authentication Process

We note that the computation of w.x requires a set of scalar multiplications, followed by a set of additions. As the encryption used (RSA) is homomorphism to multiplication, we can compute, E(wx)=E(w)E(x) at the server side. However, we cannot add the results to compute the authentication function. Unfortu- nately, sending the products to the client for addition will reveal the classifier parameters to the user, which is not desirable. We use a clever randomization mechanism that achieves this computation without revealing any information to the user. The randomization makes sure that the client can do the summation, while not being able to decipher any information from the products. The randomization is done in such a way that the server can compute the final sum to be compared with the threshold. The overall algorithm of the authentication process is given in Algorithm. Note that all the arithmetic operations that we mention in the encrypted domain will be modulo-operations, ., all the computations such as (a or b) will be done as (a or b) mod p , where p is defined by the Encryption Scheme Employeed.

2. 4. Enrollment

In the previous section, we assumed that server has copies of the client's public key 'E' as well as the classifier parameters that are encrypted using that key E(w)These were sent to the server during the enrollment phase by a trusted enrollment server. Assuming a third party as the enrollment server gives us a flexible model, where the enrollment could also be done by the client or the server if the trust allows. During the enrollment, the client sends samples of her biometric to the enrollment server, who trains a classifier for the user. The trained parameters are encrypted and sent to the authentication server, and a notification is sent back to the client. Fig.2. gives an overview of the enrollment process. The biometric samples sent by the client to the enrollment server could be digitally signed by the client and encrypted using the servers public key to protect it.

Advantages

- More Security
- Better Privacy
- Strong Encryption
- Used with wide variety of Biometric traits.

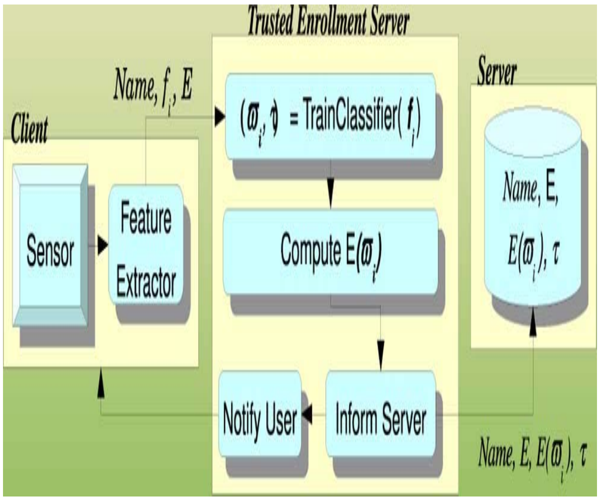

Trusted Enrollment Server
Client
Name, f_i, E
$(\varpi_i, \tau) = \text{TrainClassifier}(f_i)$
Server
Sensor
Feature Extractor
Compute $E(\varpi_i)$
Name, E, $E(\varpi_i)$, τ
Notify User
Inform Server
Name, E, $E(\varpi_i)$, τ

Fig.3 Enrollment based on a Trusted Third party.

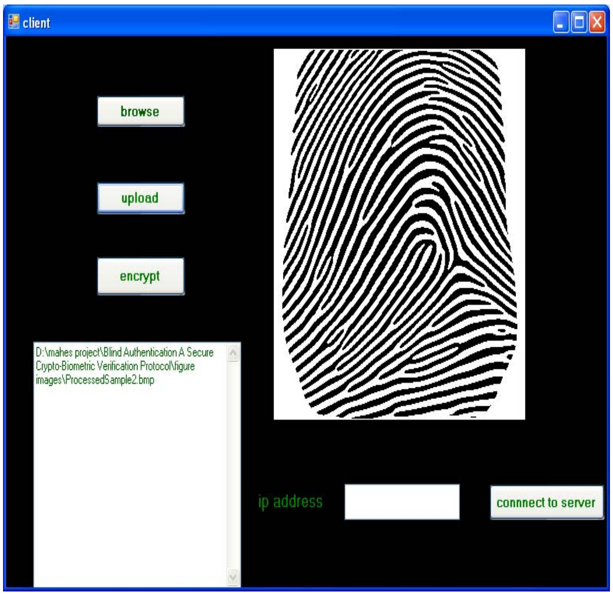
The use of a third party for enrollment also allows for long-term learning by the enrollment server over a large number of enrollments, thus improving the quality of the trained classifier. Algorithm 2 gives a step-by-step description of the enrollment process. Note that the only information that is passed from the enrollment server to the authentication server is the user's identity, public key, and Encrypted version of parameters.

3. AUTHENTICATION ALGORITHM

Steps

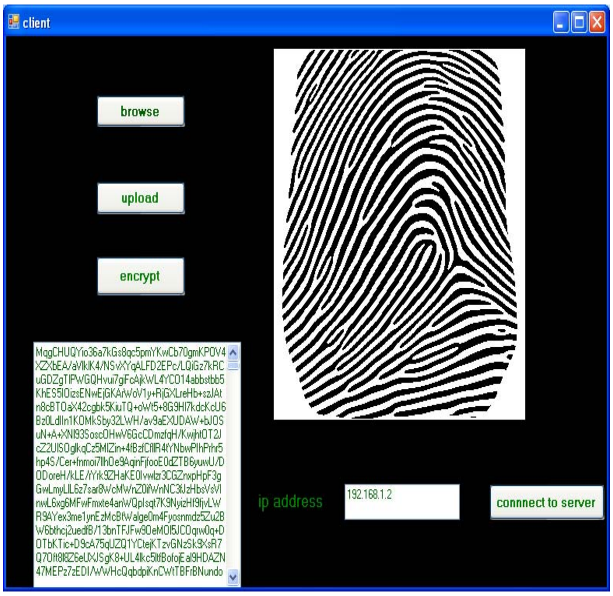
1. Client computes feature vector(x) from biometric data.
2. Feature vector is encrypted [E(x)] and sent to server.
3. Server Computes products by using Classifier parameters (w).
   i. server accepts identity of user when w.x< T
      w = parameters of classifier
      x = feature vector
      T = threshold value
   ii. Computation of w.x requires a set of scalar multiplications and additions.
   iii. Here encryption used is Homomorphic to multiplication so we cannot perform addition at server side.
4. Server performs multiple homomorphisms,
   i.e. E(wxr)= E(w)E(x)E(r)
   r = random variable.
   these random products are sent to client for addition.
5. Client decrypts products to get "wxr" and performs addition.
6. Client returns addition to server and then Server calculates final sum 'S'.
7. By comparing the final sum 'S' and threshod value 'T' ,
   if S>T, then we can accept the client else reject.

4. IMPLEMENTATION



```
D:\mahes project\Blind Authentication A Secure
Crypto-Biometric Verification Protocol\figure
images\ProcessedSample2.bmp
```

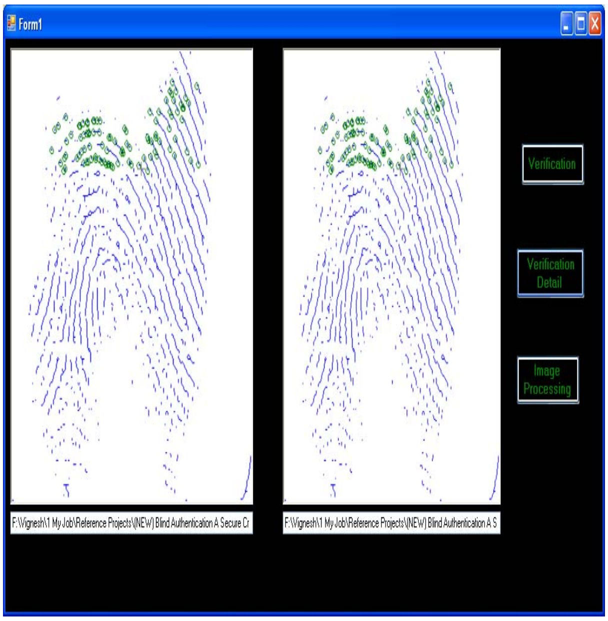
Fig: 4 Uploading and Encryption of Selected Biometric Sample.



192.168.1.2

MqgCHUQYio36a7kGs8qc5pmYKwCb70gmKPOV4
XZXbEA/aVlklK4/NSvXYqALFD2EPc/LQiGz7kRC
uGDZgTIPWGQHvui7giFcAjkWL4YC014abbstbb5
KhES5lOizsENwEjGKArWoV1y+RjGXLreHb+szJAt
n8cBTOaX42cgbk5KiuTQ+oWt5+8G9Hl7kdcKcU6
Bz0LdlIn1KOMkSby32LWH/av9aEXUDAW+bJOS
uN+A+XNI93SoscOHwV6GcCDmzfqH/KwjhtOT2J
cZ2UlSOglkqCz5MIZin+4fBzfCfllR4tYNbwPIhPrhr5
hp4S/Cer+fnmoi7llhOe9AqinFjfooE0dZTB6yuwU/D
ODoreH/kLE/rYrk9ZHaKE0lvwlzr3CGZnxpHpF3g
GwLmyLIL6z7sar8WcMWnZ0ifWnNC3fJzHbsVsVl
nwL6xg6MFwFmxte4anWQplsqt7K9NyizHf9fjvLW
R9AYex3me1ynEzMcBtWalge0m4Fyosnmdz5Zu2B
W6bthcj2uedfB/13bnTFJFw9OeMOl5JCOqrw0q+D
OTbKTic+D9cA75qUZQ1YCtejKTzvGNzSk9XsR7
Q7Oft8l8Z6eUXJSgK8+UL4lkc5ltfBofojEal9HDAZN
47MEPz7zEDI/wWHcQqbdpiKnCWtTBFrBNundo

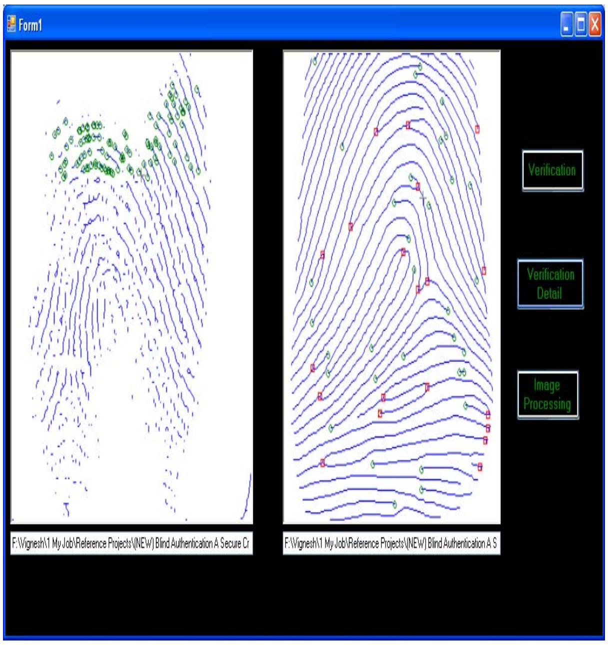
Fig: 5 this page shows encrypted data of Biometric Sample and sending this Encrypted data to Server.



F:\Vignesh\1 My Job\Reference Projects\(NEW) Blind Authentication A Secure Cr

F:\Vignesh\1 My Job\Reference Projects\(NEW) Blind Authentication A S

Fig: 6 This page shows Comparison of two Biometric Samples.



F:\Vignesh\1 My Job\Reference Projects\(NEW) Blind Authentication A Secure Cr

F:\Vignesh\1 My Job\Reference Projects\(NEW) Blind Authentication A S

Fig: 7.Page Showing Comparing of two Biometric Samples.

5. CONCLUSION

In this paper, we have proposed A Secure Crypto Biometric protocol for Authentication. The proposed blind authentication is extremely secure under a variety of attacks and can be used with a wide variety of biometric traits. Protocols are designed to keep the interaction between the user and the server to a minimum with no resort to computationally expensive protocols such as secure multiparty computation (SMC). As the verification can be done in real-time with the help of available hardware, the approach is practical in many applications. The use of smart cards to hold encryption keys enables applications such as biometric ATMs and access of services from public terminals. Possible extensions to this work include secure enrollment protocols and encryption methods to reduce computations. Efficient methods to do dynamic warping-based matching of variable length feature vectors can further enhance the utility of the approach and the great avenue is of this paper is to enhance by using Support Vector Machine, Wavelets and Neural networks.

6. REFERENCES

[1] A.K .Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp.4-20, Jan. 2004.

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

[3] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," Proc. IEEE, vol.92, no.6, pp.948-960, Jun. 2004.

[4] V. Blanz and T. Vetter, "Face recognition based on fitting a 3D morphable model," IEEE Trans. Pattern Anal. Mach. Intell., vol. 25-9, no.9, pp. 1063-1074, Sep.2003.

[5] D. M. Monro, S.Rakshit and D. Zhang, "DCT-based iris recognition," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 586-595, Apr. 2007.

[6] C. Gentry, "Fully homomorphism encryption using ideal lattices," STOC, pp. 169-178, 2009.

[7] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," in CVPR Biometrics Workshop, Jun.2007, pp. 1-7.

[8] Teoh, D. Ngo, and A. Goh,"Biohashing: Two factor authentication featuring fingerprint data and tokenized random number," Pattern Recognit., vol. 37, no. 11,pp. 2245-2255, Nov. 2004.

[9] C.-C. Yao, "How to generate and exchange secrets," Foundations of Computer Science, pp. 162-167, 1986.

[10] T. E. B. Walter and J. Scheirer, "Cracking fuzzy vaults and biometric encryption," in Biometrics Symp., Maryland, 2007, pp. 1-6.

[11] T. Mitchell, Machine Learning. New York: McGraw-Hill, 1997.

[12] Gnu Multiple Precision Arithemetic Library [Online]. Available: http://gmplib.org/.

[13] V. N. W. A. Ratanamahatana, Hand geometry verification using time series representation Sep. 2007.

[14] T. Boult, W. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: Accuracy and Security analysis," in IEEE Conf. Computer Vision and Patter Recognition (CVRR), Jun. 2007, pp.1-8.

[15] K. Nagai, H. Kikuchi, W. Ogata, and M. Nishigaki, "Zerobio: Evaluation and development of asymmetric fingerprint authentication system using oblivious neural network evaluation protocol," in 2nd Int. Conf. Availability, Reliability and Security (ARES), Apr. 2007, pp.1155-1159.

[16] A. Menezes P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC Press 1996.

[17] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issue and challenges," Proc. IEEE, vol. 92, no. 6, pp.948-960, Jun. 2004.

[18] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach. Intell., vol.29, no.4 Apr 2007.

AUTHORS BIOGRAPHY

K Hemanth received B.Tech degree in Information Technology from JNTUA, Anantapur in 2011, his research areas are Image Processing, Information Security, Database Management Systems and Software Engineering. khemanth9999@gmail.com.

Asadi Srinivasulu received the B Tech (CSE) from Sri Venkateswara University, Tirupati, India in 2000 and M.Tech with Intelligent Systems in IT from Indian Institute of Information Technology, Allahabad (IIIT) in 2004 and he is pursuing Ph.D in CSE from J.N.T.U.A, Anantapur, India. He has got 10 years of teaching and industrial experience. He served as the Head, Dept of Information Technology, S V College of Engineering, Karakambadi, Tirupati, India during 2007-2009. His areas of interests include Data Mining and Data warehousing, Intelligent Systems, Image Processing, Pattern Recognition, Machine Vision Processing and Cloud Computing. He is a member of IAENG, IACSIT. He has published more than 20 papers in International journals and conferences. Some of his publications appear in IJCA, IJCSET and IJCSIT digital libraries. He visited Malaysia and Singapore. srinu_asadi@yahoo.com

N Karimulla received B.Tech degree in Information Technology from JNTUA, Anantapur in 2011, his research areas are Data warehousing and Data Mining, Database Management Systems and Software Engineering. khemanth9999@gmail.com.

Dabbu Murali received B.Tech degree in Computer Science and Engineering from JNTUH, Hyderabad in 2002 and M.Tech degree in Computer Science from JNTUH in 2006. He is pursuing Ph.D JNTUH, Hyderabad. He has 9 years of experience in teaching. Currently working on Data warehousing Data mining recent trends in Computer Centre Laboratory at JNTU, Hyderabad, and his research areas Data Mining Pattern reorganization. dabbumurali@yahoo.com

M Aswin received B.Tech degree in Information Technology from JNTUA, Anantapur in 2011, his research areas are Image Processing, Data warehousing and Data Mining, Database Management Systems and Software Engineering. maswintpt@gmail.com