Encryption of Biometric Templates using One Time Biometric Transform

Aditya Abhyankar, Amit Vijayat, Sunil Kumar and Stephanie Schuckers

***Abstract*— Securing biometric information has become essential with growing biometric applications in different sectors of society. Vulnerability assessment plays a key role in improving the security of any security system by identifying the potential vulnerabilities and proposing countermeasures to mitigate the threats posed by them. In this work self-generated and dynamic helper data based system is proposed to encrypt the biometric templates. Biometric information is statistically learned and probabilistic matching is performed to discriminate genuine from imposters. We call this system as One Time Biometric Transformation (OTBT) system. The system was tested using CASIA iris database and by probabilistic matching an EER of 1.96% is achieved. Strength analysis of the system for three different challenging databases is also presented.**

I. Introduction

As technology and services have developed in the modern world, for human transactions, faster, reliable and more secured personal identification is required. Secure applications requiring biometric authentication over distributed open networks are desired to be able to withstand attacks at two different levels, communication level attacks and database level attacks. The security framework design of biometric systems should be able to address system level vulnerability issues and serves as the motivation for this work [1], [2].

As any other authentication system, biometric authentication system functions in two phases, enrolment phase and authentication phase. Typical vulnerabilities associated with the traditional biometric system is shown in figure (1). During the enrolment phase, biometric characteristics of an individual is acquired using a biometric sensor or a biometric scanner. Features are extracted from these biometric traits and are saved in the form of a template. During authentication, similar procedure is repeated and again a template is generated to match with the templates in the database.

In this framework attacks are possible at two levels, namely communication level and database level. Also, the nature of these attacks is twofold. First stolen information can be used for authentication resulting in a security breach. 'Security' threat here is referred to as threat to the application (online banking) and not the user. Second, the original biometric may be regenerated from the stolen information resulting in a privacy threat.

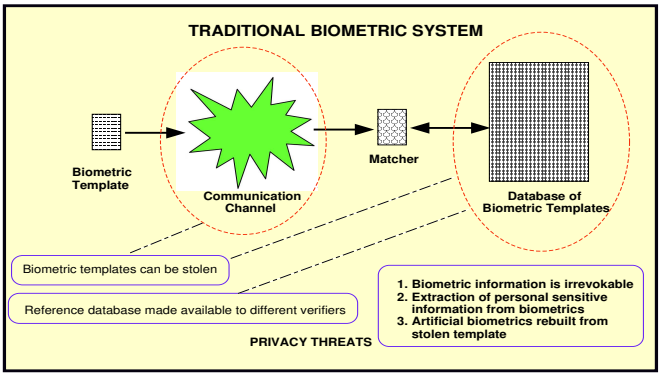


Fig. 1. Traditional biometric system. Biometric samples are collected and converted into biometric templates. These templates can be sent over communication channel. At the receiving end the template is matched with the other templates stored in the database of authentic users. Various attack points are clearly shown in the figure.

The shift from password based authentication systems to the biometric authentication systems now includes privacy threats due to the personal and 'irrevocable' nature of the biometrics. Classifying the vulnerability as 'privacy-related' or 'security' gives an a method of separating the two threats and thus better assess the vulnerabilities.

A. Comparison of existing systems

Template protection systems, as discussed earlier, improve biometric security either by a non-linear (non-invertible) transform or by deriving/binding a cryptographic secret from/to the biometric features. Template communication protection systems achieve the goal of securing the communication channel by generating dynamic information to be sent on the communication channel from encoder(feature extractor) to the decoder(matcher). This dynamic information could be generated by changing the keys for encryption, by including time stamps or by changing the challenge for every authentication session. The following table summarizes the techniques in terms of the protection they provide against these threats at the two levels.

As seen from the table, existing techniques either protect the template (as in cancelable biometric, biometric cryptosystems) or provide protection against replay attacks (as in key-based encryption, challenge response mechanisms) [3].

Manuscript received June 22, 2009, revised July 05, 2009.

The work was supported by NSF IUCRC Center For Identification Technology Research (CITeR), WV, USA. This work was also partially funded by University of Pune BCUD research grant Eng−111.

A. Abhyankar is with the Vishvakarma Institute of Information Technology, Pune, India. He is also associated with Clarkson University, NY, USA, and Government College of Engineering, Pune, India.

A. Vijayat is with a software company in Hyderabad, India as a Software Engineer.

S. Kumar is with the Electrical and Computer Engineering department at San Diego State University, San Diego, CA.

S. Schuckers is with the Clarkson University, NY, USA. She is also associated with West Virginia University, WV, USA.

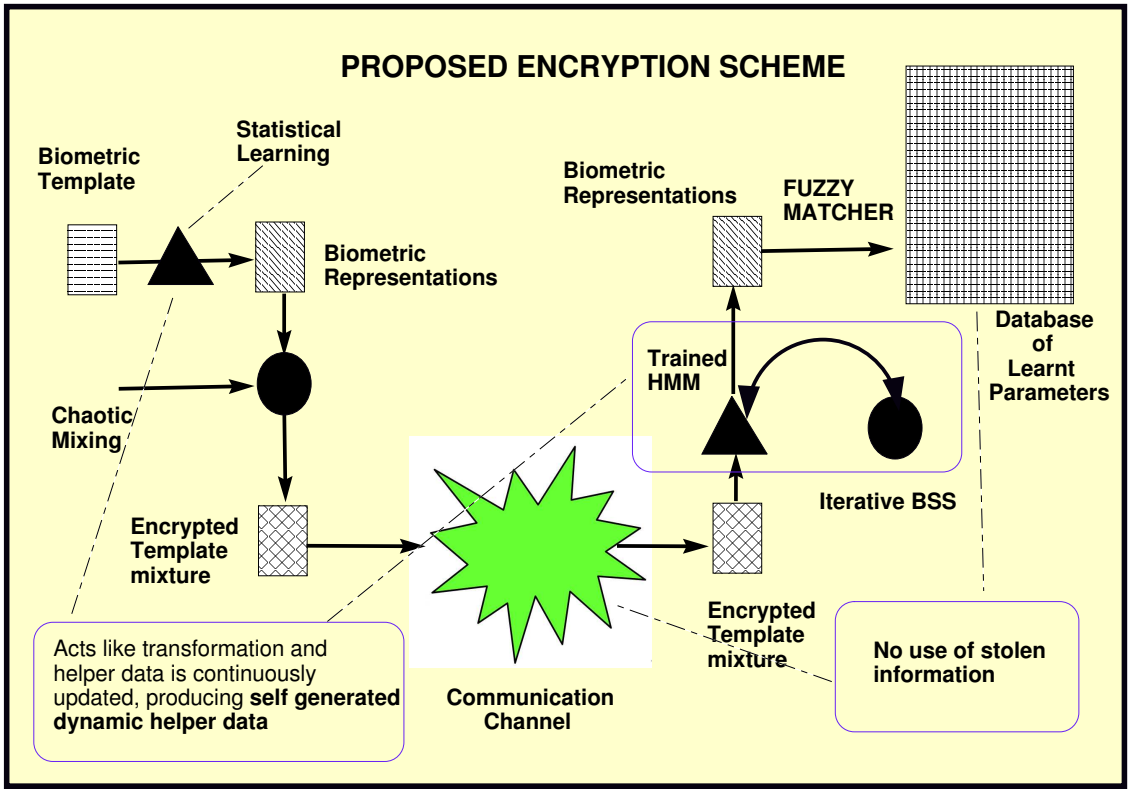


Fig. 2. Proposed system with the encoder which combines stored learned statistical representations and chaotic mixing and with the decoder which combines blind source separation with hidden Markov model.

TABLE I

COMPARATIVE ANALYSIS OF PROPOSED SCHEME WITH EXISTING SCHEMES.

	Original Biometric Protected		Authentication Protected		
	Storage level	Communication level	Storage level	Communication level	Remarks
Traditional Biometrics	NO	NO	NO	NO	-
Cancelable Biometrics	YES	YES	NO	NO	needs robust transform
Biometric Cryptosystems	YES	YES	NO	NO	key generation not robust
Key based Encryption	NO	YES	NO	NO	Administrative hassles
Modified Challenge-Response	NO	NO	YES	YES	needs smart sensor circuit
One-time Biometrics	YES	YES	YES	YES	proposed

Proposed One-time biometrics is the only attempt, to the best of our information, that proposes to combine both the techniques by finding a suitable one-time transform generator [1].

In this work, we attempt to address these four aspects of vulnerabilities in a unique biometric system. The advantage of this system is that the information stored (if stolen) can not be used for authentication (security threat) or to regenerate the original biometric (privacy threat). The dynamic and self-generating system is based on a combination of blind source separation and hidden Markov model for decoding. Iris recognition is used to demonstrate this approach in this paper.

II. DYNAMIC REPRESENTATION BASED BIOMETRIC AUTHENTICATION SYSTEM

The schematic of the designed system is shown in figure (2). The communication channel divides the system into two parts. The one on the left side of the communication channel is called as the encoder, while the right side of the communication channel depicts the decoder.

The system design does not address following

- tampering of biometric information is allowed at the sensor level
- or at the enrolment or verification stage

This research is not focused on studying physics of the devices and protecting raw biometric data, rather we focus on the security of the biometric templates, which are the features extracted from the biometric information.

- The designed system requires two databases, one at the encoder (template generation) end and other at the decoder (matcher) end. The encoder database contains the statistical learned templates known as 'representations'. The decoder database contains the α, β parameters or the forward and backward probabilities of a trained hidden Markov model.
- Dynamic representation based biometric authentication system is a method where 'self-generated dynamic helper data' derived from the biometric itself is used to transform both at the encoder and the decoder end.
- A hidden Markov model is used to match the reconstructed representations at the decoder end. HMM in this case uses multiresolution probability distributions to model the state output probabilities at different resolutions.
- Consistent features are required to be extracted for the generation of 'dynamic helper data'. In this design, iris modality was used to generate the features [4]. The region of the biometric image to generate these features is selected based on the following factors as shown in the figure (3).
  - Region in the central part of the iris
  - Region with minimum occlusion
  - Region not affected by the pupil dilations
  - Region with minimum noisy elements
  - Region that can be precisely selected every time
  - Region with complex epigenetic structure and random characteristics

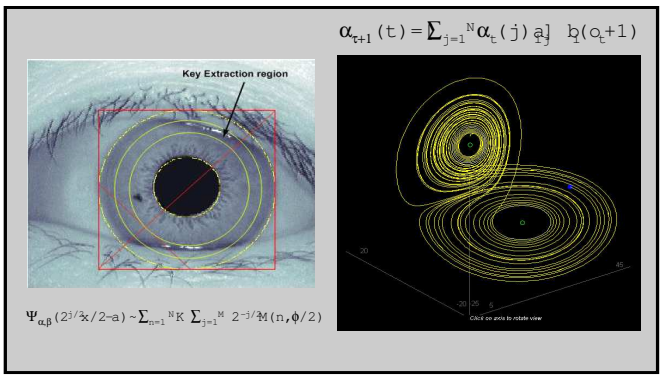


Fig. 3. Generation of dynamic helper data. From the central iris region maximally consistent keys are generated. The free fall plot of the key information guarantees the stochastic nature of the keys.

A. Encoder enrolment

During the enrollment phase at the encoder, a set of training images from the user are acquired to perform statistical template learning [5]. Prior to the statistical template learning stage, they are encoded using a biorthogonal wavelet encoder. Biorthogonal wavelet encoding of iris is used to generate templates for iris recognition in [6]. A lifting technique is used to construct the biorthogonal filters allowing faster implementation of wavelet transform. Only difference between the implementation presented in [6] and the implementation used in this study is the quantization of the wavelet coefficients is intentionally avoided. Statistical template learning of these coefficients is performed at different number of orientations (greater than 1) resulting in a set of representations $R_i, i = \{1, 2, , n\}$ where n is the number of representations. Each set refers to a different orientation at which learning takes place. These are stored in the encoder database for future use.

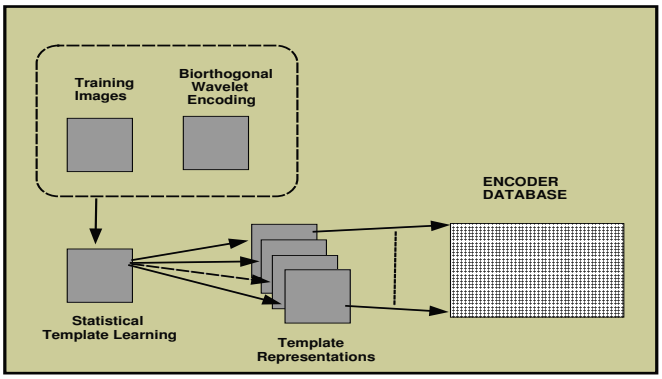


Fig. 4. Encoder Enrolment. Training images are generated through biorthogonal wavelet scheme. Through statistically learnt patterns biometric representations are prepared. These formulate the encoder database.

The learning methodology closely follows the structure given in [5]. As in [5] the joint distribution of wavelet coefficients of pattern template is a function of state variables.

$$q = \{a_i, m_i, s\}, \quad s = (s_1, ..., s_N)^T$$

The main modification we have over [5] is, state variables are projected on orthogonal planes. This is to accommodate the fact that the inter coefficient distribution is not always independent (e.g. scaling issues), which also justifies the use of HMM at the decoder end. Thus, the likelihood of the observation depends on these orthogonal spaces.

B. Decoder enrolment

During the enrollment phase at the decoder, a set of training images taken from the user are encoded using the biorthogonal wavelet encoder. Once again, the quantization is purposely avoided to decrease the loss of information. But, to reduce the training time the wavelet coefficients are streamlined. Encoded images here act like the observation sequences used to train a hidden Markov model using a supervised technique. HMM training is not required to be supervised, if HMMs are used for general categorization of the information. As against that, for this application the classes are subtle and very discrete. Naturally, while training the HMM we need to minimize the class definition function. Parameter λ' is extracted from the

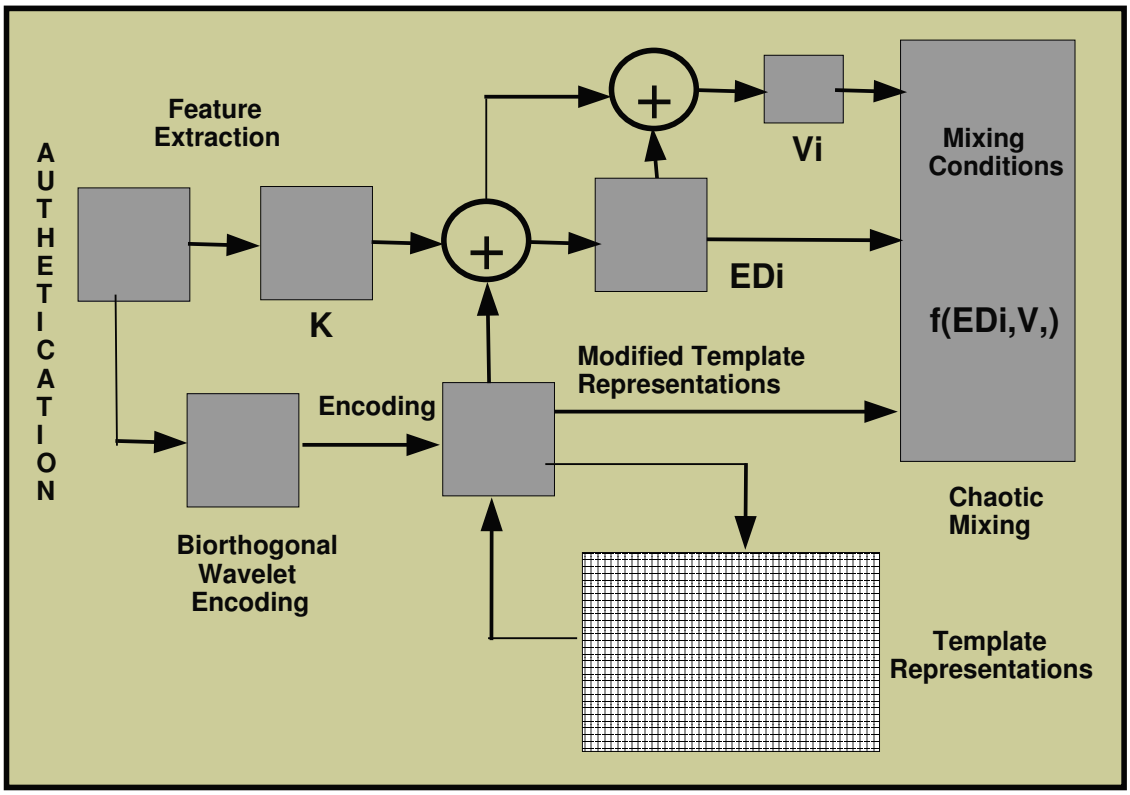


Fig. 5. Encoder Authentication. Chaotically mixed and dynamically linked stream of information is generated, which can be sent over public communication channel.

basis wavelet function used to encode images and provided along with the observation sequences to train the HMM model. The result of the training is the forward and backward probabilities of the HMM, known as α and β parameters which are stored in the decoder database. The representations are not stored in the decoder database.

C. Encoder authentication

Every time the user accesses the system, his biometric information is acquired. This acquired biometric is used to generate the encoder helper data K. The biorthogonal encoded image and the stored representations R_i are used to generate modified representations R_i'. The encoder database is updated with these modified representations R_i', every time the user accesses the system. This makes the system dynamic since its stored representations continually change. As we will see, the stored parameters in the decoder database will change in tandem.

The next steps form the procedure for generating the chaotic data. All the modified representations are used to generate ED_i by performing orthogonal convolution with the generated features K. Now, corresponding to each of the representations, decoder helper data V_i is generated by orthogonal convolution of ED_i and the generated features K. A mixing condition is derived from the modified representations and given as input to the chaotic mixer. Other inputs to the chaotic mixer are ED_i and V_i. Output of this chaotic mixer is a random bitstream

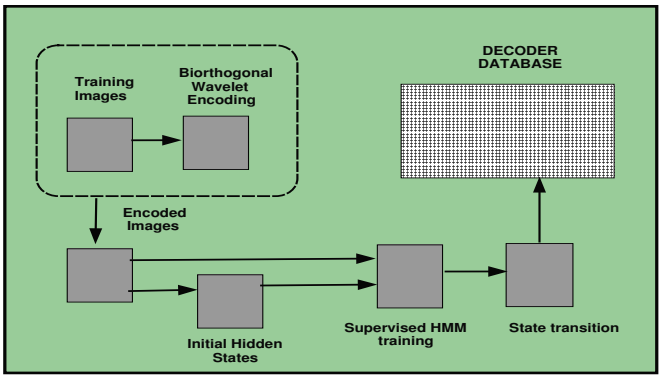


Fig. 6. Decoder Enrolment. This is achieved through supervised Hidden Markov Model (HMM) training. Generated state transition matrices formulate the decoder database.

with embedded V_i and mixed representations. Locations of the embedded decoder helper data V_i in the chaotic mixture is known prior at the decoder end. V_i is required at the decoder end to separate and match the chaotically mixed representations.

D. Decoder authentication

The chaotic mixture is received by the decoder. This decoder consists of two components working in tandem for a fixed number of iterations. The first component is the blind source

separator (BSS) and the second component is the trained hidden Markov model (HMM). BSS tries to separate out the representations from the mixture and gives the estimated representations R_i'' to the HMM. HMM with the help of the decoder helper data V_i and the stored α and β parameters perform the probabilistic match on the estimated representations R_i''. If the match score is above a certain threshold, the user is authenticated. If it is below the threshold, they are fed back to the BSS. In this whole process of separating and matching the representations, the α and β parameters are modified and updated in the decoder database.

The state distribution probability is obtained by looking at the output sequences simultaneously at different resolutions. Since we used the wavelet framework, the obtained output sequence is scalable, and hence helps in studying the simultaneous responses for varying scales. If ξ_1 represents the $2D$ space spanning the first iris class and ξ_n represents the $2D$ space spanning the n^{th} iris class. We modify the output probability sequence from [7] as,

$$P(O/\lambda) = \sum_{all\ q,l} \prod_{t=1}^{T} a_{q_{t-1}q_t} \omega_{q_t l_t} \Omega_{q_t l_t}(V(O_t)) \qquad (1)$$

where, Ωs are the probability distribution functions associated with the respective spaces. Maximization function is applied and posterior probabilities are calculated, as all the spaces are defined and known. These steps are borrowed from [7] and we get the modified a_{ij} from [7] as,

$$a_{ij} = \frac{\sum_{t=1}^{T} \xi_t'(i,j)}{\sum_{t=1}^{T-1} \sum_{g \in S(O(t))} V_t(i,g)} \qquad (2)$$

where meaning of all the terms is as given in [7].

The decision is taken using the fuzzy classifier. The genuine user will have the embedded presentation across all the spaces, as against that the imposter (may be a time stamp variant or channel blocker), will have the presentation only across that particular space in terms of time(attempts) or frequency. So the fuzzy rule which assigns the participation value to all the candidates is as follows:

$$S(O_t) = \begin{cases} \{1, 2, ...G-1\}, & \text{genuine} \\ \{G\}, & \text{imposter} \end{cases} \qquad (3)$$

III. Results

A. Basic Testing

To test our prototype system, we used the CASIA iris database [8]. The biorthogonal encoding as presented in [6] is used to represent iris information. The keys are generated from the most consistent iris regions as discussed. CASIA database consists of 756 images, 108 classes and thus has 8 images coming from each class [8]. Out of 8 images 6 are used for training and remaining 2 are used for testing. The proposed probabilistic system is used for matching. In addition, for comparison, matching is performed using the conventional template matching system for the stored representations. The inter and intra class distributions are shown in figure (8). The traditional template matching fails for the designed system and a high EER of 66.3% is obtained. Using probabilistic matching EER of 1.96% is obtained.

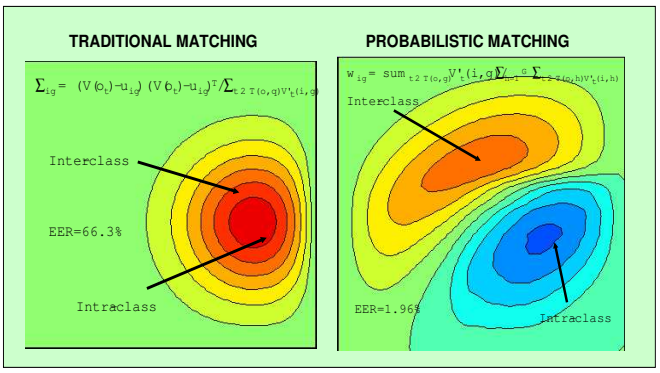


Fig. 8. Inter class and Intra class centroids and information distribution. Traditional matching gives an Equal Error Rate (EER) of 66.3%. The proposed probabilistic matching produces better EER of 1.9%.

B. Strength Analysis

The basic testing provided the base results indicating the proof of concept, however to strengthen our analysis, an extensive experimentation was performed on vivid database.

The first data set (db1 from hereon) is a data set of gray scale iris digital images provided by the Chinese Academy of Sciences (CASIA). The database consists of 756 gray scale images coming out of 108 distinct classes and 7 images of each eye. The data was collected from 80 subjects in two sessions with a one month gap between the two sessions [8].

The second data set (dataset2 from hereon) contains iris images collected at University of Bath, UK. The data set consists of 1000 high-quality eye images taken from 50 eyes (left and right) of 25 subjects. The images are compressed by the JPEG2000 codec at 0.5 bpp and have a resolution of 1280×960.

The third data set (db3 from hereon) consists of iris images collected at Clarkson University, USA. This data was collected from 80 subjects in one session with 4 images each of left and right eye for each subject. Thus, a total of 640 images from 160 classes are used for analysis. This data set is an uncontrolled data set and is collected using Oki Irispass-h hand held device (model EQ5009A). No extra care is taken to control the quality and illumination of the iris information.

The data sets together form diverse iris representations in terms of sex and ethnicity and conditions under which iris information was captured. The CASIA data set is one of the oldest and widely used and predominantly has iris data from Asians, while the data collected at the WVU has angular deformations and mostly contains iris images of Caucasians. For the data collected at Clarkson University and West Virginia University, protocols for data collection from the subjects were followed that were approved by the West Virginia University and Clarkson University Institutional Review Boards (IRB). Db3 has challenging iris images because of the uncontrolled and non-ideal conditions during iris capture respectively. The profiles of the databases used are represented in Table II.

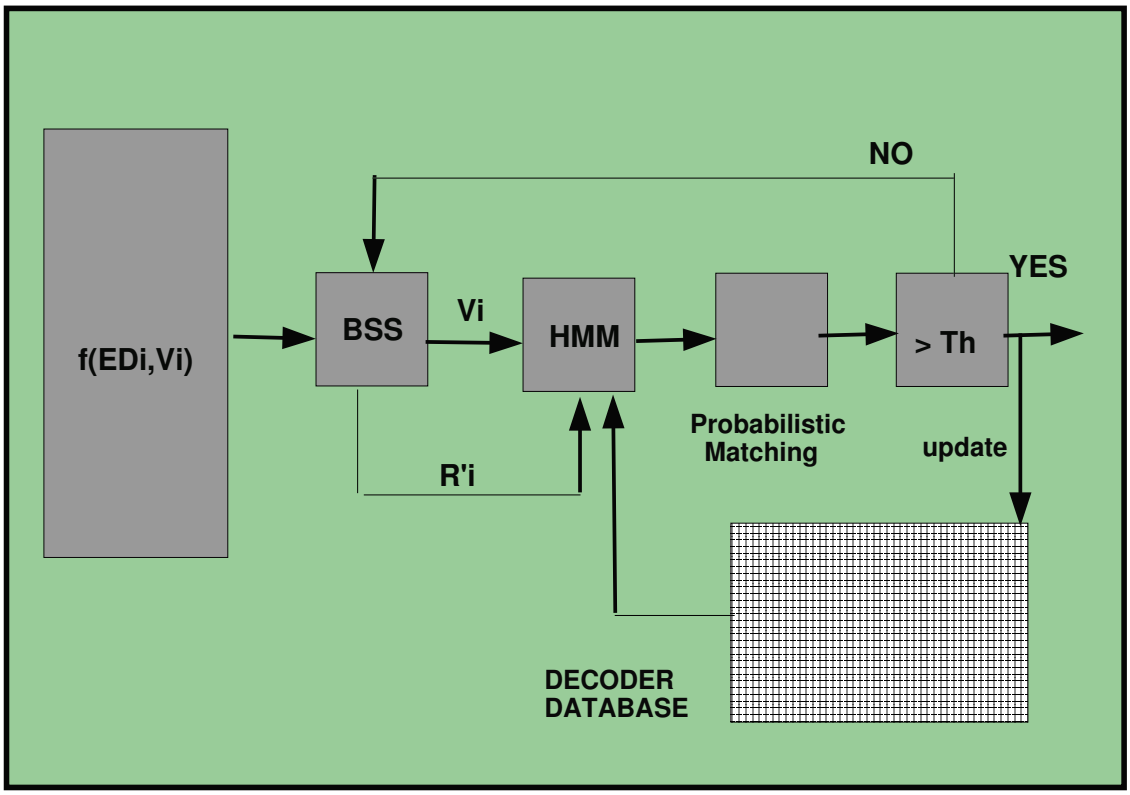


Fig. 7. Decoder Authentication. Blind Source Separator (BSS) and Hidden Markov Model (HMM) work in tandem to separate the mixed entities, which are then matched in a fuzzy way to make a decision.

TABLE II
DATA SET: PROFILES

Data set	No. of images	No. of classes	Images per Class	Intra class	Inter class
db1	756	108	7	2268	566,244
db2	1000	50	20	9500	980,000
db3	640	160	4	960	407,040

The results are shown in figure (9). The conventional matcher produces an Equal Error Rate (EER) of 23.41% for db1. This EER gets improvised to 1.44% using the proposed method for db1. Conventional matcher produces EERs of 24.93% and 33.16% for db2 and db3 respectively. Using the proposed OTBT scheme these EERs are improved to 1.63% and 3.84% for db2 and db3 respectively. This demonstrates an ability of the OTBT system to generate consistent keys and transcode the information in noisy conditions.

IV. CONCLUSION

The paper presents a new method for securing a biometric authentication system using stored statistical representations of the biometric, chaotic mixing at the encoder, and combination of blind source separation, hidden Markov model, and fuzzy classifier for decoding. In terms of securing the online application (e-banking) at authentication system and communication levels, the designed system is a step ahead of other existing systems through the use of self-generated helper data to generate and match the dynamic representations.

The advantages of the secure biometric authentication based on dynamic representations can thus be summarized as:

- Stored information in the database cannot be used to authenticate or obtain original biometric signal
- Transmitted information from encoder to decoder cannot be used to authenticate or obtain original biometric signal
- Matcher does not give information helpful in hill climbing attack
- Generated representations are 'dynamic'

More research is needed to model communication and database level attacks (replay, noise, etc) to further demonstrate the ability of this system to withstand common biometric vulnerabilities.

ACKNOWLEDGMENT

The work was funded by NSF IUCRC Center For Identification Technology Research (CITeR), USA. This work was also partially funded by University of Pune BCUD research grant Eng-111.

REFERENCES

[1] N. Ratha, "Enhancing security and privacy in biometrics-based authentication systems," *IBM systems journal*, vol. 40, pp. 614–6134, 2001.
[2] D. Osten, H. Carim, M. Arneson, and B. Blan, "Biometrics, personal authentication system," *US Patent #5,719,950*, Feb 1998.

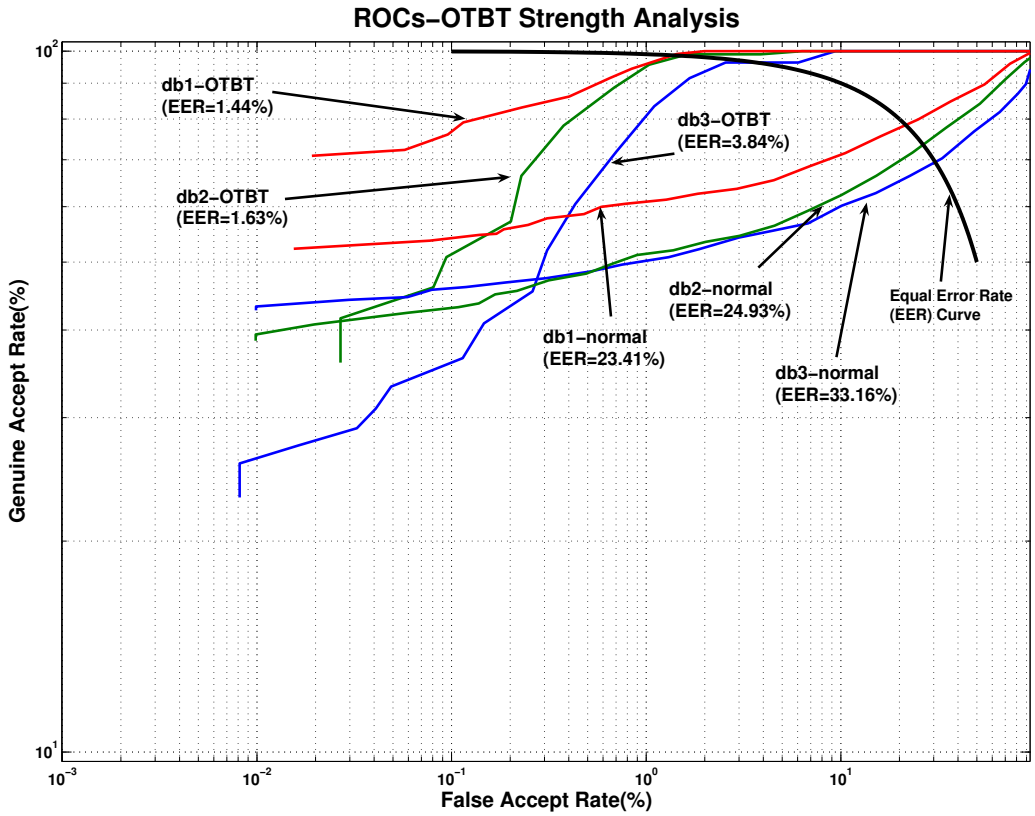


Fig. 9. Receiver Operating Characteristics (ROC) curves. ROCs for db1, db2 and db3 for conventional and proposed method are presented. A distinct improvement in terms of EER is seen for all the databases.

[3] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, 2004.

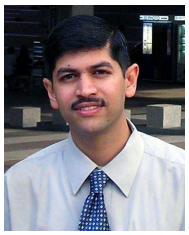
[4] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence." *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, 1993.

[5] C. Scott and R. Nowak, "Templar: A wavelet-based framework for pattern learning and analysis," *IEEE Transactions on Signal Processing*, vol. 52, no. 8, pp. 2264–2274, 2004.

[6] A. Abhyankar, L. Hornak, and S. Schuckers, "Bi-orthogonal wavelet based iris recognition," *SPIE, Defence and Security Symposium*, p. 5406, 2005.

[7] S. Furui, "Speaker independent isolated word recognition using dynamic features of speech spectrum," *IEEE Transactions on Acoust.,Speech and Signal Process*, vol. 34, no. 1, pp. 52–59, 1986.

[8] C. A. of Sciences Institute of Automation, "Database of 756 greyscale eye images," *http://www.sinobiometrics.com*, 2003.



Aditya Abhyankar received the BE degree in Electronics and Telecommunication Engineering from Pune University, India in 2001. He received the MS and Ph.D. degrees from Clarkson University, NY, USA in 2003 and 2006 respectively. He worked as a post-doctoral fellow at Clarkson University, NY, USA in the academic year 2006-07. He worked as a consultant for Biometrics LLC, WV, USA in 2007. Currently he works as a Research Associate at Clarkson University and Professor at Computer Engineering Department of Vishvakarma Institute of Information Technology (VIIT), Pune. He works as Dean of R&D and Director of CERD (Center for Excellence in Research and Development) at VIIT, Pune. He is an approved Ph.D. guide of University of Pune and is also associated as Adjunct Professor with Government College of Engineering, Pune (COEP). He is involved in consultancy with number of private industries. His research interests include signal and image processing, pattern recognition, wavelet analysis, biometric systems and bioinformatics.

Amit Vijayat received the Bachelor of Technolgy (BTech) in Electronics and Communications Engineering from Jawaharlal Nehru Institute of Technology, India in 2004. He received Master of Science in Electrical Engineering from Clarkson University in 2006. He is now working with a software company in Hyderabad, India as a Software Engineer. His research interests include Image Processing, Biometrics and Content Management Systems.

Sunil Kumar received B.E. (Electronics Engineering) degree from S.V. National Institute of Technology, Surat (India), in 1988 and the M.E. and Ph.D. (Electrical and Electronics Engineering) degrees from the Birla Institute of Technology and Science (BITS), Pilani (India) in 1993 and 1997, respectively. From 1997 to 2002, Dr. Kumar was a Postdoctoral Researcher and Adjunct Faculty in the Integrated Media Systems Center and Electrical Engineering Department at the University of Southern California, Los Angeles. From 2000 to 2002, he was also a Consultant in industry on JPEG2000 and MPEG-4 over Wireless related projects and participated in JPEG2000 standardization activities. From 2002 to 2006, Dr. Kumar was an Assistant Professor in the Electrical and Computer Engineering department at Clarkson University, Potsdam, NY.

Since August 2006, Dr. Kumar has been an Associate Professor and Thomas G. Pine Faculty Fellow in the Electrical and Computer Engineering department at San Diego State University, San Diego, CA. He was an ASEE Summer Faculty Fellow at the Air Force Research Lab in Rome, NY during summer of 2007, where he conducted research in Airborne Wireless Networks. Dr. Kumar is a senior member of IEEE and has published more than 80 research articles in international journals and conferences, including two books/book chapters. His research has been funded by National Science Foundation, Department of Defense, Department of Energy, NY State Energy Research and Development Agency (NYSERDA), Information Institute, Cisco, Sprint Advanced Technology Labs and Center for Identification Technology Research (CITeR).

Dr. Kumar's research interests include (i) QoS-aware cross-layer MAC, Routing and Transport Protocols for Multimedia Traffic in Wireless WiMAX, Cellular, Ad hoc, Sensor and Cognitive Radio Networks, (ii) Error Resilient Multimedia (Image, Video and 3D graphics) Compression techniques, including MPEG-4, H.264-AVC and JPEG2000, (iii) Image Processing techniques with applications in biomedical and fingerprint images, and (iv) Machine Learning techniques for bioactivity prediction and data mining of drug molecules (Chem-Bioinformatics).

Stephanie Schuckers received the M.S. and Ph.D. degrees in electrical engineering from the University of Michigan, Ann Arbor, in 1994 and 1997 respectively, where she was a Whitaker Foundation Graduate Fellow.

Currently, she is an Associate Professor with the Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY. Her primary research interest is the application of modern digital signal processing and pattern recognition to biomedical signals. Signals include the electrocardiogram, biometric signals like fingerprints, pulse oximetry, respiration, and electrocephalograms. Her work is funded by various sources, including National Science Foundation, American Heart Association, National Institute of Health, and private industry.