RESEARCH ARTICLE OPEN ACCESS

A Frame Work for Single Sketch Based Multibiometric Cryptosystems

Shrujan. J, KumaraSwamy.P, Dr. C. V. Guru Rao

M.Tech in CSE Dept ,SR Engineering CollegeWarangal, ANDHRA PRADESH, INDIA
Assistant Professor in CSE Dept,SR Engineering CollegeWarangal, ANDHRA PRADESH, INDIA
Professor,CSE Dept S.R.Engg college,Warangal, A.P.,India

Abstract
Biometric features are incorporated in many real world systems for unique identification of humans across the world. The features include face, fingerprints, voice, iris and so on. The reason for adapting this is that biometric features provide globally unique identification to people and the techniques are robust. Efficiency and low error rates are another reason for the popularity of biometric systems. There are issues to be resolved in such systems. For instance for every individual such systems are to store many details like fingerprints, iris, face etc. which causes risk to privacy of individuals. One existing solution to overcome this problem is storing sketches generated from biometric features of humans. However, this solution needs huge amount of storage. Recently Nagar et al. proposed a framework based on feature level fusion using biometric cryptosystems which are well known. The cryptosystems used are fuzzy commitment and fuzzy vault. In this paper we implement that framework which makes use of face, iris and fingerprint of humans for unique identification. We built a prototype application that demonstrates the proof of concept. The empirical results reveal that the proposed approach is effective.

Index Terms– Biometric features, biometric systems, multibiometrics, fuzzy vault, fuzzy commitment.

I. INTRODUCTION

Biometric systems are very popular for their security in identifying humans uniquely across the globe. They make use of biometric features of human beings such as face, iris, voice, and fingerprint and so on [1]. Instead using single biometric feature, it is very useful if multiple biometrics are used together in a system. Globally unique identification is very essential in the modern countries to protect systems from fraudulent activities. Every country in the world needs such system. Cryptography along with biometrics is very good combination for protecting systems. Many real world applications are using multiple biometrics. For instance UID department in India, IAFIS used by FBI are some of the examples of it. Biometric authentication is incorporated into both hardware and software systems [2], [3]. Undoubtedly biometric systems improved the reliability of security mechanism in organizations. However, the biometric templates stores huge amount of personal data which causes privacy problems to sensitive data. However the leakage of biometric template can cause severe security risks. They may be susbjected to various attacks such as intrusion attack besides subjecting to another problem known as function creep. Function creep is nothing but unquthorized access and misuse of biometric templates. Biometric template systems also need huge storage which is another problem being faced.

Biometric Cryptosystems

In case of a biometric cryptosystem which uses combination of cryptography and biometrics of humans, a secure sketch is derived from the biometric templates. The secure sketches are stored in databases permanently. These secure sketches make it very hard to break such security systems. When queries are made which are similar to biometric templates, it should work properly. There are many biometric cryptosystems available in the work. They include secret sharing approaches [4], PinSketch [5], fuzzy commitment [6] and fuzzy vault [7]. There are template transformation techniques available that can modify the templates to get into another format. As these transformation systems make use of user specified key, they provide another layer of security. During authentication this key needs to be used. As the key is also saved with template, it is very secure. There are some well known transformations that include cancelable biometrics [8] and bio-hashing [9]. Secure template should have two important qualities. They are known as Non-invertibility and Revocability. The former does mean computational difficulty while the latter does mean computationally hard to identify the original biometric data. Template transformation schemes provide better revocability. Hybrid cryptosystems make use of both approaches to make it more robust as explored in [10] and [11].

In this paper we focus on the biometric system that makes use of multi-biometric template. This is done using two systems such as fuzzy vault and fuzzy commitment. Biometric cryptosystems are used for specifi features of biometrics. The fuzzy commitment is responsible to find the dissimilarity between query and template. The techniques such as PinSketch and fuzzy vault make use of representations such as point-set and dissimilarity metric. However, multiple templates may not show the same features.. The features which are based on point-set are used to represent salient features of identity. For instance fingerprint minutiae can be used. In the process feature vector is built using tools such as Linear Discrimant Analysis (LDA) [12], and PCA [13]. Quantization is used to obtain binary strings in for real feature vector that reduced storage space to be used by the system. This will significantly reduce the space required thus improving performance. For instance iris code [14] is used to do so. Biometric represeantations have diversity as they need fusion of decisions, template protection schems and so on [15]. This is similar to the system that needs multiple low streanth bits that make bit strength passwords. However, such system is less secure which uses a single password with number of bits. The proposed system is motivated by this system.

The main contribution of this paper is to build a prototype application that makes use of multibiometric cryptosystems using fuzzy vault and fuzzy communication concept. The fusuion of biometric features like iris, face, fingerprint is very important in this paper. The rest of the paper is structured into the following sections. Section II provides details of the proposed system. Sectgion III provides experimental results while section IV concludes the paper.

II. PROPOSED SYSTEM

In this paper we focused on building a multibiometric cryptosystem based on the concepts provided in [16]. The application is meant for improving the templates concept that existed earlier. The template concept has security problems and also take lot of space in the storage. To avoid this problem fusion of features is concept in this paper. The main architecture of the proposed framework is as presented in figure 1.

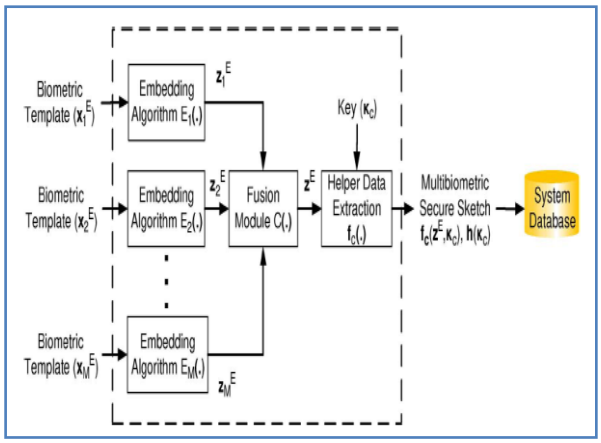

Fig. 1 – Schematic overview of the propsedmultibiometic cryptosystem

As can be seen in figure 1, it is evident that the framework takes multiple biometric templates as input and performs corresponding embedding algokitujms in order to generate a single biometric secure sketch and finally it is saved to database. There are modules like fusion module and also helper data extraction module. The embedded algorithm transforms biometric representation into another feature representation which can be subjected to fuzzy commitment and fuzzy vault later. The fusion module is responsible to combine multiple homogenous biometric features and generates multi-biometric feature representation. All the modules play an important role and they work together. Finally the framework produces the single secure biometric sketch that can represent and uniquely identity humans across the globe. Storing such sketches in database and comparing them when people are to be authenticated is the application to identify people uniquely across the globe. We have taken the fuzzy vault decoding algorithm from [17]. The algorithm is as given below.

Input: $\mathbf{y}_c^o = [(\alpha(1), \beta(1), \gamma(1)), \cdots, (\alpha(t), \beta(t), \gamma(t))]$
(Ordered vault points); k (Degree of polynomial)
forall[5] $n = (k+1)$ to t **do**
  $\mathbf{s}_n \leftarrow \{(\alpha(i), \beta(i), \gamma(i))\}_{i=1}^{n}$
  for $m = 0$ to $n - (k+1)$ **do**
    forall $\mathbf{s}_* \subset \mathbf{s}_n, |\mathbf{s}_*| = m$ **do**
      $\mathbf{s}_n^- \leftarrow \mathbf{s}_n \setminus \mathbf{s}_*$
      $P \leftarrow \text{DecodeBM}(\mathbf{s}_n^-, k)$
      if P is the required polynomial **then**
        Return P
      end if
    end forall
  end for
end forall
Return ϕ
{DecodeBM$(\mathbf{s}, k)$ performs a Berlekamp–Massey decoding of the set of points $\mathbf{s}$ for a polynomial of degree k}

Fig. 2 –Fuzzy vault decoding algorithm

As can be seen in figure 2, it is evident that the algorithm takes ordered vault points and degree of polynomial as inputs. The algoirhtm works in the concept that from many points taken if at least one point allows the recovery of polynomial and finally

decoding the multibiometrics. Another algorithm we used for decoding is fuzzy commitment. The algorithm is presented as showin figure. 3.

Input: $\mathbf{c}^*$ (corrupted codeword); $\mathbf{p} = [p_1, \cdots, p_N]$ (bit reliability vector where p_i indicates the reliability (1-crossover probability) of $\mathbf{c}^*(i)$, $i = 1, 2, \cdots, N$); $D_{\min}$.
forall $n = (N - D_{\min} + 1)$ to N **do**
  $\mathbf{s}_n \leftarrow \mathrm{RBS}(\mathbf{p}, n, N)$
  for $m = 0$ to $D_{\min} + 1$ **do**
    forall $\mathbf{s}_* \subset \mathbf{s}_n, |\mathbf{s}_*| = m$ **do**
      $\mathbf{c}' \leftarrow \mathrm{Flip}(\mathbf{c}^*, \mathbf{s}_*)$
      $\kappa_c \leftarrow \mathrm{DecodeFC}(\mathbf{c}', \mathbf{s}_n, L)$
      if κ_c is the required key **then**
        Return κ_c
      end if
    end forall
  end for
end forall

As can be seen in figure 3, it is evident that the algorithm is used to decode the codeword based on the cross over probabilities. Figure 4 shows samples of inputs taken from different databases.

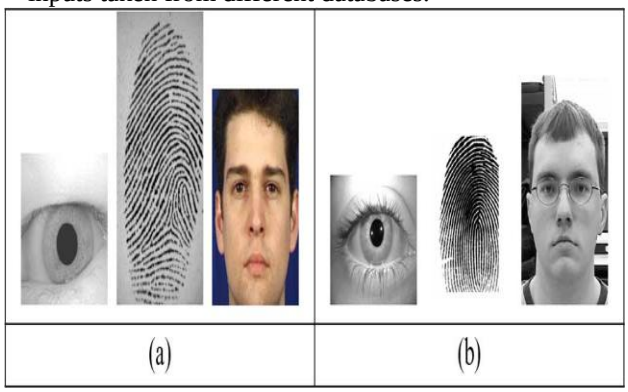

Fig. 4– (a) Iris, fingerprint and face from CASIS database (b) same from WVU database

III. EXPERIMENTAL RESULTS

We used our simulation application in order to make experiments. The experiments are done using the biometric featuers such as face, fingerprint and iris. They are subjected to the fusion concept introduced in this paper. The experimental results with biometric traits difernt databases is shown in table 1.

Traits	Real Multimodal Database		Virtual Multimodal Database	
	Fuzzy vault	Fuzzy commitment	Fuzzy vault	Fuzzy commitment
Iris	0%	37%	88%	91%
Finger	22%	30%	51%	2%
Face	67%	33%	58%	12%
Baseline Fusion	33%	27%	75%	89%
Proposed Fusion	68%	75%	99%	99%

Table 1 – Experimental Results

As can be seen in table 1, it is evident that the table shows various biometric features, methods followed and the experimental results of various techniques. The results revealed that there is less performance with iris when used with WVU multimodal database. There is performance improvement shown in case of unibiometric cryptosystems when native representation scheme is used.

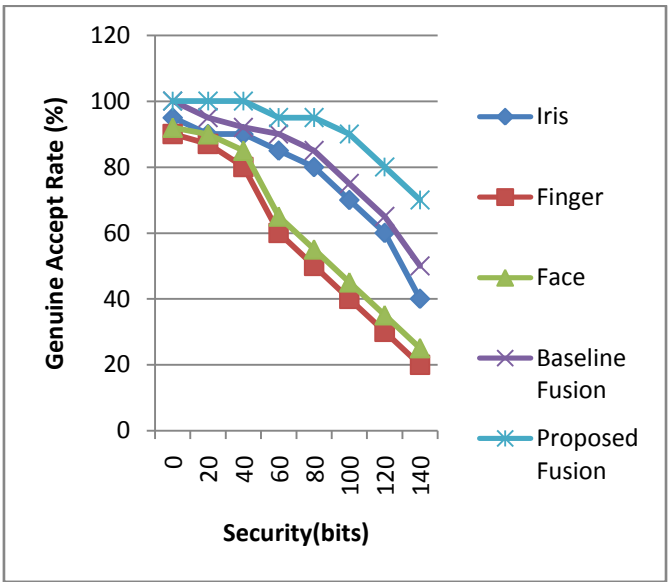

Fig. 5. G-S curves for fuzzy vault for iris, fingerprint, and face images from CASIAVer-1, FVC 2002DB-2, andXM2VTS databases, respectively, the baseline multibiometric cryptosystem based on AND-fusion rule and the proposed multibiometriccrytposystem using all three modalities.

As shown in the above figure horizontal axis represents security while vertical axis represents genuine accept rate

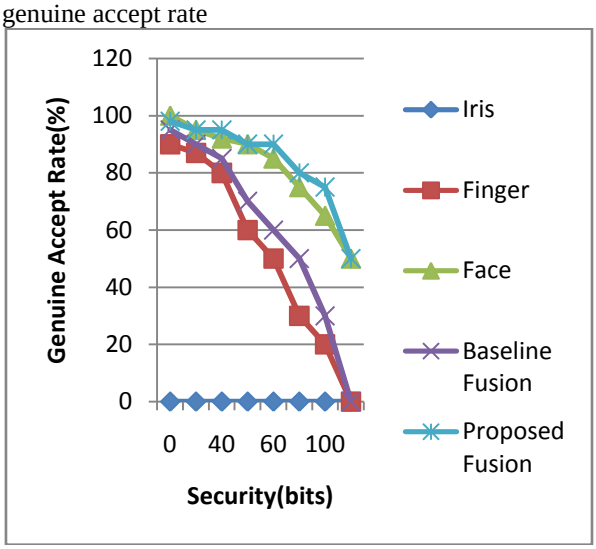

Fig. 6. G-S curves for fuzzy vault for iris, fingerprint, and face images fromWVUMultimodal database, the baseline multibiometric cryptosystem based on AND-fusion rule and the proposed multibiometric crypto system using all three modalities.

As shown in the above figure horizontal axis represents security while vertical axis represents genuine accept rate

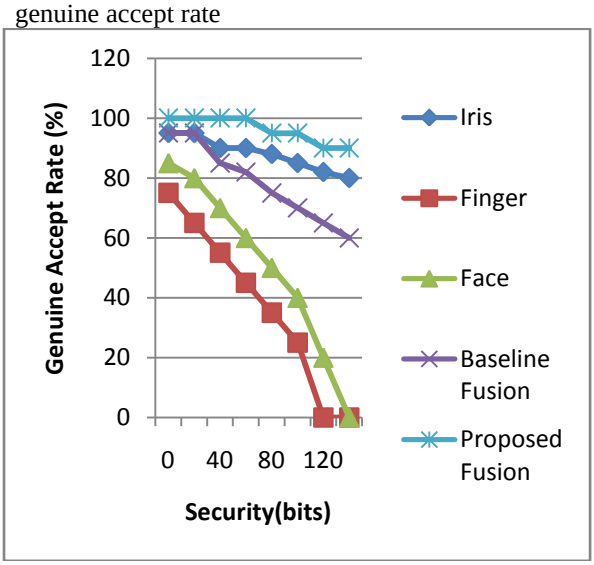

Fig. 7. G-S curves for fuzzy commitment for iris, fingerprint, and face images from CASIA Ver-1, FVC 2002 DB-2, and XM2VTS databases, respectively, the baseline multibiometriccryptosystem based on AND-fusion rule and the proposed multibiometric crypto system using all three modalities.

As shown in the above figure horizontal axis represents security while vertical axis represents genuine accept rate

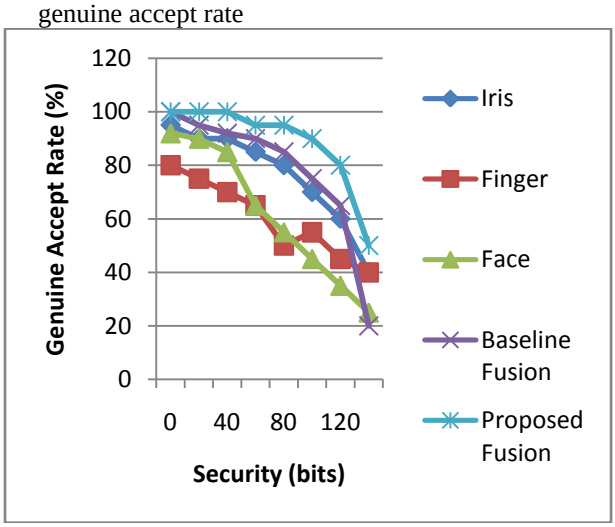

Fig. 8. G-S curves for fuzzy commitment for iris, fingerprint, and face images from WVU Multimodal database, the baseline multibiometric cryptosystem based on AND-fusion rule and the proposed multibiometric crypto system using all three modalities.

As shown in the above figure horizontal axis represents security while vertical axis represents genuine accept rate

IV. CONCLUSIONS AND FUTURE WORK

In this paper we studied the feature level fusion concept of multi-biometrics which was proposed by Nagar et al. [17]. The fusion of biometric features like iris, face and fingerprint is used in our proposed system in order to identify humans uniquely across the world. The salient feature of the system is that it needs only one secure sketch to be maintained for all features. This will save storage problem besides ensuring privacy of humans. We built a prototype application to demonstrate the feasibility of such system that makes use of fuzzy commitment and fuzzy vault cryptographic techniques. The empirical results revealed that the system which is based on fusion of features is very effective and can be used in real world applications. An important future direction to improve this system further is to explore transformation of biometric representation into another format for more flexibility while preserving the content distribution of original representation.

REFERENCES

[1] A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*.New York: Springer, 2006.

[2] 3M Cogent, Fusion—Multi-Modal Biometric Handheld Device [Online].Available: http://www.cogentsystems.com/fusion_d3.asp

[3] MorphoTrak,MetaMatcher—A multi-biometric matching architecture[Online]. Available: http://www.morphotrak.com/MorphoTrak/MorphoTrak/mt_multi-biometrics.html

[5] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int.Symp. Information Theory*, Lausanne, Switzerland, 2002, p. 408.

[6] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc.Sixth ACM Conf. Computer and Communications Security*, Singapore,Nov. 1999, pp. 28–36.

[7] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, FuzzyExtractors: How to Generate Strong Keys From Biometricsand Other Noisy Data Cryptology ePrint Archive, Tech. Rep.235, Feb. 2006, A preliminary version of this work appearedin EUROCRYPT 2004.

[8] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy andsecrecy aspects," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp.956–973, Dec. 2009.

[9] A. B. J. Teoh, K.-A.Toh, and W. K. Yip, " discretisation of BioPhasor in cancellable biometrics," in *Proc. Second Int. Conf. Biometrics*,Seoul, South Korea, Aug. 2007, pp. 435–444.

[10] N. K. Ratha, S. Chikkerur, J. H. Connell, and R.M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern*

Anal. Mach.Intell., vol. 29, no. 4, pp. 561–572, Apr. 2007.

[11] W. Scheirer and T. Boult, "Bio-cryptographic protocols with bipartitebiotokens," in *Proc. Biometric Symp.*, Tampa, FL, 2008.

[12] K. Nandakumar, A. Nagar, and A. K. Jain, "Hardening fingerprintfuzzy vault using password," in *Proc. Second Int. Conf. Biometrics*,Seoul, South Korea, Aug. 2007, pp. 927–937.

[13] M. Turk and A. Pentland, "Eigenfaces for recognition," *J. CognitiveNeuroSci.*, vol. 3, no. 1, pp. 71–86, 1991.

[14] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "EigenfacesversusFisherfaces: Recognition using class specific linear projection,"*IEEE Trans. Pattern Anal.Mach.Intell.*, vol. 9, no. 7, pp. 711–720, Jul.1997.

[15] J. Daugman, "Recognizing persons by their iris patterns," in*Biometrics: Personal Identification in Networked Society*, A. K.Jain, R. Bolle, and S. Pankanti, Eds. London, U.K.: Kluwer,1999, pp. 103–122.

[16] B. Fu, S. X. Yang, J. Li, and D. Hu, "Multibiometric cryptosystem:Model structure and performance analysis," *IEEE Trans. Inf. ForensicsSecurity*, vol. 4, no. 4, pp. 867–882, Dec. 2009.

[42] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[51] Abhishek Nagar, KarthikNandakumarand AnilK. Jain, *"Multibiometric Cryptosystems Based on Feature-Level Fusion".* IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012.

Shrujan.Jreceived the B.Tech Degree in Computer Science & Engineering from Jyothishmathi Institute Of Technology & Science,Karimnagar, A.P, India. Currently doing M.tech in Computer Science & Engineering at SR Engineering College, Warangal, India.

P.KumaraSwamy Assistant Professor in the department Computer Science & Engineering, SR Engineering College, Warangal, India.