IJCSC ISSN: 0973-7391 Volume-4, Number- 2, September, 2013 pp. 268-273 Available online at www.csjournals.com

An Approach to Secure Database Templates in Multimodal Biometric Systems

Dr. Sheetal Chaudhary
Asst. Prof, Department of Comp. Sc. & App. K.U., Kurukshetra, Haryana, INDIA

Abstract: Biometrics provides a reliable and natural solution in establishing the identity of an individual based upon person's unique body features. Multimodal biometric systems consolidate the evidence presented by multiple biometric sources of information. Multimodal biometric systems also require storage of multiple templates for the same user corresponding to the different biometric sources in multiple databases. Every database corresponding to multiple biometric sources requires a separate storage space in memory. So, template security becomes an important issue in multimodal systems. Securing templates in each biometric database separately could be an inefficient approach. Template security is more critical in biometric systems because compromised biometric templates cannot be revoked and reissued. To avoid securing templates in each database separately and misuse of templates, a novel approach is described in this paper by consolidating two biometric sources (face and hand geometry) at feature level to derive a single multi-biometric template and then securing this multi-biometric template using cancelable biometrics by applying some non-invertible transformation function. The resulting multi-biometric template will be more secure as original biometric template will not be stored in the database. If an attacker somehow succeeds in gaining unauthorized access to these multi-biometric templates, it would be completely impossible for him to circumvent the system. Thus the proposed multi-biometric template protection scheme has higher security and better recognition performance as compared to the case when the individual templates are secured separately.

Keywords: Biometric Templates, template security, feature level fusion, cancelable biometrics.

I. INTRODUCTION

Biometrics is an essential tool in meeting the increased security requirements in a variety of applications, so vulnerabilities of the biometric system must be identified and addressed systematically. Ratha et al. [1] identified several different types of attacks that can be launched against a biometric system, and grouped them into eight classes. Figure 1 shows these attacks along with the components of a typical biometric system that can be compromised. Type 1 attack involves presenting a fake biometric (e.g., synthetic fingerprint, face, iris) to the sensor. Type 2 attack (replay) involves submitting a previously intercepted biometric data. In type 3 attack, the feature extraction module is compromised to produce feature values selected by the attacker. In type 4 attack, genuine feature values are replaced with the ones selected by the attacker. Type 5 attack involves modification of matcher to produce an artificially high matching score. Type 6 attack involves attack on the template database (e.g., adding a new template, modifying an existing template, removing templates, etc.). The transmission medium between the template database and matcher is attacked in the type 7 attack, resulting in the alteration of the transmitted templates. Finally, the matcher result (accept or reject) can be overridden by the attacker in type 8 attack.

One of the most potentially damaging attacks on a biometric system is against the biometric template database [2]. Attacks on the template can lead to the following three vulnerabilities: (i) A template can be replaced by an impostor's template to gain unauthorized access, (ii) A physical spoof can be created from the template to gain unauthorized access to the system (as well as other systems which use the same biometric trait) and (iii) The stolen template can be replayed to the matcher to gain unauthorized access.

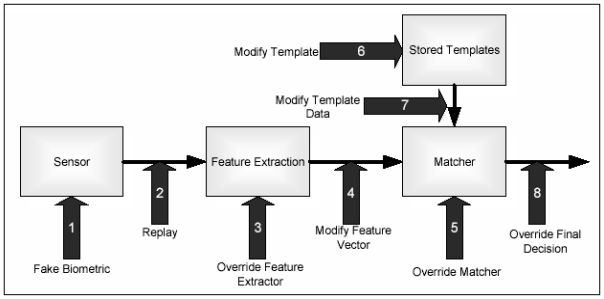

Fig.1.Vulnerabilities in a biometric system

A potential abuse of biometric templates is cross-matching or function creep [3] where the biometric templates are used for purposes other than the intended purpose without the consent of the person. For example, a fingerprint template stolen from a bank's database may be used to search a criminal fingerprint database.

One of the properties that make biometrics so attractive for authentication purposes is their invariance over time. One of the most vulnerabilities of biometrics is that once a biometric image or template is stolen, it is stolen forever and cannot be reissued, updated or destroyed [4]. Every person has only a limited number of biometrics (one face, ten fingers, two eyes etc.) and they are not easy to replace. When a credit card number is compromised, the issuing bank can just assign the customer a new credit card number. In contrast, when the biometric data are compromised, replacement is not possible. An imposter who acquires a person's biometric in one

application might use it in different applications also because sometimes same biometric may be used in many applications. Traditional password based authentication systems have the ability to cancel the compromised password and reissue a new one. In contrast, biometrics cannot be canceled and reissued if they are compromised because they are intrinsic properties of every person to be identified [5].

Multibiometric systems consolidate the evidence presented by multiple biometric sources in order to determine or verify the identity of an individual [6]. These systems can significantly improve the recognition performance of a biometric system besides improving population coverage, deterring spoof attacks, and reducing the failure-to-enroll rate. Information from multiple sources can be consolidated at several distinct levels, including sensor level, feature extraction level, match score level and decision level. While fusions at the match score and decision levels have been extensively studied in the literature, fusion at the feature level is a relatively understudied problem. Fusion at this level involves the integration of feature sets corresponding to multiple biometric information sources. Since the feature set contains richer information about the raw biometric data than the match score or the final decision, so integration at this level is expected to provide better authentication results. However, fusion at this level is difficult to achieve in practice because of the following reasons: (i) the feature sets of multiple traits may be incompatible (e.g., minutiae set of fingerprints and eigen-coefficients of face); (ii) the relationship between the feature spaces of different biometric systems may not be known; (iii) concatenating two feature vectors may result in a feature vector with very large dimensionality leading to the `curse of dimensionality' problem; and (iv) a significantly more complex matcher might be required in order to operate on the concatenated feature set [7].

As biometrics gains popularity, there is an increasing concern about misuse of biometric data held in biometric databases. To tackle this problem, in this paper, a novel approach for multimodal biometric verification systems is presented. It combines the two traits (face, hand geometry) at the feature level, resulting in a single multi-biometric template. Then some non-invertible cancelable transformation is applied on this multi-biometric template which results in a new template that is finally stored in the database. We have used face and hand geometry traits as two of the most practical and commonly accepted biometrics. The gain obtained from the proposed scheme is two-fold: increase in security and cancelability. Also, using multiple biometric traits decreases error rates by providing additional useful information to the matcher. The rest of the paper is organized as follows. Section 2 addresses the literature study. In section 3 fusion of face and hand geometry at feature level is discussed. Section 4 describes the concept of cancelable biometrics. In section 5 a framework of the proposed scheme is presented. Finally, the summary and conclusions are given in last section.

II. RELATED WORK

The template protection schemes proposed in the literature can be broadly classified into two categories (see Figure 2), feature transformation approach and biometric cryptosystem approach [2]. In the feature transformation approach, a transformation function is applied to the biometric template and only the transformed template is stored in the database. The same transformation function is applied to query features and the transformed query is directly matched against the transformed template. Depending on the characteristics of the transformation function, the feature transform schemes can be further categorized as salting and non-invertible transforms. In salting, transformation function is invertible, i.e., if an adversary gains access to the key and the transformed template, she can recover the original biometric template (or a close approximation of it). Hence, the security of the salting scheme is based on the secrecy of the key or password. On the other hand, non-invertible transformation schemes typically apply a one-way function on the template and it is computationally hard to invert a transformed template even if the key is known.

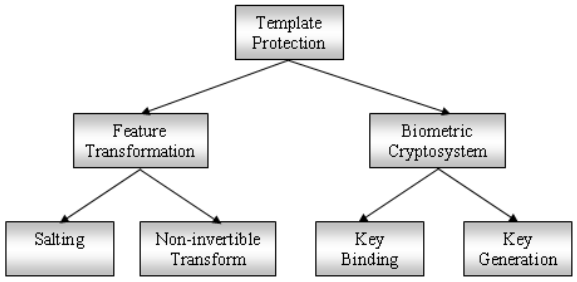

Fig.2. Categorization of template protection schemes

In a biometric cryptosystem, some public information about the biometric template is stored. This public information is referred to as helper data and hence, biometric cryptosystems are also known as helper data-based methods. While the helper data does not reveal any significant information about the original biometric template, it is needed during matching to extract a cryptographic key from the query biometric features. Matching is performed indirectly by verifying the validity of the extracted key. Biometric cryptosystems can be further classified as key binding and key generation systems depending on how the helper data is obtained. When the helper data is obtained by binding a key (that is independent of the biometric features) with the biometric template, it is referred as a key-binding biometric cryptosystem. If only the helper data is given, it is computationally hard to recover either the key or the original template. Matching in a key binding system involves recovery of the key from the helper data using the query biometric features. If the helper data is derived only from the biometric template and the cryptographic key is directly generated from the helper data and the query biometric features, it leads to a key generation biometric cryptosystem [8].

Since the biometric traits of a person cannot be easily replaced (unlike passwords and PINs), so a compromised template would mean the loss of a user's identity. Ratha et al. [9] have proposed the use of distortion functions to generate biometric data that can be canceled if necessary. They used a non-invertible transformation function that distorts the input biometric signal (e.g., face image) prior to feature extraction or, alternately, modifies the extracted feature set (e.g., minutiae points) itself. When a stored template is compromised, then the current transformation function is replaced with a new function thereby "canceling" the current (compromised) template and generating a new one. This also permits the use of the same biometric trait in several different applications by merely adopting an application-specific transformation function.

III. FEATURE LEVEL FUSION

Feature level fusion involves consolidating the evidence presented by two biometric feature sets of the same individual [10]. In this paper, face and hand geometry biometric traits are selected for fusion because the length of both feature vectors is fixed across all users. Fusion is accomplished by a simple concatenation of the two feature sets followed by feature selection or dimensionality reduction procedure. Let $X = \{x_1, x_2,\ldots x_m\}$ and $Y = \{y_1, y_2,\ldots y_n\}$ denote two feature vectors ($X \varepsilon R^m$ and $Y \varepsilon R^n$) representing the information extracted from two different biometric sources (face [11] and hand geometry [12]). The objective is to combine these two feature sets in order to yield a new feature vector, Z, that would better represent the individual. The vector Z of dimensionality k, $k < (m + n)$, is generated by first augmenting vectors X and Y, and then performing feature selection on the resultant feature vector in order to reduce its dimensionality.

A. Feature normalization

The individual feature values of vectors X and Y (i.e., the x_i's and y_i's) may exhibit significant variations both in their range and distribution. The goal of feature normalization is to modify the location (mean) and scale (variance) of the feature values via a transformation function in order to map them into a common domain. Any two of the simple min-max and the median normalization techniques may be used in this work. Let x and x′ denote a feature value before and after normalization, respectively. The min-max technique computes x′ as

$$x' = \frac{x - \min(F_x)}{\max(F_x) - \min(F_x)} \quad (1)$$

where F_x is the function which generates x. The min-max technique is effective when the minimum and the maximum values of the component feature values are known beforehand. In cases where such information is not available, an estimate of these parameters has to be obtained from the available sample training data. The estimate may be affected by the presence of outliers in the training data and this makes min-max normalization sensitive to outliers. The median normalization scheme, on the other hand, is relatively robust to the presence of noise in the training data. In this case, x′ is computed as,

$$x' = \frac{x - \text{median}(F_x)}{\text{median}(|(x - \text{median}(F_x))|)} \quad (2)$$

The denominator is known as the Median Absolute Deviation (MAD) and is an estimate of the scale parameter of the feature value. Normalizing the feature values via any of these techniques results in modified feature vectors $X' = \{x'_1, x'_2,\ldots x'_m\}$ and $Y' = \{y'_1, y'_2,\ldots y'_n\}$.

B. Feature selection

Augmenting the two normalized feature vectors, X′ (face) and Y′ (hand geometry), results in a new feature vector, $Z' = \{x'_1, x'_2,\ldots x'_m, y'_1, y'_2,\ldots y'_n\}$, $Z' \varepsilon R^{m+n}$. The `curse-of-dimensionality' dictates that the augmented vector need not necessarily result in an improved matching performance and some of the feature values may be noisy compared to the others. The feature selection process leads to choosing a minimal feature set of size k, $k < (m + n)$. The sequential forward floating selection technique is employed to perform feature selection on the feature values of Z′ [13]. This results in a new feature vector $Z = \{z_1, z_2,\ldots z_k\}$.

IV. CANCELABLE BIOMETRICS

A generic biometric system functions consist of two phases. The first phase is enrollment phase, in which the user's biometric template is acquired. The second phase is authentication phase, in which biometric sample is taken from the user and compared to the biometric template stored in the database. If they match, positive authentication is achieved. As long as the original biometric template is stored within the system database, it is vulnerable to potential attacks made by imposters. Hence the concept of cancelable biometrics is used in which the biometric templates are transformed into a different form before they are actually stored in the system database. This concept ensures that the original biometric template doesn't exist in the system. Thus cancelable biometrics can be used to upgrade the multimodal biometric system security by storing the transformed templates instead of storing the original biometric template in system database [14]. Transformation function is selected which is noninvertible, so that the template cannot be transformed back into its original form. The matching is performed by transforming the new acquired sample with the same transformation, and then making the comparison in transformed space. If an attacker is able to get to a transformed template, he would not be able to construct an artifact from it which could enable him to impersonate user. Cancelable biometrics is advantageous because when a database template is compromised, a new template can be issued just like a new password or card can be issued in a knowledge- or token-based authentication respectively. Also a cancelable template

stored in a database of certain applications cannot be used as a template in another application, thus preserving privacy [15].

The distortion transforms can be applied on either the signal level or the feature level [9]. That is, either the biometric signal can be transformed directly after acquisition, or the signal can be processed as usual and transformation is applied on the extracted feature set. Examples of transforms at the signal level include grid morphing and block permutation. Figure 3 shows the original image with an overlaid grid aligned with the features of the face and the adjacent image shows the morphed grid with resulting distortion of the face [16].

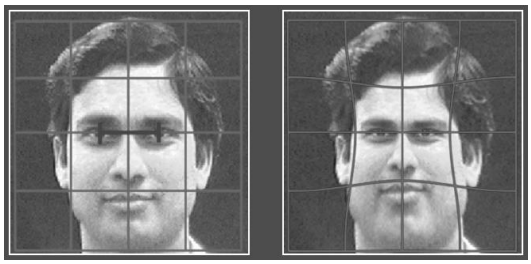

Fig.3. Distortion transform based on image morphing

An example of a transformation on the feature level [17] is a set of random, repeatable perturbations of feature points shown in figure 4. Here the blocks on the left are randomly mapped onto blocks on the right, where multiple blocks can be mapped onto the same block. Such transforms are noninvertible, hence the original feature sets cannot be recovered from the distorted versions. For instance, it is impossible to tell which of the two blocks the points in composite block B, D originally came from. Consequently, the owner of the biometrics cannot be identified except through the information associated with that particular enrollment. The distortion transforms permanently obscure the signal in a noninvertible manner.

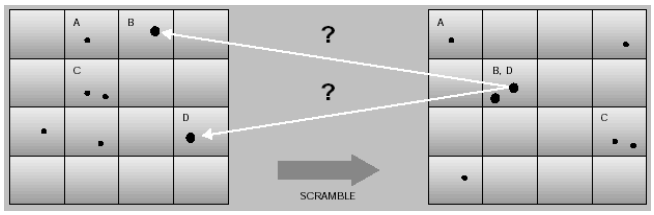

Fig.4. Distortion transform based on feature perturbation

V. PROPOSED SCHEME

To overcome the problems related with templates security (misuse of templates, modifying an existing template, adding a new template, and stolen templates) in template databases, a novel approach is proposed for the multimodal biometric verification systems. The proposed scheme also provides the ability to cancel the compromised template and reissue a new template and thus making difficult for an intruder to circumvent the system.

A. Architecture of the proposed scheme

Figure 5 shows the architecture of the proposed scheme integrating face and hand geometry at feature level to derive a single multi-biometric template and then securing this template with cancelable biometrics before storing it in the database. The proposed scheme consists of two phases: enrollment phase and verification phase.

In the enrollment phase, the two biometric sensors captures the two biometric traits (face and hand geometry) individually from the person to be verified and converts them to a raw digital format, which is further processed by the feature extraction modules individually to produce a compact representation that is known as the biometric template. The two templates resulting from the individual feature set extraction modules are then fed to the fusion module. Fusion module performs fusion of these two templates at feature level and produces as output a multi-biometric template (fused feature set) which is denoted by $Z = \{z_1, z_2, \ldots z_k\}$ of dimensionality k as described in section 3. After that, resulting multi-biometric template is fed to the cancelable transform module, which performs an intentional, repeatable distortion of this multi-biometric template based on a chosen non-invertible transformation function. This resultant multi-biometric cancelable template is finally stored in the system database.

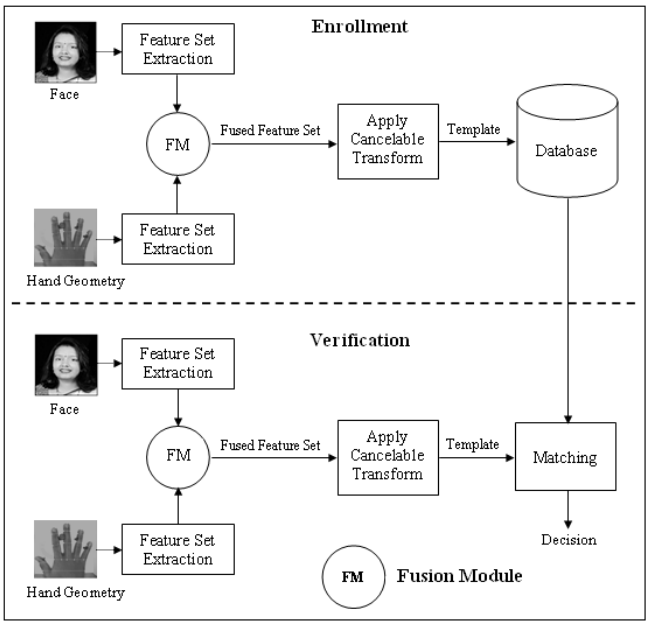

Fig.5. Architecture of the proposed template protection scheme for multimodal biometric systems

In the verification phase, the face and hand geometry sensors captures the two biometric characteristics individually from the person to be verified and converts them to a raw digital format, which is further processed by the feature extraction modules individually, fusion module, and cancelable transform module to produce a compact representation that is of the same format as the multi-biometric

templates stored in the database taken during the enrollment phase. This multi-biometric template is then compared with the claimed template in the database to find the similarity between the two feature sets. Finally the matching score is passed to the decision module where a person is declared as genuine or an imposter.

B. Working of the proposed scheme

This section describes working of the proposed scheme. Let $X = \{x_1, x_2,\ldots x_m\}$ and $Y = \{y_1, y_2,\ldots y_n\}$ denote two feature vectors ($X \varepsilon R^m$ and $Y \varepsilon R^n$) representing the information extracted from face (eigen coefficients) and hand (geometric features) biometric sources of a user respectively.

Fusion module: It combines these two feature sets X (face) and Y (hand geometry) in order to yield a new feature vector, Z. The vector Z of dimensionality k, $k < (m + n)$, is generated by first augmenting the two feature vectors, and then performing feature selection on the resultant feature vector in order to reduce its dimensionality. Normalization of X (face feature vector) and Y (hand geometry feature vector) can be done with either min-max or the median normalization techniques as discussed in section 3. Normalization of the feature vectors via any of these techniques results in modified feature vectors X′ and Y′ as given below:

$X' = \{x'_1, x'_2,\ldots x'_m\}$ and $Y' = \{y'_1, y'_2,\ldots y'_n\}$, where $X' \varepsilon R^m$ and $Y' \varepsilon R^n$

The normalized feature vectors X′ and Y′ are augmented which results in a new feature vector Z′ as given below:

$Z' = \{x'_1, x'_2,\ldots x'_m, y'_1, y'_2,\ldots y'_n\}$, where $Z' \varepsilon R^{m+n}$

Now, feature selection process [13] is performed on Z′ to reduce its dimensionality which leads to a minimal feature set Z of size k as given below:

$$Z = \{z_1, z_2,\ldots z_k\}, \text{ where } k < (m + n) \quad (3)$$

The feature selection process ensures that redundant feature values are detected and removed before invoking the matcher. This is one of the key benefits of performing fusion at the feature level.

Cancelable transform module: This module receives as input a minimal feature set $Z = \{z_1, z_2,\ldots z_k\}$ of size k, $k < (m + n)$ from fusion module. Here, some non-invertible transformation function F is applied on it which results in the new feature set Z^c of size k as given below:

$$F(Z) = Z^c, \quad (4)$$

$Z^c = \{z^c_1, z^c_2,\ldots z^c_k\}$, where $k < (m + n)$

This resulting feature vector Z^c is a cancelable multi-biometric template, which is finally stored in the database. Conceptually, a cancelable template is produced by transforming the input feature set into another representation space by applying a non-invertible transformation. Cancelable transform module distorts the multi-biometric template in the same fashion at each presentation (enrollment and every authentication), therefore these transformed templates are not required to convert back into their original form before they can be matched to new samples for authentication purposes. So, the matching is always performed in the non-invertible transformed space. The distortion transforms are selected to be noninvertible so that even if the transformation function and the resulting transformed biometric data both are known, the original (undistorted) biometrics cannot be recovered. Furthermore, if the transformed biometric data is compromised, then the transformation function can simply be changed to create a new transformed representation for reenrollment as, essentially, a new person.

This paper has proposed a multi-biometric template framework that can easily protect multiple biometric templates of a user (face and hand geometry) by first combining them at feature level and then applying a non-invertible transformation function to make it cancelable. The proposed template protection scheme also satisfies the following four properties suggested by [18] that an ideal biometric template protection scheme must possess.

1) Diversity: The cancelable transformation allows different sets of parameters in different applications, hence an individual can have a number of templates corresponding to the same biometric source that can be used in different applications.

2) Revocability: It is an ability of canceling the compromised template and reissuing the new one. The proposed scheme provides revocability in the way that it allows you to destroy the compromised template and reissue a new one by applying different transform on the same biometric data.

3) Security: The proposed scheme provides security at two steps. Feature level fusion provides the first step security by combining the two feature sets and creating a single database. Cancelable biometrics provides the second step security by making it hard to obtain original template from the transformed template and thus preventing an imposter to create a physical spoof of the stolen template.

4) Performance: The proposed template protection scheme should not adversely affect the recognition performance (i.e. FAR and FRR) of the original multimodal biometric system [10] rather it must improve the performance by providing the ability to cancel the compromised template.

C. Comparison with the existing system

1) The proposed scheme works on the basis of cancelable biometrics. It does not allow templates to be stored as original in database rather they will be stored after applying some non-invertible transformation. It helps a lot in protecting database templates by providing diversity and revocability.

The templates in database of existing multimodal biometric system are stored in the form given below

$Z = \{z_1, z_2, \ldots z_k\}$

where Z is the minimal feature set obtained after combining feature sets of face and hand geometry at feature level. Each z_i , i = 1…k represents some prominent characteristic of face or hand geometry. Here template is stored as original in the database.

The templates in database of multimodal biometric system employing proposed scheme are stored in the form given below

$Z^c = \{z^c_1, z^c_2, \ldots z^c_k\}$

where Z^c is obtained after applying some cancelable transformation (F) upon Z. Here, instead of original only transformed templates are stored in the database.

F is non-invertible transformation function, it ensures that there will be no match between original template and transformed template.

$$Z \neq Z^c \quad (5)$$

If Z^c is stolen, then by applying some another transformation (say F1), it can be reissued as Z^{cc} (new transformed template for the same biometric data). Also, it is impossible to generate original data from the stolen transformed template. This is the way, it helps in achieving diversity and revocability. Diversity is achieved by applying different transformations on the same biometric data in order to generate multiple variants to represent the same person. Revocability is achieved by specifying a new distortion transformation by changing its parameters. Cancelable biometrics always keeps original biometric data safe.

2) The proposed scheme is performing feature level fusion not only to enhance the recognition performance of individual traits but also to create single database for both traits. Multimodal biometric systems performing match score level fusion [19] or decision level fusion has to create a separate database for each biometric trait. Securing templates in each database separately could be an inefficient approach.

The above discussion indicates that multi-biometric framework followed by cancelability will provide both higher genuine accept rate and higher security.

VI. CONCLUSION

It is well known that a multimodal biometric system requires storage of multiple templates for the same user corresponding to the different biometric sources. Therefore, template security is more critical in these systems because multiple templates of the same user are to be secured. So, in this paper, we have described a unified scheme to secure multiple templates of a user by performing feature level fusion to derive a single multi-biometric template and then securing the multi-biometric template by applying cancelable biometrics. The proposed multi-biometric template protection scheme has higher security and better recognition performance as compared to the case when the individual templates are secured separately. However, the scheme presented in this paper, does not allow incompatible feature sets (minutiae points of fingerprint and eigen-coefficient of face) to be integrated. Future work will be focused upon the adoption of other biometric traits. In cancelable biometrics, the trade-off between discriminability (similarity structure) and non-invertibility of the transformation function must also be studied.

REFERENCES

[1] N.K. Ratha, J.H. Connell, and R.M. Bolle, "An analysis of minutiae matching strength", Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication, pp. 223-228, 2001.

[2] A. K. Jain, K. Nandakumar and A. Nagar, "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, January 2008.

[3] A. K. Jain, R. Bolle, and S. Pankanti, Eds., Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, 1999.

[4] B. Schneier, "The uses and abuses of biometrics", Communications of the ACM, vol. 42, no. 8, pp. 136, Aug. 1999.

[5] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns," IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp. 33-42, March-April 2003.

[6] A. Ross and A. K. Jain, "Information fusion in biometrics", Pattern Recognition Letters 24, pp. 2115-2125, Sep 2003.

[7] A. K. Jain and A. Ross, "Multibiometric systems", Communications of the ACM 47, pp. 34-40, Jan 2004.

[8] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges," vol. 92, no. 6, pp. 948–960, June 2004.

[9] N. Ratha, J. Connell and R. Bolle, "Enhancing security and privacy in biometric-based authentication systems," IBM Systems Journal, Vol. 40. No. 3, pp. 614 - 634, 2001.

[10] Arun Ross and Rohin Govindarajan, "Feature Level Fusion Using Hand and Face Biometrics", appeared in proceedings of SPIE conference on biometric technology for human identification II, Vol. 5779, pp. 196-204, (Orlando, USA), March 2005.

[11] M. Turk and A. Pentland, "Eigen-faces for Recognition", J Cognitive Neurosciences, **3** (1), 77-86 (1991).

[12] A. K. Jain, A. Ross, and S. Pankanti, "A prototype hand geometry-based verification system", in Second International Conference on Audio and Video-based Biometric Person Authentication (AVBPA), pp. 166-171, (Washington, D.C., USA), March 1999.

[13] P. Pudil, J. Novovicova, and J. Kittler, "Floating search methods in feature selection", Pattern Recognition Letters 15, pp. 1119-1124, November 1994.

[14] Miroslav Baca, Marko Antoni, "Upgrading Existing Biometric Security Systems by Implementing the Concept of Cancelable Biometrics".

[15] Anil K. Jain, Arun Ross, Umut Uludag, "Biometric Template Security: Challenges and solutions", appeared in the proceedings of EUSIPCO, September 2005.

[16] G. Wolberg, "Image Morphing: A Survey," The Visual Computer 14, 360–372 (1998).

[17] T. Beier and S. Neely, "Feature-Based Image Metamorphosis," Proceedings of SIGGRAPH, ACM, New York (1992), pp. 35–42.

[18] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Springer-Verlag, 2003.

[19] Sheetal Chaudhary, Rajender Nath, "A Multimodal Biometric Recognition System based on Fusion of Palmprint, Fingerprint and Face", in IEEE Xplore, International Conference on Advances in Recent Technologies in Communication & Computing, ARTCom 2009.