A Secure Biometric Authentication Scheme Based on Robust Hashing

Yagiz Sutcu  
Polytechnic University  
Six Metrotech Center  
Brooklyn, NY 11201  
ysutcu01@utopia.poly.edu

Husrev Taha Sencar  
Polytechnic University  
Six Metrotech Center  
Brooklyn, NY 11201  
taha@isis.poly.edu

Nasir Memon  
Polytechnic University  
Six Metrotech Center  
Brooklyn, NY 11201  
memon@poly.edu

ABSTRACT
High variability and irreplaceability of biometrics render the security paradigm governing conventional authentication and access control techniques inadequate. In this paper, we propose a technique that relies on a robust biometric hashing scheme to ensure the security and privacy of biometric templates. The privacy of a biometric template is preserved by using one-to-many transformed versions of the biometric features, obtained by means of polynomials generated in a template specific manner. The confusion property of the biometric hashing method is established by evaluating the designed polynomials at the measured feature values, and robustness of the proposed scheme is built into the polynomial design by limiting the effects of variation in biometric features. To ensure a proper diffusion effect, we deployed cryptographic hash functions. Our design takes into consideration security, performance and scalability issues. Experiments are conducted by applying the method on face biometric using the Olivetti and Essex Faces94 face image databases. Results show that the proposed scheme provides a simple and effective solution to the template security and privacy problems of biometric based authentication systems.

Keywords
Authentication, biometrics, robust one-way transform, security
1. INTRODUCTION

Multi-user systems are becoming more and more essential and indispensable parts of our daily life. From security point of view, in such systems, authentication is one of the most important mechanism needed for successful operation as it ensures someone or something is, in fact, who or what it is declared to be. In this regard, authentication mechanisms can be grouped into three main categories depending on the type of the authentication factor used. These are: 1) knowledge based (what you know; e.g., password, PIN); 2) object based (what you have; e.g., token, smartcard); and 3) identity based (who you are; e.g., biometrics) [1].

Most generally, the security of an authentication system is determined by the entropy of the secret information possessed by the users, and therefore, choosing a high entropy secret is essential to ensure security. However, today, majority of authentication mechanisms rely on private credentials like passwords and/or PINs for the proof of user identity, and relatively weak human memory puts a limitation on the achievable level of security since the passwords/PINs chosen by the users are easy to guess through automated procedures. In such systems, one common approach to increase the level of a security is by deploying multi-factor authentication schemes (e.g., using passwords and/or PINs in conjunction with smart cards or tokens).

One of the competing technologies for multi-factor authentication systems is the use of biometrics like fingerprints, iris data, face and voice characteristics. It is known that biometric data have much higher entropy as compared to ordinarily chosen passwords and PINs [1] but more importantly, they uniquely represent its owner. Furthermore, biometric features cannot be stolen, forgotten or duplicated easily. Due to these properties, biometrics based authentication systems are becoming widely used. Despite the inherent qualities, biometrics has its limitations. Most notably, biometric data are irreplaceable, they exhibit dramatic variability, and they are subject to imperfect data acquisition process.
Typically, a biometric system employs a matching algorithm which tries to match the biometric data acquired by a sensor with a template, created at the enrollment stage and stored in a database, to decide whether authentication succeeds or fails. However, this template cannot be a true representation of the user’s biometrics because if the template database is compromised the biometrics cannot be renewed and they are no more usable. Also, due to the dramatic variability of biometrics and the imperfect data acquisition process, cryptographic hashing algorithms, which are designed to have good diffusion properties, cannot be used for securing the template.

In this work, we propose a simple yet practical solution to the template security problem of biometric authentication systems. The scheme is based on robust one-way transformation (robust hashing) of the biometric data. We assume that the biometrics is subject to noisy measurement but ordered, i.e., each measurement yields same values except for the measurement noise. Our approach takes into consideration security, performance, and scalability issues. We provide results (e.g., probability of false acceptance and false rejection rates) obtained using Olivetti face image database (ORL database) and Essex Faces 94 face image database (E94 database).

The paper is organized as follows. We start by providing a survey of proposed biometrics based authentication methods in Section 2. Design issues and objectives will be stated in Section 3. In Section 4, the basic idea behind the proposed scheme will be introduced and details of the construction will be provided. In Section 5, we elaborate on the test setup and present performance results obtained with the two face image databases. Our conclusions and the scope of future work will be provided in the last section, Section 6.

2. PREVIOUS WORK

Many different ideas have been proposed in recent years to overcome the security problems associated with biometric-based authentication systems. Davida et al. [2] were among the first to propose off-line
biometric authentication scheme for iris biometric is based on error correcting codes (ECC). They suggested storing a signed form of biometric template in a portable storage device, like smartcard, instead of a database and matching the biometric data locally. However, despite provable security of the algorithm, storing error-correcting bits in the database leak some amount of information about biometric data of the user.

Juels and Wattenberg [3] proposed a fuzzy commitment scheme which is also based on ECC. The basic idea in [3] is that, a secret key is chosen by the user and then encoded using a standard ECC. This encoded secret key is xored with the biometric template to ensure the security of the template and then stored in the database. During verification, the biometric data is xored with the values stored in the database. If the biometric data is close to the one presented at the enrollment stage, the authenticator will be able to correct some of the errors (present in the newly measured biometric data) and secret key will be retrieved correctly and revealed to the user. In fact, it is not clear how this method can be used with some biometric data because it is not evaluated on any real-life biometric data.

Later, to address the problem of unordered feature representations (e.g., the minutae representation of fingerprints), Juels and Sudan [4] proposed the “fuzzy vault” scheme. The “fuzzy vault” scheme combines the polynomial reconstruction problem with ECC. In the method, an appropriately chosen secret polynomial with degree k is evaluated at each and every component of n dimensional feature vector (with n>k) to construct a set of points. Then, a number of fake (randomly generated) points that do not lie on the initially selected polynomial are mixed with the real points so that genuine users with enough number of real points (k+1 real points) will be able to reconstruct the secret polynomial. Although authors provided detailed analysis of the theoretical bounds on the security provided by the scheme, their construction assumes discrete valued data without any noisy perturbation, thereby making the approach unsuitable for noisy biometric data. In [5], Clancy et al. modified the fuzzy vault scheme by incorporating a quantization step (fingerprint vault) considering minutae representation of
fingerprints. In their model, minutae points are defined in two-dimensional space under additive (spherical) Gaussian measurement noise. They provided optimal operating parameters under various attack scenarios. (It should be noted that, successful operation of this scheme requires near-perfect pre-alignment of the fingerprints.)

Linnartz and Tuyls [6] introduced the concept of versatile secure biometric authentication scheme which employs shielding functions to preprocess the measured biometric data. They later extended their ideas in [7]. Their construction focuses on the continuous spaces and assumes a particular input distribution (a known multivariate Gaussian) and is inspired from dithered quantization techniques used by watermarking [8]. Dodis et al. [9] introduced the notion of secure sketch and fuzzy extractor as two primitives for extracting uniform randomness from biometric data. Their construction is based on creating helper data, called secure sketch, which does not reveal much information about the original data and which will be used for reconstructing the original data from its noisy version. Then, the secret key is extracted reliably from reconstructed data. Hamming distance, set difference and edit distance measures are considered as a metric that defines the closeness of noisy data to the original one and they analyzed entropy loss vs. error tolerance trade-off and decoding efficiency of their construction. The reusability of sketches is considered in [10] and it is shown that when more than one sketch of the same data are obtained by an attacker, the scheme may become insecure. All methods proposed in [2-7, 9, 10] are based on an architecture which uses helper data extracted from original data. In [11], secrecy and identification capacity concepts are introduced and performance bounds are derived for schemes that employ helper data architecture.

The concept of cancelable biometrics was first introduced by Ratha et al. [12]. The underlying idea of the scheme is to store a distorted version of the template (instead of the original one) through the use of a fixed noninvertible transformation which is applied directly at the sensor. This approach gives the
opportunity to cancel that template and corresponding transformation when the biometric data and/or transformations are compromised.

Connie et al. [13], Teoh et al. [14] and Jin et al. [15] proposed similar biometric hashing methods for cancelable biometrics problem. The basic idea of these approaches is to create an orthogonal basis using a tokenized random number to project the feature vectors and then thresholding them to obtain a binary hash value. Although high performance is achieved for faces, fingerprints and palmprints, their results are obtained under the assumption that tokenized random numbers cannot be stolen and used by an impostor. In [15] the authors showed that when the tokenized random numbers are stolen and used by impostors, the system performance becomes unacceptable for real-world applications. More detailed analysis of this flaw is elaborated in [16]. In [17], authors proposed to improve this biometric discretization idea by classifier based fusion. They suggested combining the matching scores by fusion among on-line signature matchers where only half of the matchers use the biometric data combined with the tokenized pseudo-random numbers.

In the literature, there are many other approaches which address the same problems. Vielhauer et al. [18] proposed a simple method to calculate biometric hash values using statistical features where the hash is calculated as the integer quotient obtained by first subtracting an offset value from the measured feature value and then dividing the result by the length of the allowable range for that feature. Password hardening approach which takes into consideration the keystroke dynamics is introduced by Monrose et al. in [19] and generating cryptographic keys using voice proposed in [20]. A key binding algorithm is proposed by Soutar et al. in [21] and minimum average correlation energy filters based face recognition scheme is proposed by Savvides et al. in [22].
3. DESIGN GOALS

The most important step in a system design process is to determine appropriate set of goals to conduct systematic evaluation of the system. Considering the security and privacy related problems inherent to biometrics and proposed solutions to these problems, it can be deduced that a biometric-based authentication scheme should satisfy the following three essential design goals.

Performance: The performance of the biometric systems is determined in terms of basic performance measures, namely, *false acceptance rate (FAR)* and *false rejection rate (FRR)*. *FAR* measures the rate of impostors who are incorrectly accepted as legitimate users, while *FRR* measures the ratio of valid users who are rejected as imposters and for biometric systems the *FAR* and *FRR* can typically be traded off against each other by changing some tunable threshold parameter. Another important performance measure of real-world biometric systems is the rate at which both accept and reject errors are equal, i.e., the equal error rate (*EER*). The lower the *EER*, the more accurate the system is considered to be. However, two factor authentication schemes that rely on biometrics and smartcards or tokens, suffer from another problem which arises when an impostor steals or duplicates the smartcard of a particular user and tries to authenticate himself as that user. (This is the likelihood of user A authenticating himself as user B while using user B’s smartcard.) This type of error can be interpreted as a factor contributing to *FAR*. For the sake of clarity, we will denote such errors by *FAR-II*.

Scalability: One of the basic design considerations for authentication and/or recognition based schemes is the scalability which refers to the capability of responding efficiently to increasing number of users. Most of the well known pre-processing techniques such as principal component analysis (PCA) require the whole dataset of users for training, which degrades the scalability of the scheme in which it is employed. Since the number of users may vary over a time, the design has to be flexible enough to accommodate new user addition/deletion with minimum cost by ensuring collision-free operation.
Security: Another critical design challenge of a biometric-based authentication system is template security and privacy. This requires the presence of a mechanism such that even if the template database and/or any other side information is compromised, it should be very hard, if not impossible, to recreate or to get the original template. Furthermore, the scheme should be able to provide an easy and efficient way to reset the user’s authentication data which might be stored in a database or any other portable device when security is compromised.

4. PROPOSED SCHEME

In this section, firstly, basic idea behind the proposed scheme will be introduced. Then, details of our step-by-step construction will be provided.

4.1 Basic Idea

In password-based authentication systems, secure cryptographic hashing algorithms (such as MD-5 and SHA-1) ensure the secure storage of the passwords in a database. In that case, authentication process is basically a comparison of the two hash values which are the hash of the password typed and the hash value stored in the database. However, unlike passwords, the high variability of biometric data and the imperfect data acquisition process prevents the use of secure cryptographic hashing algorithms for securing the biometrics data because of the fact that, secure cryptographic hashing algorithms give completely different outputs even if the inputs are very close to each other.

In the context of biometric authentication, the solution of this problem requires the need for a new class of hash functions, namely, robust hashing algorithms. Ideally, a robust hashing algorithm hashes two close inputs to the same hash values whereas inputs that are significantly apart hashed to unpredictable hash values. Unfortunately, the design of such a function with very good confusion and diffusion properties is a challenging research problem. To realize such a function, we adopted the idea of decoupling the robustness/error-tolerance and security aspects of the problem into two parts. So that
the first component provides robustness to noise, modeling errors and input variability (which is very high when biometric data are considered), and the second one enables incorporating the security properties provided by a cryptographic hash functions. Furthermore, this decoupling gives the freedom of designing these robust one-way transformations in a user-dependent way which are then stored in either a smartcard or a database.

In this study, based on this decoupling idea, a one-way transformation-based hashing scheme is proposed. In the proposed scheme, one-way transformations are tailored specifically for each user based on their biometrics. This is realized first by obtaining a transformed version (through a random mapping) of the feature vector of a user at the enrollment, and then the resulting transformed vector is used to design a number of polynomial functions such that when evaluated at the transformed values, the polynomials yield a unique and independently determined output vector. Finally, the biometric hash value is obtained as the cryptographic hash of this output vector and stored in the template database. In a similar manner at the time of authentication, the captured biometric features are hashed using the user specific one-way transformations and compared to its stored version for a decision. We assume the parameters of these transformations are obtained by a trusted entity and either kept in a separate database or provided to the users in a smart-card. In the proposed system, the only trusted component is the device that captures the biometric data and performs the one-way transformation. On the other hand, the template database and user specific parameters are not trusted, and their compromise does not reveal any information on the actual biometrics of the user.

In [23], a similar robust hashing method has been proposed where one-way transformations are designed as a sum of properly weighted and shifted Gaussian functions rather than as polynomials. However, one of the main weaknesses of that scheme was its inability to compensate small amount of errors introduced by measurement noise and modeling errors. That is even if one of the feature components is slightly shifted out of the estimated range for that component, due to measurement noise
and modeling errors in the training phase, the authentication would fail. In this modified version of the scheme, the error-tolerance of the scheme is further improved by incorporating a randomization step as a part of the one-way transformation stage. This randomization step also provides more freedom and flexibility in creating user-specific output vectors by increasing the dimensionality of the new feature vector representation of the biometric data without any performance degradation. We also tested our scheme on a larger dataset and compared the results with the results of the scheme in [23]. In the following subsections, basic steps of our construction will be explained in details.

4.2 Details of Construction

In this section, we will provide details of our construction to achieve our design objectives. The enrollment and authentication processes are illustrated in Figure 1. At the enrollment stage, the biometrics of each user is acquired and feature vectors are extracted several times as a part of training process. These feature vectors are then transformed into a new representation via multiplying with a random matrix specific to each user. Then the variation of each transformed feature vector component is estimated by analyzing the training dataset. This statistical information is then used to design high order polynomials associated with each feature component. All these user dependent information (random transformation and polynomials) are assumed to be stored in smartcards which are needed at the time of authentication. (It should be noted that this information can also be kept in a separate database to be used during authentication.) At the time of authentication, similar to enrollment, each user’s biometric data is acquired with the sensor and the corresponding feature vectors are extracted. Then, the random mapping matrix and the one-way transformation function stored in the smartcard are generated, and these functions are evaluated at transformed feature values. Finally, the resulting values are quantized and arranged into a vector and hashed using a secure cryptographic hash function (such as MD5 or SHA-1). The hashed value will be compared to user’s entry in the database for authentication.
4.2.1 Feature Extraction

Due to the ease of capturing and availability of many powerful digital signal processing tools to analyze digital images, face images are one of the widely used biometrics for authentication purposes. As it is the case for many face image based biometric recognition systems proposed in recent years, singular values are used as feature vector [24-26]. Although in [27], authors showed that singular values only contain a limited amount of useful information about the image and the most useful part of the information is contained in the two orthogonal matrices of singular value decomposition, another important concern is the robustness of the features. In this regard, singular values are widely used in image watermarking applications due to their robustness to malicious processing (aimed at removing embedded watermarks). Thus, feature selection requires a trade-off between distinctiveness and robustness of the features. Due to established properties of singular values, we also used them for testing...
our scheme. However, it should be noted that the essence of the technique is not specific to face image data and can be applied to any type of ordered biometric features.

Following theorems will be helpful to understand the singular value decomposition and robustness properties of singular values.

**Theorem 1 (Singular Value Decomposition)**

If $A \in \mathbb{R}^{m \times n}$ then there exist orthogonal matrices $U \in \mathbb{R}^{m \times m}$ and $V \in \mathbb{R}^{n \times n}$ such that $A = U \Sigma V^T$ where $\Sigma = \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_p)$ with $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_p$ and $p = \min(m, n)$.

**Theorem 2 (Perturbation)**

Let $\tilde{A} = A + E \in \mathbb{R}^{m \times n}$ be a perturbation of $A$ and let $\tilde{A} = U \Sigma V^T$ be singular value decomposition of $\tilde{A}$, then $|\lambda_i - \tilde{\lambda}_i| \leq \|E\|_2$ for $i = 1, \ldots, p$ where $\|E\|_2$ is induced-2 norm of $E$.

Since SVD is one of the well-known topics of linear algebra, we omitted to give detailed analysis of this subject and interested reader may find more details in [28].

### 4.2.2 Robust Noninvertible Transformation Design

In this approach, we simply assume that every component of the $n$-dimensional feature vector is taking some value in some range without imposing any constraint on the values and ranges as follows:

$$V_i = [v_{i1}, v_{i2}, \ldots, v_{im}]^T$$

is the $n$-dimensional feature vector of $i$th user of the system and

$$\bar{v}_{ij} - \delta_j \leq v_{ij} \leq \bar{v}_{ij} + \delta_j \quad i = 1, \ldots, m; j = 1, \ldots, n$$

where $2\delta_j$ determine the range of the $j$th component of the feature vector of the $i$th user and $m$ is the total number of the users. The one-way transformation includes the following basic operations.
• **Randomization:**

A $k$-by-$n$ matrix, $R_i$ for user $i$, with the elements which are uniformly distributed random numbers between $-\theta$ and $\theta$ is generated. By multiplying feature vector with this random matrix, $n$ dimensional feature vector is mapped into another $k$ dimensional vector as

$$W_i = R_i V_i = [w_{i1}, w_{i2}, ..., w_{ik}]^T$$ (2)

with $-\rho_j \leq w_{ij} \leq \rho_j$ for $i = 1, ..., m; j = 1, ..., k$ and where $2\rho_j$ determine the range of the $j$th component of the new $k$ dimensional feature vector of the $i$th user and $m$ is the total number of the users.

Main reason behind using such a random mapping is due to the fact that, using randomly weighted sum of feature vector components, instead of using features separately, provides a simple error-correction action. That is, the correlation of the feature vector components, injected by randomization step, will be able to compensate for small number of out-of-range variations of the original feature values in the new feature representation.

To understand this fact more clearly, let’s assume that the feature vector components are Gaussian distributed. For user $i$, $V_i = [v_{i1}, v_{i2}, ..., v_{im}]^T$ is a vector of $n$ independent jointly Gaussian random variables (RVs) and random mapping operation is realized by an $n$-by-$n$ (here we assume that $k=n$) matrix. Before random mapping, probability density function (pdf) of the $n$-dimensional feature vector can be written as a pdf of a multivariate Gaussian random variable

$$f_{V_i}(V_i) = \frac{1}{(2\pi \det(C_i))^{n/2}} \exp\left(-\frac{1}{2} [V_i - \mu_i]^T C_i^{-1} [V_i - \mu_i]\right)$$ (3)

where $\mu_i = [\mu_{i1}, \mu_{i2}, ..., \mu_{in}]^T$ is a vector of mean values and $C_i = E\{(V_i - \mu_i)^T (V_i - \mu_i)\} = \text{diag}\{\sigma_{i1}^2, \sigma_{i2}^2, ..., \sigma_{in}^2\}$ is the covariance matrix which is a diagonal matrix of variance values of user $i$’s feature vector,
respectively. Since these $n$ RVs are independent, joint pdf can be written in the form of product of corresponding $n$ scalar Gaussian pdf as

$$f_{V_i}(V_i) = \prod_{j=1}^{n} \frac{1}{(2\pi\sigma_j^2)^{1/2}} \exp(-\frac{1}{2} \frac{(V_{ij} - \mu_{ij})^2}{\sigma_j^2})$$

Under these model assumptions, authentication will be successful if all of the $n$ feature vector component values (measured at the time of authentication) are in the corresponding interval $[\mu_{ij}-3\sigma_{ij}, \mu_{ij}+3\sigma_{ij}]$ which covers the 99.73% of the area under the scalar Gaussian pdf.

Since the linear transformation of jointly Gaussian RVs is also jointly Gaussian, after $n$-by-$n$ random mapping operation, pdf of our new feature vector will be

$$f_{W_i}(W_i) = \frac{1}{(2\pi \text{det}(K_i))^{n/2}} \exp(-\frac{1}{2} \frac{(W_i - \eta_i)^T K_i^{-1} [W_i - \eta_i]}{\text{det}(K_i)})$$

where $\eta_i = [\eta_{i1}, \eta_{i2}, \ldots, \eta_{in}]^T$ is a vector of mean values and $K_i = E\{(W_i - \eta_i)^T (W_i - \eta_i)\} = R_i^T C_i R_i$ is the covariance matrix (which is not diagonal) of user $i$’s new feature vector, and $R_i$ is $n$-by-$n$ random matrix which is non-singular. As a result of random mapping, new feature vector components will also be a jointly Gaussian RVs but not independent. After this transformation, authentication will be successful if all of the $n$ feature vector component values (measured at the time of authentication) are in the interval $[\eta_{ij}-3s_{ij}, \eta_{ij}+3s_{ij}]$ where $s_{ij}$ is the standard deviation of the $j^{th}$ component of $i^{th}$ user’s new feature vector.

Due to the correlation injected by random mapping, we will have

$$\text{Pr}\{|W_i - \eta_i| \leq 3s_i\} \geq \text{Pr}\{|V_i - \mu| \leq 3\sigma_i\}$$

where $\text{Pr}\{|V_i - \mu| \leq 3\sigma_i\}$ is the probability of correct authentication of user $i$ when $n$ dimensional feature vector (before random transformation) is considered and $\text{Pr}\{|W_i - \eta_i| \leq 3s_i\}$ is the probability of correct authentication of user $i$ when $k$ dimensional ($k=n$) new feature vector (after random transformation) is
considered. This will eventually provide some degree of error resilience against measurement noise and modeling errors and therefore will improve the performance of the scheme by decreasing $FRR$. Joint probability distribution functions of two dimensional independent and correlated Gaussian random variables and probability of correct authentication ($\Pr\{\|W - \eta_i\| \leq 3s_i\}$) for different values of correlation coefficient (for two dimensional case) are illustrated in Figure 2.

When the dimensionality of new feature space, $k$ is greater than $n (k> n)$, rank of the covariance matrix $K_i$ will be $n$ and as a result, $K_i$ will be singular. Eigenvalue decomposition of $K_i$ will be

$$K_i = E_i D_i E_i^T$$  \hspace{1cm} (7)

where $E_i$ is $k \times n$ matrix with rank $n$ and has the columns that are the eigenvectors of the $n$ positive eigenvalues of $K_i$ and $D_i$ is $n \times n$ diagonal matrix with $n$ positive eigenvalues of $K_i$ which are on the diagonal. Therefore, pdf of $W_i$ with a singular covariance matrix will be defined in terms of generalized inverse of $K_i$ and the reduced dimension pdf as

$$f_{W_i}(W_i) = \frac{1}{(2\pi \det(D_i))^{n/2}} \exp\left(-\frac{1}{2}[W_i - \eta_w_i]^T K_i^{-1} [W_i - \eta_w_i]\right)$$  \hspace{1cm} (8)

where $K_i^{-1}$ is the generalized inverse of $K_i$ defined as

$$K_i^{-1} = E_i D_i^{-1} E_i^T$$  \hspace{1cm} (9)

In that case, the possible sample values for $W_i$ would all lie in an $n$-dimensional proper subspace of $\mathbb{R}^k$, meaning that, only $n$ of these $k$ random variables will be sufficient and remaining $k-n$ random variable will be expressed by appropriate linear combinations of first $n$ random variable. Therefore, increasing $k$ beyond $n$ will not provide any more performance increase. However, if $k$ is chosen greater than $n$, capacity of collision-free system (in terms of maximum number of user) becomes much higher.
Figure 2. 2-dimensional joint pdf of gaussian distributions for correlated and uncorrelated random variables (on the left) and corresponding correct authentication probabilities for different correlation coefficient values.

It should be noted that choosing $k$ smaller than $n$ ($k < n$) translates into throwing away some amount of useful information which will reduce the entropy of biometric data. This entropy loss will consequently decrease the distinctiveness of the biometric features and will cause an increase in $FAR-II$ of the system. Therefore choosing $k < n$ is not a clever choice. (This performance degradation due to entropy loss is clearly observed in our simulation results as will be shown in Section 4.)

• **Output Vector Selection**

To ensure collision-free operation of proposed scheme, we have to ensure that the output of the one-way transformation for each user is different. Let $\mathbf{o}_i = [o_{i1}, o_{i2}, \ldots, o_{ik}]^T$ for $i = 1, \ldots, m$ (where $m$ is the total number of users and $k$ is the dimensionality of the feature vector) represent the designated output vector (codevector) for user $i$. Therefore, considering $m$ potential users, a $k$-by-$m$ matrix $\mathbf{O} = [\mathbf{o}_1 \ \mathbf{o}_2 \ \ldots \ \mathbf{o}_m]$ has to be generated in advance to ensure that any two columns are not same. This can be interpreted as a real valued codevector generation with a minimum distance requirement By the time of a new user addition,
one unassigned column from that matrix will be assigned to that user and the corresponding one-way transformation will be designed using these codevector values.

Since proposed scheme combines robust transformation with a cryptographic hashing algorithm which is assumed secure and collision resistant, one may argue that, collision-free operation can be achieved by satisfying the condition that any two columns of matrix $O$ are not identical. However, due to high variability of biometric data and measurement noise, we need to be more conservative and make certain that code-vectors are sufficiently *distanted* to each other. For this purpose, we defined the following measure for quantifying the closeness of two code-vectors.

**Definition:** Let $o_i=[o_{i1}, o_{i2}, ..., o_{ik}]^T$ and $o_j=[o_{j1}, o_{j2}, ..., o_{jk}]^T$ be two different $k$-dimensional output vectors with $\Delta$-quantized real numbers. If there exists a set $Q \subseteq \{1, 2, ..., k\}$ with cardinality $\Omega$ such that; for every $q \in Q$, $|o_{iq} - o_{jq}| > \Delta$ is satisfied, then we will say that $o_i$ and $o_j$ are separated by $\Omega$.

It should be noted that the above closeness definition is based on the notion that the maximum variation in any of the feature vector components might at most induce a variation of $\Delta$ in the codevector component (output of the one-way transformation) which has to be determined empirically based on the variation of the feature vector components at the enrollment stage. The quantization step size $\Delta$ can be fixed to the same value for all users based on the worst case variation of the user feature vector components, e.g., depending on the maximum of the ratio of $\rho_{ij}$ to overall range. Another possibility is that, $\Delta$ can be determined separately for each user (or even separately for each feature of each user). In the latter case, there will be different quantization steps, $\Delta_i$ (or $\Delta_{ij}$) for each and every user and these values need to be stored at smartcards as well.

That is, to ensure collision-free operation, any two different columns of $O$ should be well-separated by $\Omega$ where $\Omega$ can be set to a fixed value or lower bounded by some value depending on the problem setting and distribution characteristics of selected features. The $O$ matrix satisfying this constraint can
be systematically generated. For example, one trivial realization is by generating the first code-vector randomly and generating each of the following codevectors by incrementing (decrementing) $k$-$\Omega$ component values by $\Delta$ and the select $\Omega$ component values with some multiples of $\Delta$.

- **Polynomial generation:**

There are many possible non-invertible transformations that can be deployed in achieving template privacy and providing some degree of robustness to input variability. In this study, we realized this through generating higher-order polynomials which can be easily and uniquely determined by solving a set of linear equations when appropriate set of points is given.

At the first step of enrollment stage, the biometric data of a user is acquired a number of times to capture the inherent variation of the user $i$’s biometrics, then each feature is multiplied by $R_i$ (for user $i$) and range information of each user’s new $k$ dimensional feature vector ($\rho_{ij}$) is obtained. Notice that due to the correlation of the components of the $k$ dimensional feature vector, $\rho_{ij}$ will be different from $\delta_{ij}$ (1). Once this information is determined, every component of the $k$ dimensional feature vectors are considered separately and a higher order polynomial is fitted to corresponding range considering the quantized output value assigned to that component of the feature vector. Let us explain this fitting operation with the help of an example.

Consider $j^{th}$ component, $w_{ij}$, of the feature vector of user $i$. Assume that $w_{ij}$ takes values between $(\bar{w}_{ij} - \rho_{ij})$ and $(\bar{w}_{ij} + \rho_{ij})$ and also assume that $o_{ij}$ is the assigned output value for that component of the feature vector. Then, first set of points to be used for polynomial fitting will be the set $C_1 = \{(x_1, y_1), (x_2, y_2), (x_3, y_3)\}$ where $(x_1, y_1) = (\bar{w}_{ij} - \rho_{ij}, o_{ij} + \alpha)$; $(x_2, y_2) = (\bar{w}_{ij}, o_{ij})$ and $(x_3, y_3) = (\bar{w}_{ij} + \rho_{ij}, o_{ij} - \alpha)$ with $\alpha \in \{-\Delta/2, \Delta/2\}$. Furthermore, we generate another set of points, $C_2$, consist of $d$-2 randomly generated points (where $d$ is the degree of the polynomial to be created) over all
feature range. Using the set of points, \( C = C_1 \cup C_2 \) polynomial \( P_j(x) \) is obtained as shown in Figure 3. Same procedure is repeated for every component of the feature vector for \( j = 1, \ldots, k \) and set of polynomials obtained then stored in the smartcard of the user \( i \).

![Graph showing high order polynomial as robust one-way transformation.](image)

**Figure 3. High order polynomial as robust one-way transformation.**

5. EXPERIMENTAL RESULTS

In our experiments we have used the Olivetti Face Database (ORL database) [29] and Essex Faces 94 face database (E94 database) [30] which are essentially created for face recognition related research studies. However, these databases are also used by some researchers for biometric authentication system design enabling a common ground for researchers to compare the performance of their algorithms [14, 15]. In comparison to ORL database, E94 database is considered less challenging due to the fact that illumination, scales and aspects of images taken from the same person have relatively less variations compared to the images of ORL database and this fact can be observed in our experimental results. Sample image sets from the two different databases are given in Figure 4.
ORL face database consists of 10 different images of 40 distinct subjects and the size of each image is 92x112, 8-bit grey levels. On the other hand, E94 database consists of 20 different images of 152 distinct subjects and the size of each JPEG image is 180x200. However, before we start our simulations, we transformed these JPEG images to 8-bit grey level images and then used in our experiments. In our simulation, we randomly divide each 10 samples of subjects from ORL database into two parts, namely, training and test sets where training set is assigned 6 of the images and test set has the remaining 4 sample face images. Similarly, each 20 samples of subjects from E94 database is divided into two sets while training set has 12 of the images, test set has the remaining 8 samples. In our simulations, only first 20 singular values of the images are considered.

After extracting \( n \) dimensional feature vectors (simply the first n singular value of the face image) from the set of training images, we transform this feature vectors to another \( k \) dimensional feature space and then we determine the range of variation for each \( k \) dimensional feature vector component. The range for each component is estimated by measuring the maximum and minimum values observed in the training set to obtain the interval \([ \bar{w}_j - \rho_j, \bar{w}_j + \rho_j ]\) and expanding this interval by some tolerance factor \( t \) which is the tunable threshold value of our biometric authentication scheme, ROCs of the proposed scheme are obtained. However, since the random mapping, \( R_s \) will be different for each realization; it is needed to calculate an average value of the performance metrics, namely, \( FRR \) and \( FAR-II \). Therefore, we evaluated performance metrics over 300 realizations in our simulations to calculate the average. Furthermore, since our datasets consist of rather small number of users, the output codevectors, i.e., \( O \), is generated randomly for \( \Omega \geq 1 \) to satisfy the constraints described in Section 3.2.2. For this setup, we fixed the quantization step size \( \Delta \) based on the worst case variation of the user feature vector components, e.g., depending on the maximum of the ratio of \( \rho_j \) to overall range.
For ORL database, 4 test data for every user is used to generate 40x4=160 genuine authentication attempts and 39x40x4=6240 impostor authentication attempts (4 attempts by 39 remaining users for every user in the system). Our results obtained by changing the dimensionality of new feature vector space, $k$, from 20 to 140 and $FRR$ vs. $FAR-II$ curves are given for these values of $k$ and the curve of the earlier version of this scheme as well. Similarly, for E94 database, 8 test data for every user is used to generate 152x8=1216 genuine authentication attempts and 151x152x8=183616 impostor authentication attempts (8 attempts by 151 remaining users for every user in the system). Our results obtained by changing the dimensionality of new feature vector space, $k$, from 5 to 140 for ORL database and from 20 to 280 for E94 database and $FRR$ vs. $FAR-II$ curves are given for these values of $k$ together with the curve of the earlier version of this scheme as well. We also analyzed the variation of $EER-II$ with
respect to the ratio of $k/n$, which represents the ratio of dimensionality augmentation obtained by random mapping.

In terms of performance, proposed scheme achieves arbitrarily low $FRR$ values when $FAR$ value is set to zero. However these results are meaningful under the assumption that, every smartcard will always be used by its legitimate owner and will never be stolen and/or duplicated. Definitely, this assumption is not realistic. However $EER-II$ values presented here (Figure 5) actually are the values obtained by $FAR-II$ vs $FRR$ curves which represent the case when the smartcard of user A is stolen/duplicated by another user of the system, namely, B, and user B tries to authenticate himself/herself as A using smartcard of user A.

Figures 5a and 5c show the performance of the proposed scheme for ORL database and E94 database, respectively, for $\theta=100$. As observed in all cases, random linear transformations increase the performance of the biometric authentication system in terms of $EER-II$. As mentioned earlier, this performance improvement is the consequence of the random mapping which actually performs an error-correction like task by creating correlated feature vector components. Since the new feature space is less sensitive to the modeling errors and sensor noise, minor out-of-range variations of the feature values are corrected.

In [14] and [15], outstanding performance reported with the same datasets considered in this study. However, the assumption in these studies is that, tokens are always used by legitimate users and never used by impostors. Although dataset used in [16] is different from the datasets considered in [14] and [15], authors proved that the performance of the scheme (proposed in [14] and [15]) becomes unacceptable when stolen/duplicated tokens are considered. In contrast, under the framework proposed, performance results ($FRR$ vs. $FAR-II$) completely depend on the distinctiveness of the selected biometric features considered, e.g., singular values. If the pairwise distances between biometric feature vectors of
each and every user are large enough, it will be possible to achieve very low $EER-II$ values as well. It should be noted that, to further improve the performance of the proposed scheme, one can employ data pre-processing techniques such as PCA or other well-known techniques. However in this case, the degree of scalability of the scheme will be drastically lower.

![Graphs showing performance metrics](a)(b)(c)(d)

Figure 5. Performance of the proposed scheme.
In Figure 5b and 5d, effect of increasing the dimensionality of the transformed feature vector, $k$, on the system performance ($EER-II$ versus the ratio of the dimensionality augmentation, $k/n$) investigated for three different value of $\theta$ ($\theta=1$, $\theta=10$ and $\theta=100$). It can be concluded that the effect of $\theta$ on the performance of the scheme is not significant. However, as seen from the graphs depicted, $EER-II$ values are improved by increasing the ratio $k/n$ at the beginning but then stabilized at very close values for all three cases considered. Although, as explained in the previous section, increasing the dimensionality $k$ beyond $n$ has no effect on the performance of successful authentication due to the rank deficiency of the covariance matrix of the distribution of the transformed feature vector, this random mapping lowers the $FAR-II$ value as well, which results in overall performance improvement in terms of $EER-II$. Although it is very difficult to analyze the effect of increasing $k$ on the change of the $FAR-II$ value mathematically, this convergence-like behavior to a minimum may be explained by the fact that taking the random linear combination of the features vector components injects some amount of redundancy into the information contained in the feature vector itself and therefore $FAR-II$ performance of the scheme cannot be improved continuously by only increasing the dimensionality of the transformed feature vector, $k$.

This approach is scalable not only because of the fact that generating random matrices and polynomials is relatively a simple task, but also it is possible to generate and assign different output values for polynomial transformations while satisfying collision-free operation. In the proposed scheme it is possible to create new accounts at minimum cost (e.g. no need for pre-processing the data) as well as providing collision free operation. However, when the smartcard is stolen or duplicated, pre-processing (e.g., PCA) might improve the performance of the scheme (in terms of $EER$). However, as pointed out earlier, such operations are very likely to degrade the scalability of the system.

The security of the proposed scheme lies in the following factors. First, since the biometric data is transformed into a sequence of numbers by randomizing and passing them through the one-way polynomial transformation, need for template database is eliminated. These one-way transformations
make it possible to transform biometric feature values into a designated codevector in an error-tolerant way followed by cryptographic hashing to further improve the security. Correspondingly, for an attacker who has access to the database, determining the real values of the feature vector by looking at hashed values stored in the database will not be possible. Third, even though the information on the smartcard might be compromised, it still remains difficult for an attacker to guess the real values of the biometric data of the user by only analyzing the one-way transformation of that user as the polynomial transformations are non-invertible (Figure 2). It should be noted that, last cryptographic hashing step not only ensures the security of the user database but also eliminates the brute-force attacks with side information, e.g., when a user’s database information and smartcard are compromised together.

In this regard, a brute-force attack on the proposed scheme can be formulated as follows. Assume an attacker obtains the one-way transformations tailored for user \(i\) and the quantization step size \(\Delta\). The attacker by observing the one-to-many inverse transformations may guess possible intervals in the feature space over which user \(i\)’s biometric data might vary. The difficulty in correctly determining the range for each feature value can be expressed in terms of the number of possibilities as

\[
BF_i = \left( \prod_{j=1}^{\min(n,k)} \prod_{m=1}^{M_{i,j}} \gamma_{i,j}^m \right)
\]  

(10)

where \(\gamma_{i,j}^m\) is the number of possible feature vector ranges corresponding to the value \(o_{ij}\) (the index \(j\) stands for the feature vector components) in the region of whole feature space \(S_j\) as shown in Figure 5. Defining \(M_{i,j}\) as the maximum number of possible output values, i.e. \(o_{ij}\) values, which correspond to potential feature vector ranges can be approximated for a given polynomial \(P_{i,j}(x)\) as

\[
M_{i,j} = \left\lceil (\max_{x \in S_j} P_{i,j}(x) - \min_{x \in S_j} P_{i,j}(x)) / \Delta \right\rceil
\]

(11)
For example in Figure 6, it is easy to see that, $\gamma_{i,j}^m = 7$ for the designated $o_{ij}$ value. (It should be noted that since $o_{ij}$ values are quantized each quantized value will correspond to a range of feature vector values on the x-axis.) Similarly, $o_{ij} + \Delta$ and $o_{ij} - \Delta$ are two other possible output values with different number of possible corresponding feature vector ranges, which will be denoted as $\gamma_{i,j}^{m+1}$ and $\gamma_{i,j}^{m-1}$, respectively. In Equation 10, the reason for considering $\min(n,k)$ as the maximum bound for product is due to the fact that, even if $k$ is chosen to be greater than $n$, it is sufficient to consider only $n$ linearly independent equation to solve completely $k$ unknowns due to the rank deficiency of the random matrix. (This fact was already shown in previous section in more details.)

It should be noted that the above analysis is formulated based on the assumption that the attacker knows the quantization step size, $\Delta$. If $\Delta$ is determined globally and fixed to a specific value by making it only available to the trusted smartcard reader, the attacker has to also search over $\Delta$ values to perform brute-force attack. In this case, the complexity of the attack will be much higher.
To give an idea about the complexity of brute-force attack, which aims at determining some user’s biometric data completely, the number of possibilities that need to be considered by the attacker is approximately equal to $BF_i = ((4)^{10})^{20}/2 = 2^{399}$ when $n=20$, $M_{i,j}=10$ for all $j$, and $\gamma'_{i,j} = 4$ for all $m$.

Obviously, high values of $M_{i,j}$ and $n$ will ensure high complexity of brute-force attack. However, in order to have high $M_{i,j}$ value, degree of the polynomial, $d$, needs to be as high as possible and randomly generated points ($d$-2 points) used for polynomial construction should be generated by following an appropriate pattern such that, in addition to uniformly distributing these $d$-2 random points over x-axis, these points need to be generated in a manner such that two consecutive random points (in x dimension) yield values that are as far as possible from each other in the y-axis. As an example, some random points which have that kind of pattern are illustrated by “+” signs in Figure 3. Despite all these design considerations, still it is likely that some parts of the polynomials, that are poorly shaped, may be eliminated by the attacker, thereby reducing the complexity of the brute-force attack. Although it is not easy to quantify the amount of entropy loss due to analysis of the polynomial, the above discussed design considerations will limit the amount of information that can be deduced by the attacker.

6. CONCLUSION AND FUTURE WORK

We provided details of a secure biometric based authentication scheme which employs a user-dependant, robust, one-way transformation combined with a secure hashing algorithm. We discussed the performance improvement provided by random mapping idea which simply makes error-correction by using correlation of feature vector components. We also discussed the design issues such as scalability, collision-freeness and security and tested our scheme using ORL and E94 face databases and presented simulation results. Preliminary results show that, proposed scheme has a reasonable performance and offers a simple and practical solution to one of the privacy and security weakness of biometrics-based authentication systems namely, template security and privacy. Our future work focuses on devising
alternatives to random mapping and polynomial based one-way transformations and testing our approach with different types of biometric data on larger databases.
REFERENCES


