Cancelable Biometrics: A Review

Vishal M. Patel, *Member, IEEE,* Nalini K. Ratha, *Fellow, IEEE,* and Rama Chellappa, *Fellow, IEEE*

Abstract

Recent years have seen an exponential growth in the use of various biometric technologies for trusted automatic recognition of humans. With rapid adaptation of biometric systems, there is a growing concern that biometric technologies may compromise privacy and anonymity of individuals. Unlike credit cards and passwords, which can be revoked and reissued when compromised, biometrics are permanently associated with a user and cannot be replaced. In order to prevent the theft of biometric patterns, it is desired to modify them through revocable and non-invertible transformations to produce *Cancelable* biometric templates. In this paper, we provide an overview of various cancelable biometric schemes for biometric template protection. We discuss the merits and drawbacks of available cancelable biometric systems and identify promising avenues of research in this rapidly evolving field.

Index Terms

Biometrics, cancelable biometric templates, biohashing, salting, random projections, biometric template protection.

I. Introduction

Biometrics refers to the physiological or behavioral characteristics of an individual. Many physical characteristics, such as face, fingerprints and iris and behavioral characteristics such as voice, gait and keystroke dynamics, are believed to be unique to an individual. Hence, biometric analysis offers a reliable solution to the problem of identity verification. Recent developments in sensing and computing technologies have made biometric systems more affordable and as a result they are easily embedded in a

Vishal M. Patel is with the Center for Automation Research, UMIACS, University of Maryland, College Park, MD 20742 (e-mail: pvishalm@umd.edu).

Nalini K. Ratha is with IBM Watson Research Center, Hawthorne, NY 10532 USA (e-mail: ratha@us.ibm.com).

Rama Chellappa is with the Department of Electrical and Computer Engineering and the Center for Automation Research, UMIACS, University of Maryland, College Park, MD 20742 (e-mail: rama@umiacs.umd.edu).

variety of smart consumer devices such as mobile phones and tablets. Despite the widespread deployment of biometric systems in various applications, the use of biometrics raises several security and privacy concerns as outlined below [1].

1) *Biometrics is not secret*: The knowledge-based authentication methods totally rely on secrecy. For instance, passwords and cryptographic keys are known only to the user and hence secrecy can be maintained. In contrast, biometrics such as voice, face, signature and even fingerprints can be easily recorded and potentially misused without the user's consent. Face and voice biometrics are vulnerable to being captured without the user's explicit knowledge.
2) *Biometrics cannot be revoked or cancelled*: If a biometric can be presented by a human being who is one of the enrolled users, many biometrics security issues will be different. For example, biometric-based authentication systems will not have to deal with spoofed biometrics and also replay attacks on biometric systems. If a hacker gets access to the biometrics samples and has the ability to present it to the system at choice emulating a human presence, there will be no trust associated with the biometrics. In this scenario, we say that the biometrics has been compromised forever. Passwords, crypto-keys and PINs can be changed if compromised. When tokens such as credit cards and badges are stolen, they can be replaced. However, biometrics is permanently associated with the user and cannot be revoked or replaced if compromised.
3) *Cross application invariance and cross-matching*: It is highly encouraged to use different passwords and tokens in traditional authentication systems. However, biometrics-based authentication methods rely on the same biometrics. If a biometric template is exposed once, it is compromised forever. If a biometric template is compromised in one application, then the same method can be used to compromise all applications where the biometric is used. Furthermore, since the same biometrics is used across all applications and locations, the user can be potentially tracked if one or more organizations collude and share their respective biometric databases.
4) *Persistence*: While relative robustness over time is a boon for biometrics it can also be a big challenge from a privacy point of view when it needs to be changed. The uniqueness contained in them is still the same even though the signal as well the template can look different.

Regarding privacy violations, cross-matching and inability to revoke a biometric are two major issues. A simple approach would be to use standard encryption techniques such as hash functions or encryption to enhance the privacy. Hash functions have been used to protect biometric templates in which one way functions are used to compute a digest. Even though these functions are almost impossible to invert,

they produce significantly different digest even with minor changes in the input. In practice, all biometric templates change with environmental conditions. For instance, face and iris biometrics are significantly affected by illumination variations. Therefore, these functions can not be used directly in practice despite being theoretically very strong as they apply only to exact data. Furthermore, when data are encrypted, they need to be decrypted to carry out matching. This creates a possible attack point to get access to the decrypted templates.

In order to overcome the vulnerabilities of biometric systems, both biometrics and crypto research communities have addressed some of the challenges. Several biometric template protection schemes have been proposed in the literature [2], [3], [4], [5], [6], [7], [8]. In particular, *Cancelable biometrics* [3], [4], [5], [9] has gained a lot of interest in recent years. In this method, instead of storing the original biometric, it is transformed using a one way function. The transformation can be applied either in the original domain or in the feature domain. It was shown that this way of constructing biometric templates has the desired properties of cancelable biometric templates [3], [4], [5]. In particular, it provides revocability since a compromised biometric can be re-enrolled using another transformation. It preserves privacy since it is computationally difficult to recover the original biometric from a transformed one. It prevents cross-matching between databases since each application uses a different transformation. And it does not degrade the accuracy of a matching algorithm as the statistical characteristics of features are approximately maintained after transformation. This allows one to use existing matching algorithms.

There are also some closely related but not equivalent biometric template protection schemes based on *cryptosystems* [10] that have been studied extensively. These methods combine cryptographic keys with transformed versions of the original biometric templates to generate secure templates. In these methods, some public information, known as *helper data*, is generated. Depending on how the helper data is used, biometric cryptosystems can be broadly classified into *key binding* and *key generation* systems. In the key generation systems, both the helper data and the key are directly generated from the biometric templates, while in the key binding systems, the helper data are obtained by combining the key with the biometric template. Examples of key binding systems include fuzzy commitment [11] and fuzzy vault [6]. Key generation schemes based on secure sketches [7] have also been proposed in the literature. In the biometric cryptosystems, the level of security depends on the amount of information revealed by the helper data. Other methods for biometric template protection include distributed source coding [12] and fuzzy extractors [13]. A review of biometric cryptosystems can be found in [10], [8], and [14].

Our goal in this paper is to survey recent available approaches for designing cancelable biometric templates, discuss their advantages and limitations, and identify areas still open for exploration. Fur-

thermore, we will discuss possible ways of attacking cancelable biometric systems. Development of cancelable schemes for biometric template protection is crucial as biometric systems are beginning to proliferate into the core physical and information infrastructure of our dynamic society.

Rest of the paper is organized as follows. Section II reviews various recent cancelable biometric template protection methods. Attacks against cancelable biometric systems are discussed in Section III. Finally, Section IV concludes the paper with a brief summary and discussion.

II. Cancelable Biometric Templates

In this section, we review a number of recent strategies for generating cancelable biometric templates. In these methods, a function that is dependent on some parameter is used to generate protected biometric templates. The parameter of the function is used as the key. Figure 1 shows the basic concept of cancelable biometric template-based on non-invertible transformations.

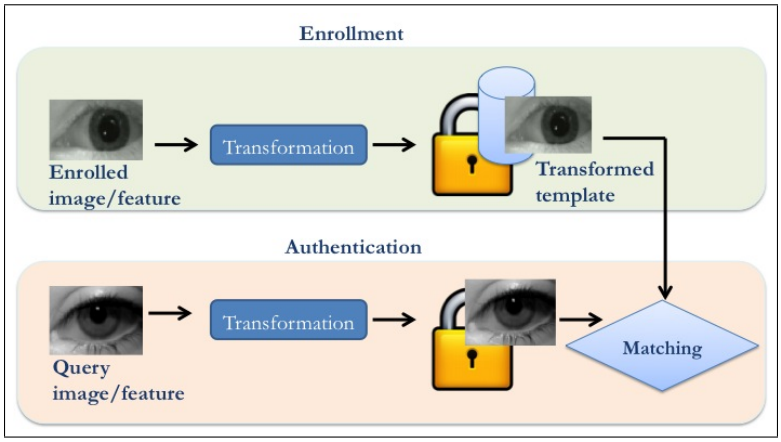
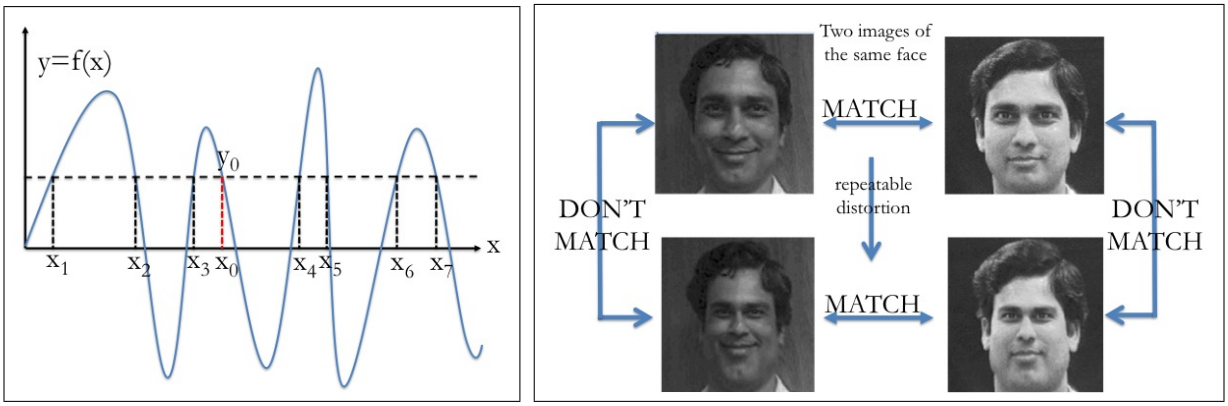


Fig. 1: Block diagram of a cancelable biometric system.

A. Non-invertible Geometric Transforms

One of the earliest methods for generating cancelable biometric templates was based on non-invertible geometric transformations. The idea is to morph the original biometric templates by applying signal domain or feature domain transformations [3], [4], [5]. Figures 2(a) and (b) show examples of these transformations applied in the signal domain and in the feature domain, respectively for face and fingerprint biometrics. Three different transformations were proposed for fingerprint biometric in [4], [5]. These transformations are the Cartesian transformation, the polar transformation and the functional

transformation. Prior to applying these transformations, the images are registered by first estimating the position and orientation of the singular points (core and delta) and expressing the minutiae positions and angles with respect to these points. Registration is an integral part of this method.



(a) (b)

Fig. 2: Illustration of non-linear transformation applied to face and fingerprint biometrics [4]. (a) Feature domain transformation for fingerprint biometrics. Each minutiae (feature) position is transformed using a non-invertible function $y = f(x)$. The minutiae position x_0 is mapped to $y_0 = f(x_0)$. If we know y_0, the inverse mapping is a many-to-one transformation. $x_1, x_2, x_3, x_4, x_5, x_6, x_7$ are all valid inverse mappings to y_0. (b) Illustration of cancelable biometrics for face recognition. The face is distorted in the original pixel (signal) domain prior to feature extraction. The distorted version does not match with the original face, while the two instances of distorted faces match among themselves.

For the cartesian transformation, the minutiae positions are measured in rectangular coordinates with reference to the position of the singular point by aligning the x-axis with its orientation. The coordinate system is divided into cells of fixed size. The transformation consists of changing the cell positions [4], [5]. Note that this transformation is not a simple permutation as the condition of irreversibility requires that cells are mapped to the same cell.

In the polar transformation method, the minutiae positions are measured in the polar coordinate with reference to the core position. The angles are measured with respect to the core orientation. As a result, the coordinate space is divided into polar regions. The non-invertible transform consists of changing the polar wedge positions. The minutiae angles also change with differences in the wedge positions before and after transformation [4], [5].

One of the limitations of both polar and Cartesian transformations is that they are unstable in the sense

that a small change in minutiae position in the original fingerprint can lead to a large change in minutiae position after transformation if the point crosses a sharp boundary [4]. As a result, various functions giving a locally smooth transformation of the minutiae positions were introduced in [4], [5]. The transformation is modeled using a vector valued function $\vec{F}(x,y)$ whose phase determines the direction of translation and the extent of translation is given by the magnitude $|\vec{F}|$ or alternately another vector valued function $\vec{G}(x,y)$. One such function proposed in [4], [5] is an electric potential field parameterized by a random distribution of charges. The magnitude and phase of this function are given by

$$|\vec{F}| = \left| \sum_{i=1}^{K} \frac{q_i(z-z_i)}{|(z-z_i)|^3} \right|,$$

$$\Phi(x,y) = \frac{1}{2} \arg \left(\sum_{i=1}^{K} \frac{q_i(z-z_i)}{|(z-z_i)|^3} \right),$$

where $z = x + iy$ is the position vector and the random key $K = [z_1, z_2, \cdots, z_K, q_1, q_2, \cdots, q_K]$ determines the position and magnitude of the charges. The transformation is given by

$$x' = x + K|\vec{G}(x,y)| + K\cos(\Phi_F(x,y))$$

$$y' = y + K|\vec{G}(x,y)| + K\sin(\Phi_F(x,y))$$

$$\theta' = \mod (\theta + \Phi_G(x,y) + \Phi_{rand}, 2\pi).$$

See [4] for more examples of various transformations and their analysis in terms of non-invertibility and attack strength. This method was later extended in [15] so that it does not require the registration of images. However, the approach in [15] exhibits lower verification rates than [4].

In a related work, [16] proposes a mesh warping-based approach for generating cancelable iris templates. In this method, the iris texture is re-mapped according to a distorted grid mesh laid over it. Distortions are specified by a key which offsets each vertex in the original mesh by some amount. Specifically, a regular grid is placed over the texture in which the vertices are then randomly displaced using the key as seed to a random number generator.

B. Random Projections

Another non-invertible transformation that is widely used for generating cancelable biometric templates is based on random projections [17], [18]. In these methods, the extracted feature $\mathbf{x} \in \mathbb{R}^N$ from a biometric is projected onto a random subspace $\mathbf{A} \in \mathbb{R}^{n \times N}$ with $n < N$. Here, each entry $a_{i,j}$ of $\mathbf{A}$ is an independent realization of a random variable. This process is described as follows

$$\mathbf{y} = \mathbf{A}\mathbf{x}, \tag{1}$$

where $\mathbf{y}$ is the n dimensional random projection vector. Since we are embedding N dimensional feature vectors in a space of a lower dimension n, for any biometric recognition to be effective, it is important that the relative distances between any two points in the feature space be preserved in the output random space. This is essentially characterized by the Johnson-Lindenstrauss (JL) lemma [19].

Lemma 1: For any $0 < \epsilon < 1$ and any integer p, let n be a positive integer such that $n \geq \frac{4\ln(p)}{\epsilon^2/2 - \epsilon^3/3}$. Then, for any set $\mathcal{S}$ of $p = |\mathcal{S}|$ data points in $\mathbb{R}^N$, there is a map $f : \mathbb{R}^N \to \mathbb{R}^n$ such that, for all $\mathbf{x}, \mathbf{y} \in \mathcal{S}$,

$$(1-\epsilon)\|\mathbf{x}-\mathbf{y}\|^2 \leq \|f(\mathbf{x}) - f(\mathbf{y})\|^2 \leq (1+\epsilon)\|\mathbf{x}-\mathbf{y}\|^2. \tag{2}$$

This lemma essentially states that, a set $\mathcal{S}$ of points in $\mathbb{R}^N$ can be embedded into a lower-dimensional Euclidean space $\mathbb{R}^n$ such that the pairwise distance of any two points is approximately maintained. In fact, it can be shown that f can be taken as a linear mapping represented by an $n \times N$ matrix $\mathbf{A}$ whose entries are randomly drawn from certain probability distributions [19]. This in turn implies that it is possible to change the original form of the data and still preserve its statistical characteristics useful for recognition.

In recent years, various improvements in the proof and the statement of the JL lemma have been made (see [20] and [21] for more details). In fact, it has been shown that given any set of points $\mathcal{S}$, the following are some of the matrices that will satisfy (2) with high probability, provided n satisfies the condition of the Lemma 1 [21]:

- $n \times N$ random matrix $\mathbf{A}$ whose entries $a_{i,j}$ are independent realizations of Gaussian random variables $a_{i,j} \sim \mathcal{N}(0, \frac{1}{n})$.
- Independent realizations of ± 1 Bernoullie random variables

$$a_{i,j} = \begin{cases} +\frac{1}{\sqrt{n}} & \text{with probability } \frac{1}{2} \\ -\frac{1}{\sqrt{n}} & \text{with probability } \frac{1}{2}. \end{cases}$$

- Independent realizations of related distributions such as

$$a_{i,j} = \begin{cases} +\sqrt{\frac{3}{n}} & \text{with probability } \frac{1}{6} \\ 0 & \text{with probability } \frac{2}{3} \\ -\sqrt{\frac{3}{n}} & \text{with probability } \frac{1}{6}. \end{cases}$$

A random projection-based cancelable biometric method for iris recognition was proposed in [17]. Applying the random projections directly on the iris images usually degrades the performance due to the following reasons. First of all in real iris images, despite good segmentation algorithms, there will

still be some outliers due to specular reflections, eye lashes and eyelids. Also, different parts of the iris have different quality. By taking a linear transformation of the entire vector, one combines the good iris regions as well as the outliers and thereby corrupts the data. To deal with this, [17] proposes Sectored Random Projections (SRP) in which random projections are applied separately on each sector and the resulting transformed vectors are concatenated to form the cancelable template. As a result, outliers can corrupt only the corresponding sector and not the entire iris vector.

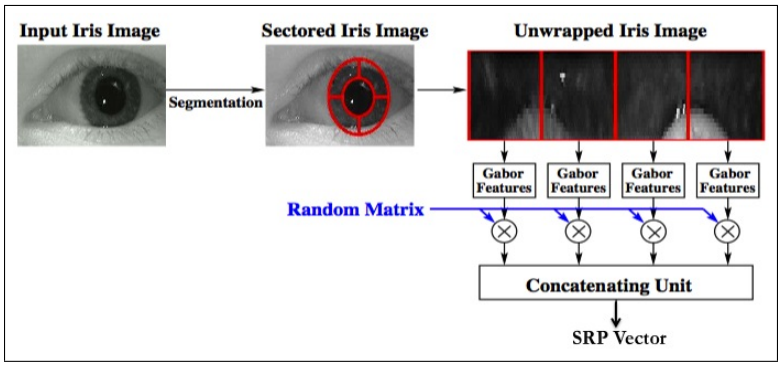


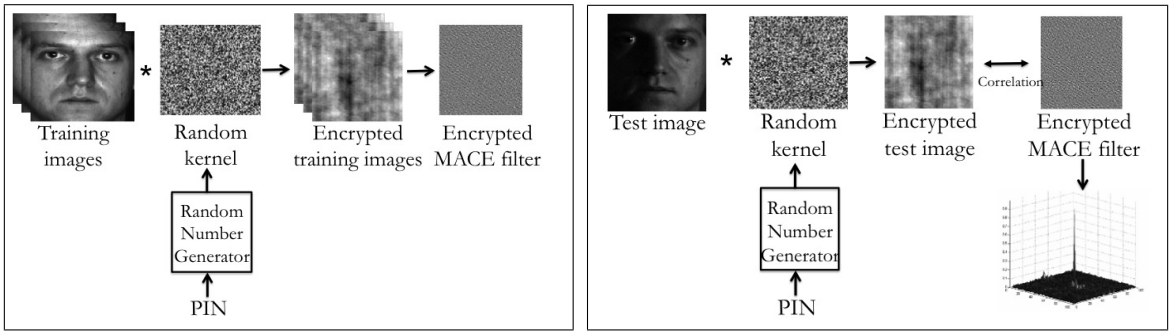
Fig. 3: An overview of the SRP method [17].

Figure 3 shows an overview of this method [17]. The enrollment system extracts the iris pattern of the user, computes the Gabor features, applies a different random projection for each application and transfers the new pattern to the application database. Note that even if the transformed pattern and the key (i.e. the projection matrix) are stolen, the user's iris pattern cannot be generated from them due to the dimension reduction caused by the projection. Also even if a hacker steals the user's iris pattern either from the client system or using a hidden scanner, without knowing the random projection he/she cannot generate the transformed patterns required by the application. During the verification stage, the application obtains the iris image and the random projection matrix from the user, computes the transformed pattern and compares it with the ones in its database. In case, the random projection matrix or the transformed patterns are compromised, one can create a new random projection matrix and obtain a new transformed pattern which can be updated into the application database. Instead of the user providing the random matrix during verification, the application can generate and store it along with the cancelable template in its database. Though this will be an easier scheme for the user to operate, it is less secure as a hacker can get both the random projection matrices and the transformed patterns by breaking into the application database.

The approach of SRP [17] was later extended in [18] using sparse representation-based classification. It was shown that the sparsity patterns that one obtains before and after applying random projections are similar. As a result, cancelable biometric templates can be directly used for authentication rather than the original ones without degrading the performance of a sparse representation-based classification algorithm.

C. Cancelable Biometric Filters

Motivated by the success of the correlation filter-based methods in pattern recognition and computer vision applications [22], a random convolution method for generating cancelable biometric templates was proposed in [23]. The idea is to encrypt biometric templates using random user specific convolution kernels. The training images are convolved with a random convolution kernel. The seed used to generate the random convolution kernel is used as the PIN. The convolved training images are then used to generate a Minimum Average Correlation Energy (MACE) biometric filter. This encrypted filter is stored and used for authentication. Figure 4(a) shows the enrollment stage using this method.



(a) (b)

Fig. 4: Correlation filter-based approach to cancelable biometrics [23]. (a) Enrollment stage for encrypted filters. (b) Authentication stage using encrypted MACE filters.

During the recognition stage, the user presents the PIN and the encrypted filter which is used to generate the convolution kernel. This random convolution kernel is convolved with the test face images presented by the user. The convolved test images are cross-correlated with the encrypted MACE filter and the resulting correlation outputs are used to authenticate the user. Figure 4(b) shows authentication stage for this method.

It was shown that convolving the training images with any random convolution kernel prior to building the MACE filters used for biometric recognition does not change the resulting correlation output [23].

As a result, the recognition accuracy is maintained. Furthermore, different cancelable biometric templates can be generated from the same biometric by simply changing the convolution kernels.

Other correlation-based cancelable biometric methods include correlation invariant random filtering (CIRF) [24], [25] which was shown to have almost the same accuracy as the conventional fingerprint verification based on the chip matching algorithm.

D. BioConvolving

Another convolution-based approach for generating cancelable biometric templates was recently proposed in [26]. This method is applicable to any biometric whose template can be represented by a set of sequences. In this method, each transformed sequence $f_{(i)}[n], i = 1, \cdots, F$, is obtained from the corresponding original sequence $r_{(i)}[n], i = 1, \cdots, F$, which represents a generic discrete sequence of length N belonging to the original biometric template. In particular, a number $(W-1)$ of different integer values d_j between 1 and 99 are randomly selected, ordered in ascending order such that $d_j > d_{j-1}, j = 1, \cdots, W,$. These numbers are arranged in a vector $\mathbf{d} = [d_0, \cdots, d_W]^T$, where d_0 and d_W are set to 0 and 100, respectively. Here, the vector $\mathbf{d}$ represents the key of the transformation. The original sequence $r_{(i)}[n]$ is divided into W non-overlapping segments $r_{(i)j,N_j}[n]$ of length $N_j = b_j - b_{j-1}$

$$r_{(i)j,N_j}[n] = r_{(i)}[n + b_{j-1}], \quad n = 1, \cdots, N_j, \;\; j = 1, \cdots, W, \tag{3}$$

where

$$b_j = \left\lceil \frac{d_j}{100} N \right\rceil, \quad j = 1, \cdots, W. \tag{4}$$

A transformed sequence $f_{(i)}[n], n = 1, \cdots, K$, is then obtained through the linear convolution of the sequences $r_{(i)j,N_j}[n], j = 1, \cdots, W$ as

$$f_{(i)}[n] = r_{(i)1,N_1}[n] * \cdots * r_{(i)W,N_W}[n]. \tag{5}$$

Each original sequence $r_{(i)}[n], i = 1, \cdots, F$ undergoes the same decomposition before applying convolutions. As a result, the length of the transformed sequences is equal to $K = N - W + 1$. A normalization is applied to make the transformed sequences zero mean and unit standard deviation. Different templates can be generated from the original biometric template by simply changing the size or the values of the parameter key $\mathbf{d}$. Figure 5 shows an example of a feature transformation where $W = 3$ [26]. See [26] for more details on different ways of generating transformed sequences, invertibility analysis and their application in signature-based authentication.

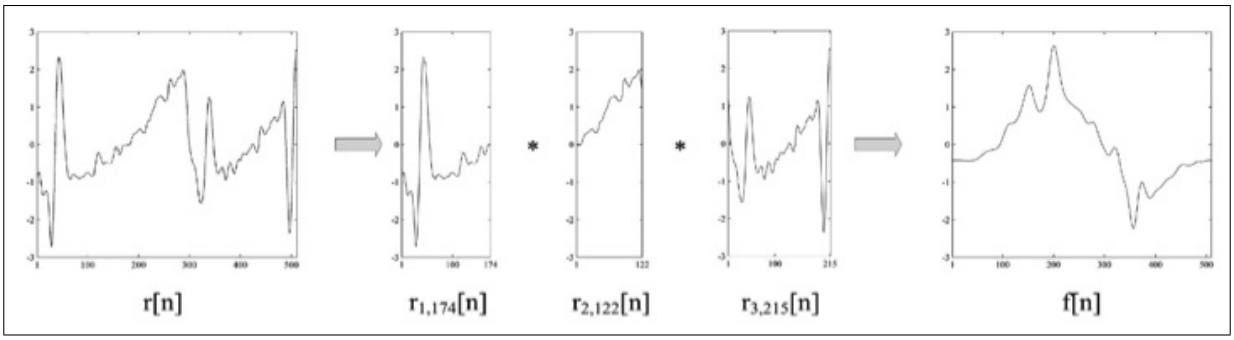


Fig. 5: Sequence transformation using the BioConvolving approach [26], where $W = 3$.

E. Bloom Filters

Recently, Bloom filter-based cancelable biometric template protection schemes were proposed in [27], [28], [29]. A Bloom filter is essentially a space-efficient probabilistic data structure representing a set in order to support membership queries. In particular, alignment-free cancelable iris biometric templates based on adaptive Bloom filters were introduced in [27] in which the generic adaptive Bloom filter-based transform is applied to binary feature vectors of different iris recognition algorithms. It was shown that such a method can enable template protection, compression of biometric data, and computationally efficient biometric identification. Furthermore, rotation-invariant Bloom filter-based transform can provide a high level of security while maintaining recognition accuracy [27].

F. Knowledge Signatures

Voice-based cancelable biometric templates using knowledge signatures were proposed in [30]. The idea is based on a group signature scheme which allows members of a group to sign messages on the group's behalf such that the resulting signature does not reveal their identity. They consider voiceprint as the knowledge of the user and the user's voiceprint transmitted to the template which isn't the original feature, but a signature of knowledge. Legitimate signatures can not be generated without factorizing a large integer and the original feature. As a result, an individual's privacy can be protected. We refer readers to [31] and [30] for more details on knowledge signatures and their uses in generating cancelable biometric templates for voiceprints.

G. BioHashing Methods

BioHashing methods are essentially an extension of random projection. In BioHashing [9], [32], [33], [34], [35], [36], [37], [38] feature extraction method such as wavelet transform is first used to extract

the biometric feature $\mathbf{x} \in \mathbb{R}^N$ from the input biometric data. Using a user specific Tokenized Random Numbers (TRN), n orthogonal pseudo-random vectors, $\mathbf{b}_i \in \mathbb{R}^N, i = 1, \cdots, n$, are generated, where $n \leq N$. Then, the dot product of the feature vector and all the random vectors is calculated. Finally, a binary discretization is applied to compute n bit BioHash template as

$$\mathbf{c} = \text{Sig}\left(\sum_i \mathbf{x}\mathbf{b}_i - \tau\right), \tag{6}$$

where $\text{Sig}(\cdot)$ is defined as a signum function and τ is an empirically determined threshold. Eq. (6) only applies to a user who holds the user-specific random vectors $\mathbf{b}_i \in \mathbb{R}^N, i = 1, \cdots, n$, and thus the formulation can be extended to introduce an ensemble of random subspaces, where each subspace represents different individual k. The resulting BioHash is given as

$$\mathbf{c}^k = \text{Sig}\left(\sum_i \mathbf{x}^k \mathbf{b}_i^k - \tau\right), \quad k = 1, \cdots, g, \tag{7}$$

where g is the total number of users in the system. Finally, the BioHash code is compared by the Hamming distance for the similarity matching. Figure 6 shows the progression of BioHshing [33]. The BioHashing framework is demonstrated to be a one-way transform, hence providing a high degree of security to the biometric and external factors. A detailed statistical analysis of the BioHashing framework in terms of random multispace quantization operations can be found in [9].

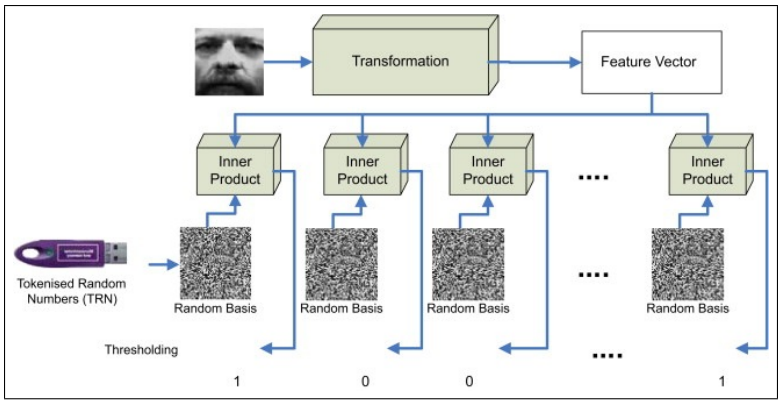


Fig. 6: Overview of BioHashing [33].

H. Random Permutations

Another common approach for generating cancelable biometric templates is based on random permutation of features. In [39], two such methods were proposed for generating cancelable iris templates. The

first method, namely GRAY-COMBO, transforms the Gabor features by circularly shifting and adding rows at random. BIN-COMBO, the second method, applies similar transformations on the iris codes by random shifting and XOR-ing. As pointed out by the authors, these methods gradually reduce the amount of information available for recognition. Since these methods employ linear transformations on the Gabor feature vectors, they are also sensitive to outliers in the form of eyelids, eye lashes and specular reflections. [18] proposes to overcome this limitation by dividing the feature into different regions and permuting them randomly in a dictionary. Without prior knowledge of the locations of sectored features in a dictionary, it is impossible to perform recognition. A similar approach was also proposed in [16] where each block of the target texture is mapped to a block from the source texture. In this method, a re-mapping of blocks instead of a permutation is performed, as it is not reversible. Source blocks which are not part of the mapping are not contained in the transformed texture. As a result, it is impossible to reconstruct the original iris texture. Another permutation-based cancelable method for fingerprint biometric was presented in [40]. This method permutes a binary vector obtained from fingerprint features and stores them in the database. During authentication, the binary vector obtained from the fingerprints of the user are permuted using the key provided by the user and matched with the database.

In these methods, key security is essential for protecting privacy of individuals. One of the advantages of these methods is that since permutations are merely rearranging the feature vector, authentication accuracy is not affected by these operations.

I. Salting Methods

One of the simplest ways of generating cancelable biometric templates is by simply mixing in a totally artificial pattern. The mixing patterns can be pure random noise, a random pattern or a synthetic pattern. Two such *salting* methods were proposed in [39] for iris recognition namely GRAY-SALT and BIN-SALT. These methods add random patterns or synthetic iris patterns to the Gabor features and iris codes, respectively. Unlike GRAY-COMBO and BIN-COMBO permutation-based methods, they do not suffer from the problem of outlier amplification and reduction of useful area. However, it is difficult to decide the relative strength of the noise patterns to be added. Adding very strong patterns will reduce the discriminative capacity of the original iris patterns and hence lead to lower recognition results. Adding weaker patterns can lower the non-invertibility property, making it easier to extract useful information about the original iris biometric from the transformed patterns. Also, if the added patterns are compromised, the original iris patterns could be extracted from the transformed patterns by a simple subtraction operation.

J. Hybrid Methods

Several biometric template protection approaches make use of both cryptosystems and cancelable biometrics [41], [42]. One such *hybrid* system was proposed in [41] for face biometric. They introduced *biotoken* which is "the revocable identity token produced by applying a revocable transform to biometric data, such that identity matching is done in the encoded/revocable form" [41], [42]. Specifically, this approach combines the ideas of transformation of data, robust learning measures and encryption of biometric data. The method essentially separates the data into two parts, the fractional part which is retained for local distance computation and the integer part which is encrypted. It was shown that for face biometric this method significantly improved the performance of the PCA and LDA algorithms. This work was later extended for fingerprints in [42].

K. Summary of Cancelable Biometric Template Protection Schemes

The cancelable biometric template protection schemes reviewed in this paper can be broadly divided into two main categories as shown in Figure 7 - methods that require a special matcher and methods that can work with the existing matchers. These schemes can be further classified into two categories, namely, registration free methods and methods that require good registration of biometric samples. Finally, these methods can be further divided into two types of schemes - schemes that work with the original biometric samples (denoted as signal) and schemes that work with the features extracted from the biometric signals (denoted as feature).

Among the methods that require a special matcher and good registration of biometric samples, Biotokens [41], [42] is a signal-based method and BioConvolving [26], salting, PalmHashing [37] and PalmPhasor [37] methods are feature-based methods. On the other hand, correlation-based MACE filter approach [23] is a signal-based, registration-free method that requires a special matcher. Combo [39], block-remapping [16], image warping [16], non-invertible transforms [4] and dynamic RP [43] methods fall under signal-based methods that require registration and can work with the existing matchers. Whereas permutations [18], RP [17], BioHashing [35], [9] and PalmHashing [34] methods are feature-based that can work with the existing matchers and require good registration. Registration-free methods that can work with existing matchers include minimum distance graph [44] and curtailed circular convolution [45] methods which are signal-based and a registration free approach proposed in [15] which is a feature-based method.

Furthermore, Table I summarizes key cancelable biometric template protection approaches in terms of their performances on various biometric datasets. Note that the performances of different methods are

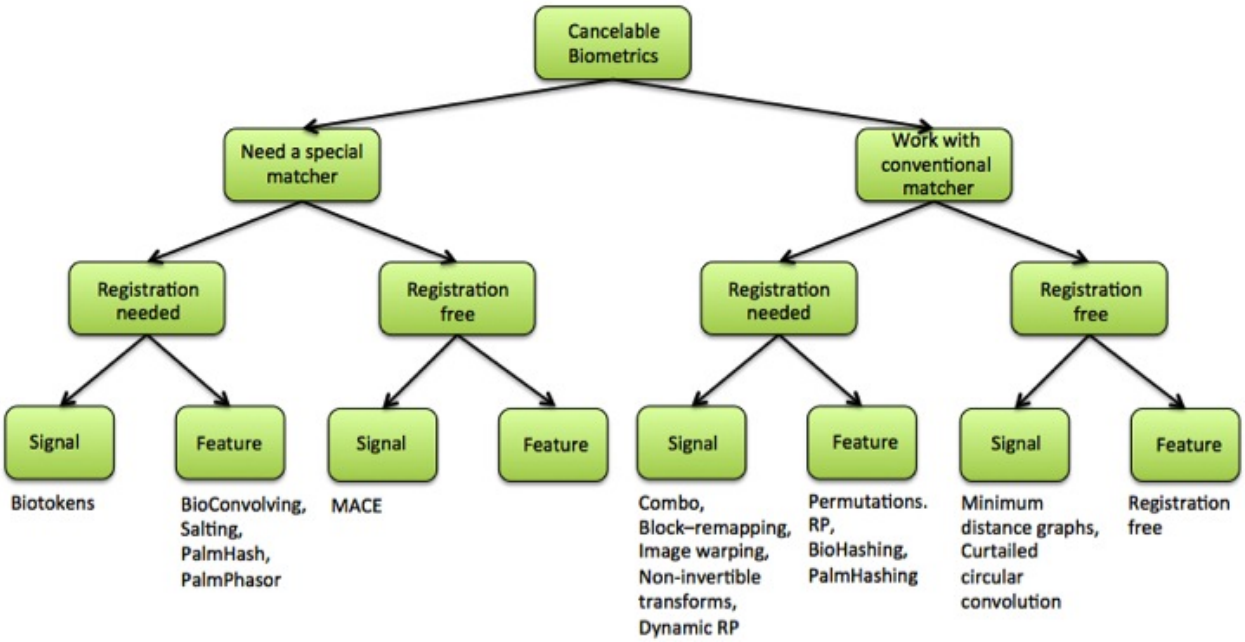


Fig. 7: Categorization of cancelable biometric template protection schemes.

reported in terms of False Rejection Rate (FRR), Equal Error Rate (EER), rank-1 Recognition Rate (RR), Genuine Accept Rate (GAR), and False Acceptance Rate (FAR).

TABLE I: Key cancelable biometric template protection schemes.

Method	Biometric	Dataset (Subjects)	Performance	Remarks
Non-invertible transforms [4]	Fingerprint	IBM-99 (188)	FRR: $\sim$ 35, 15, 15	-
Image warping [16]	Iris	CASIA Iris V3 (396)	EER: 1.6 - 6	-
Random projections [17]	Iris	MMU1 dataset (100)	RR: 97.7	-
Biometric filters [23]	Face	CMU PIE (65)	RR: 100	-
BioConvolving [26]	Online signature	MCYT (330)	EER: 6.33 - 15.40	-
BioHashing [35]	Fingerprint	FVC 2002 (100)	EER: $\sim$ 0	FAR: 0
PalmHashing [34]	Palmprint	Palmprint dataset (50)	EER: 0-0.222	FAR: 0
BioHashing [9]	Face	FERET (1196)	EER: 0.002 - 7.51	-
GRAY-COMBO [39]	Iris	MMU1 dataset (100)	GAR: $\sim$ 0.995	FAR : 10^{-4}
BIN-COMBO [39]	Iris	MMU1 dataset (100)	GAR: $\sim$ 0.965	FAR : 10^{-4}
Block re-mapping [16]	Iris	CASIA Iris V3 (396)	EER: 0.2 - 1.6	-
GRAY-SALT [39]	Iris	MMU1 dataset (100)	GAR: $\sim$ 1	FAR : 10^{-4}
BIN-SALT [39]	Iris	MMU1 dataset (100)	GAR: $\sim$ 0.995	FAR : 10^{-4}
Atom permutations [18]	Iris	ND-IRIS-0405 (356)	RR: 99.17	-
Biotokens [42]	Fingerprint	FCV 2000-4 (100)	EER: 0.012-0.086	Hybrid method
Biotokens [41]	Face	FERET (1196)	EER: 0.9997	Hybrid method
Dynamic random projections [43]	Fingerprint	FVC2002DB2-A (800)	EER: ~ 0.05	-
PalmHash code [37]	Palmprint	PolyU dataset (7752)	EER: 0.38	2D PalmHash code
PalmPhasor code [37]	Palmprint	PolyU dataset (7752)	EER: 0.32	2D PalmPhasor code
Minimum Distance Graph [44]	Fingerprint	FVC2002-DB1a,b (100)	EER: 0.0227	-
Curtailed circular convolution [45]	Fingerprint	FVC2002-DB1,2,3 (100)	EER: 0.02, 0.03, 0.0612	-

III. Attacks against Cancelable Biometric Templates

A generic biometric system consists of a sensor, a feature extraction module, a biometric template database, a matcher module, and an application device which is driven by the matcher's response. Researchers have identified different points of attacks in a biometric system as shown in Figure 8. The attacks can come in various forms such as: trojan horse attack, front end attack, phishing and farming attacks, back end attack and communication channel attack. The unauthorized access to raw biometric templates is among the most serious threats to users' privacy and security. Some of the attacks can be averted using cancelable biometric systems while some of them are extremely difficult to detect. See [46] for more details on different types of attacks.

The cancelable biometric systems can be attacked by exposing the parameter (key) of the transformation

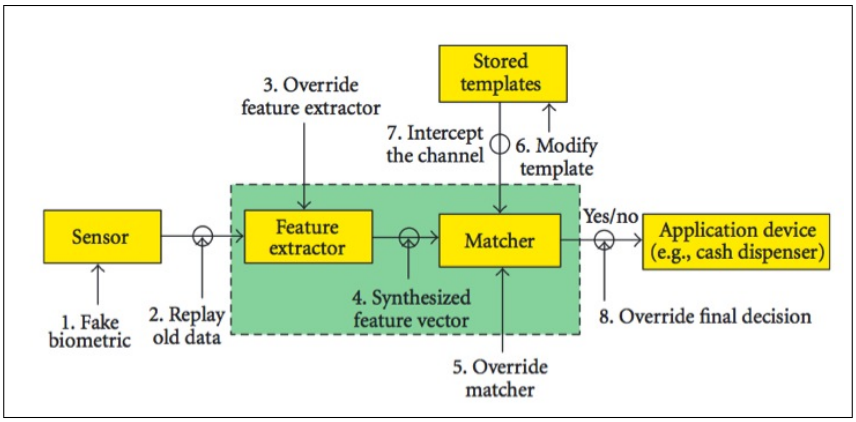


Fig. 8: Possible attack points in a generic biometric system [46], [8].

being applied to biometric templates. In the case when the transformation is invertible, the original biometric can be reconstructed. In this case, security is in the secrecy of the key. If the transformation is not invertible, then an attacker can try to approximately recover the original biometric templates. For instance, it was shown in [47], [48], [49] that face images can be restored from encrypted templates. Attacks against the cancelable system using non-invertible transforms [4] are proposed in [50]. It was argued that when multiple transformed templates are generated from the same original template, they can be cracked by a method known as Attack via Record Multiplicity. In particular, given a transformed template, an attacker can find the inverse solutions by inverting the transformation. Due to many-to-one property of transform functions, there may be several solutions out of which is the original solution. The attacker can come up with a way to to pick out the right solution. A similar dictionary attack method is also proposed in [51] to recover the original templates from the cancelable templates. Also, convolution-based cancelable biometric systems' [26], [23] security depends on how well blind deconvolution algorithms are able to recover the original biometric templates.

Several vulnerabilities in BioHashing-based systems have also been investigated [52], [53], [54], [55]. One of the major limitations of BioHashing methods is their low performance when attackers are in possession of secret key. To deal with this problem, [52] proposed an improved BioHashing method which is more robust than the original BioHashing method [32], [33]. In [53], it was shown that even without having a genuine users' private random vectors, a preimage of a BioCode can be easily calculated from a lost BioCode. As a result, an attacker can gain an illegal access to a system. It was observed that simple data dimension reduction and discretization as is done in most BioHashing methods may be vulnerable to preimage attacks. Similarly, a new way to approximate the original biometric feature

from the transformed template in a cancelable biometric scheme was recently proposed in [54]. Their method is based on a genetic algorithm which essentially determines the optimal value of a criterion by simulating the evolution of a population and survival of best fitted individuals [54]. It was shown that a genetic algorithm can allow an intruder to recover a biometric template, similar to the original template, under some realistic assumptions.

In a related work, [43] analyzed the security concerns over random projection-based cancelable systems [49], [56] and proposed a dynamic random projection method to alleviate these concerns by forming a non-linear projection process which relates the random matrix's assembly to the biometric feature vector itself. The dynamic random projection method greatly increases the computational complexity to apply inversion attacks in the token stolen cases. Furthermore, it was shown that this method does not degrade the biometric performance compared with the fixed matrix-based random projection [43].

In recent years, several biometrics protection schemes have been proposed in the literature that attempt to protect the privacy of biometric templates without using a key [57], [58], [59], [60]. For instance, a visual cryptography method is introduced in [58] which decomposes a biometric image into two noise-like images, called sheets, that are stored in two different databases. During the authentication, the two sheets are overlaid to create a temporary image for matching. One of the limitations of this method is that it requires two separate databases to work together, which may not be practical in some applications. Another method for protecting fingerprint biometric combines two fingerprints from two different fingers to generate a new template [57]. For authentication, two query fingerprints are required and a two-stage matching process is proposed for matching the two query fingerprints against a combined template. One of the advantages of this method is that by using the combined template, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen [57].

In order to deploy a biometric template protection system, one needs to investigate the security strength of the template transformation technique and define metrics that facilitate security evaluation. Towards this end, six different evaluation metrics were defined in [49]. Furthermore, the security of BioHashing and cancelable fingerprint templates were analyzed based on these metrics. It was reported that both these schemes are vulnerable to intrusion and linkage attacks because it is relatively easy to obtain either an approximation of the original biometric template in the case of BioHashing or a preimage of the transformed template in the case of cancelable fingerprints.

In a related work, [61] presents several evaluation criteria, metrics and testing methodologies for assessing biometric template protection algorithms. In particular, criteria such as accuracy of the recognition algorithm, throughput, storage requirements, performance degradation of a biometric template protection

scheme, diversity and error rate of failing to generate a protected template are discussed in detail. These definitions will help researchers in designing robust biometric template protection schemes.

IV. Conclusions and Future Directions

Often we use standard information security tools such as encryption or secure hashing methods to protect the biometric content. There are two issues with this approach. First, as the biometrics data (image, template) constantly change with every sample acquisition, the encrypted biometrics has to be decrypted for matching. If it is decrypted, that opens an opportunity for the hacker to attack at the output point of the decryption. If a secure hash function is used, the matching of the secure hashes is totally useless as biometrics signals never reproduce exactly. While the hash will be best in terms of privacy, the biometrics matching will not ever produce the positive authentication result. Cancelable biometrics is inspired by this approach but handles biometric variability. The transformation management in cancelable biometrics is equivalent to key management in information security. For example, a part of the transform can be retained by the user, another part can stay with the authentication system. Until the two come together, the biometrics authentication can't take place. But the keys in encryption or hash functions are derived totally differently than the cancelable biometrics transform. Secondly, because of the special construction, the matching of the cancelable biometrics signal or template is carried out in the transformed domain. In fact, the original biometrics signal is not required to be retained as both enrollment and authentication is carried out using the transformed biometrics.

This article presented a review of recent developments in such template protection schemes which included non-invertible transform-based methods, BioHashing and hybrid methods. There are several challenges to be overcome before successfully designing a cancelable biometric system. Below we list a few.

1) In order for the transform to be repeatable, the biometric signal must be positioned in the same coordinate system each time. This requires that an absolute registration be done for each biometric signal acquired prior to the transformation. Registration-free cancelable biometric systems have also been proposed in the literature [15], [44], [62], [45]. However, some of these methods do not perform well in practice. For instance, a registration-free construction of cancelable fingerprint biometric templates [15] exhibits lower verification performances than the one proposed in [4] which requires registration. More robust registration free non-invertible transform and BioHashing methods are needed.

2) The recently introduced theory of compressive sampling allows one to reconstruct the original signal from a few random measurements provided that certain conditions are met. Many cancelable biometric template protection systems make use of random projections [17], [18], [32], [33]. It remains an interesting problem to study the vulnerability of such cancelable systems using compressive sampling.
3) In the past few years, we have witnessed an exponential growth in the use of mobile devices such as smartphones and tablets. Most mobile devices use passwords, pin numbers, or secret patterns for authenticating users. As long as the device remains active, there is no mechanism to verify that the user originally authenticated is still the user in control of the device. As a result, unauthorized individuals may improperly gain access to personal information of the user if the password is compromised. Active authentication systems deal with this issue by continuously monitoring the user identity after the initial access has been granted. Examples include systems based on screen touch gestures [63], gait recognition [64], and device movement patterns (as measured by the accelerometer) [65]. Development of cancelable active authentication systems is a nascent area of research.
4) Blind deconvolution is an extremely ill-posed problem in which one attempts to recover the original signal from convolved outputs without the explicit knowledge of the convolution kernel. Recent advances in signal processing community have shown that one can approximate the convolution kernel directly from the observations. These methods exploit some underlying structure of signals such as sparsity. It remains to be seen whether convolution-based cancelable systems are robust to these blind deconvolution methods.
5) Most cancelable biometric template protection schemes have been evaluated on small and mid-size datasets consisting of hundreds and thousands of samples. However, in order to really see the significance and impact of various biometric template protection schemes, they need to be evaluated on large-scale datasets containing millions of samples.
6) As the research community advances biometric template protection schemes, third party evaluation for security attacks and evaluation of the revocable methods are needed. Some efforts are being made [66], however, more standardization efforts are needed to establish guidelines and procedures for testing and evaluating various cancelable biometric systems.

AUTHOR BIOGRAPHIES

Vishal M. Patel (Ph.D., UMD, 2010) is a member of the research faculty at the University of Maryland Institute for Advanced Computer Studies (UMIACS). His research interests are in signal processing, computer vision and machine learning with applications to biometrics and object recognition. Dr. Patel was a recipient of the ORAU postdoctoral fellowship in 2010. He is a member of the IEEE, Eta Kappa Nu, Pi Mu Epsilon, and Phi Beta Kappa.

Nalini K. Ratha (Ph.D., MSU 1996) is a Research Staff Member at the IBM Thomas J. Watson Research Center, Yorktown Heights, New York where he leads the biometrics research efforts in building efficient biometrics systems. In addition to more than 80 publication in peer reviewed journals and conferences, and co-inventor on 12 patents, he has co-edited two books on biometrics recognition. He is a Fellow of IEEE, Fellow of IAPR and Senior Member of ACM. His current research interests include biometrics, computer vision, pattern recognition and special purpose architecture for computer vision systems.

Rama Chellappa (Ph.D., Purdue, 1981) is a Professor and Chair of Electrical and Computer Engineering (ECE) and an affiliate Professor of Computer Science at the University of Maryland (UMD), College Park. He is also affiliated with the Center for Automation Research, the Institute for Advanced Computer Studies (Permanent Member) and a Minta Martin Professor of Engineering. He is a Fellow of IEEE, IAPR, OSA, AAAS, ACM and AAAI. His current research interests are clustering, 3D modeling from video, image and video-based recognition of objects, dictionary-based inference, and domain adaptation.

REFERENCES

[1] N. K. Ratha, "Privacy protection in high security biometrics applications," in *Ethics and Policy of Biometrics*, ser. Lecture Notes in Computer Science, A. Kumar and D. Zhang, Eds. Springer Berlin Heidelberg, 2010, vol. 6005, pp. 62–69.

[2] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," *IEEE Symposium on Security and Privacy*, pp. 148–157, May 1998.

[3] N. K. Ratha, J. H. Connel, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[4] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561 –572, April 2007.

[5] R. M. Bolle, J. H. Connel, and N. K. Ratha, "Biometrics perils and patches," *Pattern Recognition*, vol. 35, no. 12, pp. 2727–2738, 2002.

[6] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237–257, Feb. 2006.

[7] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 503–512, Sept 2007.

[8] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, pp. 113:1–113:17, Jan 2008.

[9] A. Teoh, A. Goh, and D. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1892–1901, Dec. 2006.

[10] U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, June 2004.

[11] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *ACM Conference on Computer and Communications Security*. New York, NY, USA: ACM, 1999, pp. 28–36.

[12] S. Draper, A. Khisti, E. Martinian, A. Vetro, and J. S. Yedidia, "Using distributed source coding to secure fingerprint biometrics," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 2, April 2007, pp. II–129–II–132.

[13] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Advances in cryptology-Eurocrypt 2004*. Springer Berlin Heidelberg, 2004, pp. 523–540.

[14] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 3, pp. 1–25, 2011.

[15] S. Chikkerur, N. Ratha, J. Connell, and R. Bolle, "Generating registration-free cancelable fingerprint templates," in *IEEE International Conference on Biometrics: Theory, Applications and Systems*, Sept 2008, pp. 1–6.

[16] J. Hmmerle-Uhl, E. Pschernig, and A. Uhl, "Cancelable iris biometrics using block re-mapping and image warping," in *Information Security*, ser. Lecture Notes in Computer Science, P. Samarati, M. Yung, F. Martinelli, and C. Ardagna, Eds. Springer Berlin Heidelberg, 2009, vol. 5735, pp. 135–142.

[17] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Sectored random projections for cancelable iris biometrics," in *IEEE International Conference on Acoustics Speech and Signal Processing*, March 2010, pp. 1838–1841.

[18] ——, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 30, no. 9, pp. 1877–1893, Sept. 2011.

[19] W. Johnson and J. Lindenstrauss, "Extensions of lipschitz maps into a hilbert space," in *Contemporary Mathematics*, 1984, pp. 189–206.

[20] S. Dasgupta and A. Gupta, "An elementary proof of a theorem of johnson and lindenstrauss," *Random Structures & Algorithms*, vol. 22, no. 1, pp. 60–65, Jan 2003.

[21] D. Achlioptas, "Database-friendly random projections: Johnson-lindenstrauss with binary coins," *Journal of Computer and System Sciences*, vol. 66, no. 4, pp. 671–687, Jun 2003.

[22] B. V. K. V. Kumar, A. Mahalanobis, and R. D. Juday, *Correlation Pattern Recognition*. Cambridge University Press, 2005.

[23] M. Savvides, B. Kumar, and P. Khosla, "Cancelable biometric filters for face recognition," in *International Conference on Pattern Recognition*, vol. 3, Aug 2004, pp. 922–925 Vol.3.

[24] K. Takahashi and S. Hirata, "Cancelable biometrics with provable security and its application to fingerprint verification," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 94-A, no. 1, pp. 233–244, 2011.

[25] S. Hirata and K. Takahashi, "Cancelable biometrics with perfect secrecy for correlation-based matching," in *Advances in Biometrics*, ser. Lecture Notes in Computer Science, M. Tistarelli and M. Nixon, Eds. Springer Berlin Heidelberg, 2009, vol. 5558, pp. 868–878.

[26] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable templates for sequence-based biometrics with application to on-line signature recognition," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 40, no. 3, pp. 525–538, May 2010.

[27] C. Rathgeb, F. Breitinger, C. Busch, and H. Baier, "On the application of bloom filters to iris biometrics," *IET Journal on Biometrics*, vol. 3, no. 4, pp. 207–218, 2014.

[28] C. Rathgeb and C. Busch, "Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters," *Computers & Security*, vol. 42, no. 0, pp. 1 – 12, 2014.

[29] C. Rathgeb, F. Breitinger, and C. Busch, "Alignment-free cancelable iris biometric templates based on adaptive bloom filters," in *IAPR International Conference on Biometrics*, June 2013, pp. 1–8.

[30] W. Xu, Q. He, Y. Li, and T. Li, "Cancelable voiceprint templates based on knowledge signatures," in *International Symposium on Electronic Commerce and Security*, Aug 2008, pp. 412–415.

[31] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," in *International Cryptology Conference on Advances in Cryptology*. London, UK, UK: Springer-Verlag, 1997, pp. 410–424.

[32] A. B. J. Teoh and C. T. Yuang, "Cancelable biometrics realization with multispace random projections," *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, vol. 37, no. 5, pp. 1096–1106, 2007.

[33] A. B. Teoh, Y. W. Kuan, and S. Lee, "Cancellable biometrics and annotations on biohash," *Pattern Recognition*, vol. 41, no. 6, pp. 2034 – 2044, 2008.

[34] T. Connie, A. Teoh, M. Goh, and D. Ngo, "Palmhashing: a novel approach for cancelable biometrics," *Information Processing Letters*, vol. 93, no. 1, pp. 1 – 5, 2005.

[35] A. Teoh, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, no. 11, pp. 2245 – 2255, 2004.

[36] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of biohashing and its variants," *Pattern Recognition*, vol. 39, no. 7, pp. 1359 – 1368, 2006.

[37] L. Leng and J. Zhang, "Palmhash code vs. palmphasor code," *Neurocomputing*, vol. 108, no. 0, pp. 1 – 12, 2013.

[38] L. Leng, A. B. J. Teoh, M. Li, and M. K. Khan, "Analysis of correlation of 2dpalmhash code and orientation range suitable for transposition," *Neurocomputing*, vol. 131, no. 0, pp. 377 – 387, 2014.

[39] J. Zuo, N. Ratha, and J. Connell, "Cancelable iris biometric," *International Conference on Pattern Recognition*, pp. 1–4, 2008.

[40] F. Farooq, R. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," in *IEEE Conference on Computer Vision and Pattern Recognition*, June 2007, pp. 1–7.

[41] T. Boult, "Robust distance measures for face-recognition supporting revocable biometric tokens," in *International Conference on Automatic Face and Gesture Recognition*, April 2006, pp. 560–566.

[42] T. Boult, W. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: accuracy and security analysis," in *IEEE Conference on Computer Vision and Pattern Recognition*, June 2007, pp. 1–8.

[43] B. Yang, D. Hartung, K. Simoens, and C. Busch, "Dynamic random projection for biometric template protection," in *IEEE International Conference on Biometrics: Theory Applications and Systems*, Sept 2010, pp. 1–7.

[44] P. Das, K. Karthik, and B. C. Garai, "A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs," *Pattern Recognition*, vol. 45, no. 9, pp. 3373 – 3388, 2012.

[45] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," *Pattern Recognition*, vol. 47, no. 3, pp. 1321 – 1329, 2014.

[46] N. Ratha, J. Connell, and R. Bolle, "An analysis of minutiae matching strength," in *Audio- and Video-Based Biometric Person Authentication*, ser. Lecture Notes in Computer Science, J. Bigun and F. Smeraldi, Eds. Springer Berlin Heidelberg, 2001, vol. 2091, pp. 223–228.

[47] A. Luong, M. Gerbush, B. Waters, and K. Grauman, "Reconstructing a fragmented face from a cryptographic identification protocol," in *IEEE Workshop on Applications of Computer Vision*, Jan 2013, pp. 238–245.

[48] A. Adler, "Sample images can be independently restored from face recognition templates," in *IEEE Canadian Conference on Electrical and Computer Engineering*, vol. 2, May 2003, pp. 1163–1166 vol.2.

[49] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: A security analysis," in *Proceedings of SPIE, Electronic Imaging, Media Forensics and Security XII*, vol. 7541, 2010, pp. 75 410O–75 410O–15.

[50] F. Quan, S. Fei, C. Anni, and Z. Feifei, "Cracking cancelable fingerprint template of ratha," in *International Symposium on Computer Science and Computational Technology*, vol. 2, Dec 2008, pp. 572–575.

[51] S. Shin, M.-K. Lee, D. Moon, and K. Moon, "Dictionary attack on functional transform-based cancelable fingerprint templates," *ETRI Journal*, vol. 31, no. 5, pp. 628–630, 2009.

[52] A. Lumini and L. Nanni, "An improved biohashing for human authentication," *Pattern Recognition*, vol. 40, no. 3, pp. 1057 – 1065, 2007.

[53] Y. Lee, Y. Chung, and K. Moon, "Inverse operation and preimage attack on biohashing," in *IEEE Workshop on Computational Intelligence in Biometrics: Theory, Algorithms, and Applications*, March 2009, pp. 92–97.

[54] P. Lacharme, E. Cherrier, and C. Rosenberger, "Reconstruction attack on biohashing," in *International Conference on Security and Cryptography*, 2013.

[55] R. Belguechi, E. Cherrier, and C. Rosenberger, "Texture based fingerprint biohashing: Attacks and robustness," in *IAPR International Conference on Biometrics*, March 2012, pp. 196–201.

[56] X. Zhou and T. Kalker, "On the security of biohashing," in *Proceedings of SPIE, Electronic Imaging, Media Forensics and Security II*, vol. 7541, 2010, pp. 75 410Q–75 410Q–8.

[57] S. Li and A. Kot, "Fingerprint combination for privacy protection," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 350–360, Feb 2013.

[58] A. Ross and A. Othman, "Visual cryptography for biometric privacy," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 70–81, March 2011.

[59] A. Othman and A. Ross, "On mixing fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 260–267, Jan 2013.

[60] ——, "Privacy of facial soft biometrics: Suppressing gender but retaining identity," in *European Conference on Computer Vision Workshops*, vol. 8926, 2015, pp. 682–696.

[61] K. Simoens, B. Yang, X. Zhou, F. Beato, C. Busch, E. Newton, and B. Preneel, "Criteria towards metrics for benchmarking template protection algorithms," in *IAPR International Conference on Biometrics*, March 2012, pp. 498–505.

[62] N. Zhang, X. Yang, Y. Zang, X. Jia, and J. Tian, "Generating registration-free cancelable fingerprint templates based on minutia cylinder-code representation," in *IEEE International Conference on Biometrics: Theory, Applications and Systems*, Sept 2013, pp. 1–6.

[63] H. Zhang, V. M. Patel, M. E. Fathy, and R. Chellappa, "Touch gesture-based active user authentication using dictionaries," in *IEEE Winter Conference on Applications of Computer Vision*, 2015.

[64] M. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Oct 2010, pp. 306–311.

[65] A. Primo, V. V. Phoha, R. Kumar, and A. Serwadda, "Context-aware active authentication using smartphone accelerometer measurements," in *IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2014, pp. 98–105.

[66] S. Rane, "Standardization of biometric template protection," *IEEE MultiMedia*, vol. 21, no. 4, pp. 94–99, Oct 2014.