Pattern Recognition 48 (2015) 458–472

Contents lists available at ScienceDirect

Pattern Recognition

journal homepage: www.elsevier.com/locate/pr

Secure biometric template generation for multi-factor authentication

Salman H. Khan [a,*], M. Ali Akbar [b], Farrukh Shahzad [b], Mudassar Farooq [b], Zeashan Khan [c]

[a] School of Computer Science and Software Engineering, The University of Western Australia, Crawley, WA 6009, Australia
[b] Next Generation Intelligent Networks Research Center, Institute of Space Technology, Islamabad 44000, Pakistan
[c] Riphah International University, I-14, Islamabad 44000, Pakistan

ARTICLE INFO

Article history:
Received 12 January 2014
Received in revised form
20 August 2014
Accepted 28 August 2014
Available online 8 September 2014

Keywords:
Two factor authentication
Biometric template protection
Feature transformation
Dynamic signature verification
Biohashing
Random projections
Distance matching

ABSTRACT

In the light of recent security incidents, leading to compromise of services using single factor authentication mechanisms, industry and academia researchers are actively investigating novel multi-factor authentication schemes. Moreover, exposure of unprotected authentication data is a high risk threat for organizations with online presence. The challenge is how to ensure security of multi-factor authentication data without deteriorating the performance of an identity verification system? To solve this problem, we present a novel framework that applies random projections to biometric data (inherence factor), using secure keys derived from passwords (knowledge factor), to generate inherently secure, efficient and revocable/renewable biometric templates for users' verification. We evaluate the security strength of the framework against possible attacks by adversaries. We also undertake a case study of deploying the proposed framework in a two-factor authentication setup that uses users' passwords and dynamic handwritten signatures. Our system preserves the important biometric information even when the user specific password is compromised – a highly desirable feature but not existent in the state-of-the-art transformation techniques. We have evaluated the performance of the framework on three publicly available signature datasets. The results prove that the proposed framework does not undermine the discriminating features of genuine and forged signatures and the verification performance is comparable to that of the state-of-the-art benchmark results.

1. Introduction

The ubiquitous Internet connectivity has led to provision of an ever increasing list of diverse online services ranging from financial transactions to online gaming. With cloud computing on the rise, geographically distant employees of organizations tend to access and share the sensitive organizational resources online. This trend has increased the stakes of user authentication process. An ever increasing need to control the access to sensitive resources, through user authentication process, demands that the data needs to be stored on the server in a secure manner.

The three different types of elements (known as *factors*) that can be used for authentication of a user's identity are the *ownership*, *knowledge* and *inherence* factors. The traditional passwords based approach belongs to the knowledge factor (something user knows) and has been the prevalent method of authentication for the last couple of decades. However, as the recent security incidents have demonstrated, the single-factor authentication (SFA) approach is insufficient [38,12,17]. The threats against poorly protected authentication information are rising exponentially. The major leaks of the period 2012–2013 – include Twitter [38], LinkedIn [21], IEEE.org [12], Dropbox [6] and Yahoo [17] – corroborate the argument. Therefore, there is a requirement for adoption of multi-factor authentication (MFA) schemes (e.g., Dropbox offered two-factor authentication (TFA) in July 2012 [6]). A directive from US Federal Financial Institutions Examination Council (FFIEC) also makes it compulsory for the banks to use MFA in online transactions [14].

Biometrics based identity verification systems are unique from the ownership factor (ATM, National ID Card, badges, etc.) and knowledge factor (password, security questions, PIN number, etc.) based authentication paradigms. Consequently, such systems free the user from concerns like identity lost/theft, illegal distribution, repudiation, expiry dates, bearing the identity all times or remembrance issues [33]. Human biometrics are characteristic of a user (inherence factor) and can be used collectively with passwords for MFA for highly secure systems. The verification performance achieved through the analysis of human biometric traits has reached up to a mature level. However, the security and privacy of biometric templates for storage and communication is still a challenging problem [54]. The possible vulnerabilities in the existing biometric authentication systems have been explored in various recent studies [7,1,19], thus advocating that the security of biometric templates is an open research problem. It must be noted that biometric data needs special attention for its security because

* Corresponding author.
E-mail address: salman.khan@research.uwa.edu.au (S.H. Khan).

http://dx.doi.org/10.1016/j.patcog.2014.08.024
0031-3203/

standard encryption techniques (like RSA, DES and AES) cannot be employed in this case [3]. Mainly, this is due to the reason that template matching cannot be performed in encrypted domain since intra-user variability is not preserved.

The current need is to design security mechanisms that make use of multi-factor authentication in such a way that not only the user privacy is preserved but the biometric authentication is also accurate. A scheme for secure storage of user authentication template can be evaluated over a set of necessary requirements that ensures relatively foolproof template usage, handling and accessibility [26,4]. These requirements are:

- *Security*: The secured template should not leak the original authentication data and the user-specific factors. Privacy of each user should remain intact when data of one user is matched with other users.
- *Performance*: The performance of user authentication system using secure template must not seriously degrade in comparison to its non-secured counterparts. False reject rate (FRR) and false accept rate (FAR) should be as low as possible.
- *Renewability*: The secured template and the user-specific factors must be easily cancellable in an event of compromise. It should be possible to generate a new unique template when the same authentication data is provided.

In view of the aforementioned challenges and requirements, we present our template generation framework that applies random projections to biometric data (inherence factor), using secure keys derived from passwords (knowledge factor), to generate inherently secure, efficient and revocable/renewable biometric templates for user verification. We discuss how compressed sensing can weaken the security of randomly mapped biometric data. We apply an arithmetic hash function to further secure the mapping acquired after random projections. The key distinguishing feature of this novel scheme KRP−AH (Keyed Random Projections and Arithmetic Hashing) is its strength against attacks despite compromise of user specific key. Moreover, this scheme does not require the random subspace mapping to be strictly orthogonal as opposed to schemes that only consider orthogonal random projections for mapping biometric data [31,52]. Since our framework does not use error correcting codes or biohashing, there is no need to restrict real valued biometric signals to binary domain and this also helps in preserving security. The framework performs user authentication by using a bi-stage scheme requiring genuine biometric data and correct user specific key/password.

The rest of the paper is organized as follows. In Section 2, we describe the related work in the area of biometrics security. We formulate the mathematical constructs for the KRP−AH scheme in Section 3. The proposed framework architecture for the TFA utilizing KRP−AH scheme is presented in Section 4. Our scheme uses a novel operation named *Arithmetic Hashing* to strengthen the security of biometric templates. We discuss the security strengths of the framework against different attack scenarios in Section 5. To empirically establish that the generated secure biometric templates are still highly usable for authentication purposes, we evaluate the proposed framework in a TFA setup by using user passwords and dynamic handwritten signatures in Section 6. Unlike the traditional feature transformation techniques [20,35,29,25], our system preserves the important biometric information even when the user specific password is compromised. We have identified a number of local and global features related to dynamic signatures for template generation, and we use both dynamic and static distance measures to match the secure templates. We have evaluated the performance of the framework over three publicly available dynamic handwritten signature datasets. The results show that our proposed framework does not undermine the discriminating features of genuine and forged signatures and the verification performance is at par with the reported benchmark results. Finally, we conclude the paper with an outlook to future work.

2. Related work

The proposed scheme (KRP−AH) focuses on TFA by generating secure templates derived from user-provided password and biometric data. In this section, we discuss the related work in the literature that attempts to solve the problem of securing biometric data based authentication templates. Several schemes have been proposed to protect the biometric templates. These schemes can be broadly classified in to two categories: *Biometric cryptosystems* and *feature transformation schemes* [3]. The general idea is to store and process a variant of the original biometric so that an intruder cannot extract exact biometric data if he/she gets hold of a user's template.

Biometric cryptosystems combine biometrics with standard cryptographic techniques to generate data that can be used as a proof of user's identity. Error correcting codes are usually used to deal with the intra-user variability of templates during enrollment and verification process [30,55]. Biometric cryptosystems show good performance by preserving the inter-user variability [34]. However, these systems pose a difficulty in generating revocable templates that can be easily cancelled and reissued. In feature transformation techniques, instead of storing the original biometric data, transformation functions are applied on them. When the applied transformation is invertible, we call it *salting transform*. In case when an inversion is not possible, we call it *non-invertible transform*. In either case, the transformation is dependent on a randomly generated user specific key. These schemes have good revocability; however, their performance generally decreases with an increase in complexity level of transformation function. In the following discussion, we will discuss a brief overview and shortcomings of existing feature transformation schemes.

Orthonormal random projections are studied in [20] to secure biometric templates. A random multispace quantization technique is proposed in [52] to secure face biometrics by applying orthogonal random projections and biohashing. Similar to biohashing, palmhashing technique is presented in [29] to generate revocable palmcode using Gabor filters. However the security of all these salting transforms is dependent on the security of parameters that define user specific transformation characteristics. As an example, the above-mentioned techniques that employ random projections to map users' data are dependent on user specific key or token. They use key/token as a seed to generate random projections. When this key is compromised, the security gets weak and the intruder can recover original biometric either partially or completely.

The non-invertible transforms are applied in [28,25,56] for template protection of face and finger print biometrics. Maiorana et al. have used a signature transformation technique to secure online signature templates that can be matched via HMM [35]. A universal background model based approach is discussed in [4] for dynamic signatures protection. The problem with these techniques is their relatively low performance levels compared to salting transforms. Moreover, it is difficult to quantify the level of security provided by such techniques [3]. As an example, a revocable transform is applied on finger print templates in [49] which can be cracked by the technique proposed in [47].

Our method is inspired by the work of Feng et al. [13] that uses a hybrid mechanism consisting of random projections, discriminability preserving transform (DPT), and fuzzy commitment scheme to secure face templates. Whilst the hybrid approach successfully combines positives of biometric cryptosystems and feature transformation schemes, it is different from our approach in several ways.

Firstly, our scheme combines salting and non-invertible transforms to achieve a high level of security. This ensures easy revocability and avoids the restrictions posed on security by binary templates. Moreover, our application area is different and requires special treatment since DPT cannot work on variable length handwritten signature samples. Our approach is also robust towards large intraclass differences in signatures collected from the same person, for which error correcting ability of biometric cryptosystems [55] is insufficient.

3. Keyed random projections and arithmetic hashing (KRP−AH)

Having established the need for MFA and challenges involved in secure storage of authentication data, we now propose a scheme KRP−AH for generating secure, efficient and renewable authentication templates. This scheme involves random projection of biometric data using a random key derived from a user's password, and arithmetic hashing of the resulted projections (see Fig. 1). We formulate the mathematical constructs for the keyed random projections and arithmetic hashing (KRP−AH) scheme in the following subsections. The complete overview of the proposed scheme is given in Fig. 2.

3.1. Notation

We will denote matrices with bold capital alphabets **A** and the associated vectors as bold small alphabets **a**. Sample values of vectors will be denoted by a_i (ith value). Transpose and pseudo-inverse of **A** are denoted as $\mathbf{A}^T$ and $\mathbf{A}^\dagger$ respectively. Cardinality of sets is represented by $|\cdot|$ while real and normally distributed number sets are denoted by $\mathbb{R}$ and $\mathbb{N}$ respectively. I shows the identity matrix and the sans-serif letter R is the matrix used for mapping biometric data onto random subspace. Function AH(·) denotes one-way arithmetic hash operation. Attacker's tools i.e an attack algorithm and maintained dictionary are represented as $\mathcal{A}$ and $\mathcal{D}$ respectively. Pr(·) is used to denote the probability of an event. First order and second order time derivatives of a time series $\{x_n\}$ are represented as $\{\dot{x}_n\}$ and $\{\ddot{x}_n\}$ respectively.

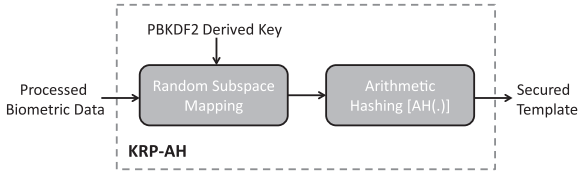

Fig. 1. KRP−AH scheme for secure template generation.

3.2. Mathematical prolegomena

3.2.1. Random projections for secured biometric templates

Random projections (RP) govern a mapping that project's high dimensional data to a lower dimensional space with an assurance that the pair-wise distances between points will be retained within an agreed threshold (ϵ). If ($\mathbf{X}^{d\times n}$) is the biometric data and R is a random matrix of dimensions $k \times d$ whose elements are sampled from a known probability distribution, then the matrix product R**X** is the randomly projected output.

Johnson and Lindenstrauss lemma (JL-lemma) [16] is one of the most important results in the theory of random projections. It states that n points in Euclidean space can be mapped to a much lower dimensional Euclidean space without loosing the preservation of relative distances between points. Formally,

JL-Lemma. *For any $0<\epsilon<1$ and any integer n, let k be a positive integer such that $k \geq 8\epsilon^{-2} \times \ln(n)$. Then for any set Z such that $|Z| = n$ in $\mathbb{R}^d$, there exists a Lipschitz mapping f: $\mathbb{R}^d \to \mathbb{R}^k$ such that for all $a, b \in Z$*

$$(1-\epsilon)\|a-b\|^2 \leq \|f(a)-f(b)\| \leq (1+\epsilon)\|a-b\|^2$$

Thus, JL-lemma puts a lower bound of $k = O(\epsilon^{-2} \log n)$ on the amount of dimensionality reduction while keeping the pair-wise distortion bounded (i.e. $<\epsilon$) [16].

In the previous RP based template protection schemes, either R is presumed to be an orthogonal matrix or it is converted into one using familiar orthogonalization techniques like Gram–Schmidt algorithm [52]. If transformed templates are denoted by $\mathbf{U} = \mathsf{R}\mathbf{X}$ and $\mathbf{V} = \mathsf{R}\mathbf{Y}$, then the inner product is given as

$$\mathbf{U}^T\mathbf{V} = \mathbf{X}^T\mathbf{Y} \quad \because \mathsf{R}\mathsf{R}^T = I$$

This means that the orthogonalization practice makes the system weak against brute-force attacks. But a stacked version of orthonormal vectors (to be used as rows of a random matrix R) was

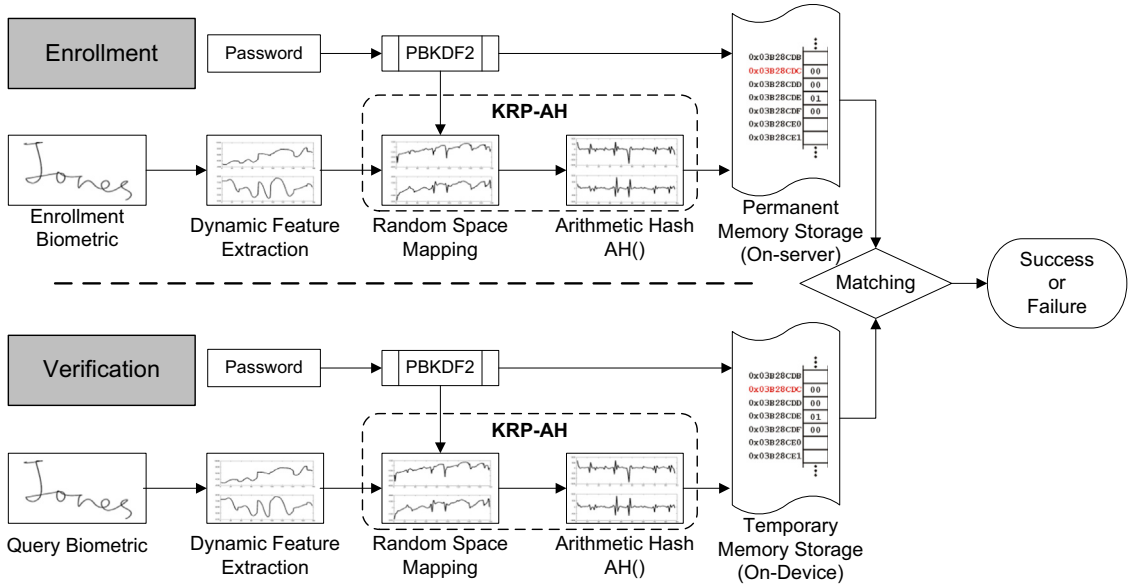

Fig. 2. Complete architecture of bi-stage two-factor user authentication framework using KRP−AH scheme.

required for constituting a valid Lipschitz mapping: $f(\mathbf{x}) = \mathsf{R}\mathbf{x}$. We may define a valid Lipschitz embedding as

Definition 1. A Lipschitz embedding $f(\mathbf{x}) = (1/\sqrt{k})\mathsf{R}\mathbf{x}$ is said to be a valid JL mapping (i.e. satisfying JL-lemma), if the elements of R are chosen such that they are independent and identically distributed (i.i.d.) according to some distribution ($\mathbb{D}$) and the probability of success in distance preservation is $(n^2-1)/n^2$ when R is formulated this way.

Any random matrix with elements chosen from an i.i.d. normal distribution $\mathbb{N}(0,\sigma^2)$ satisfies the conditions to be a valid JL-transform [8]. We have used such matrices for RP. This makes the system more secure since $\mathsf{R}\mathsf{R}^T \neq I$ and the pair-wise distances are also preserved. It is also important to mention that in this work, we have applied random projections that result in the reduction in number of features instead of data points. This helps in obfuscation of actual features and leaves us with enough points in each feature domain to carry out arithmetic hashing without performance degradation.

3.2.2. Properties of random projections

We will now briefly outline some of the relevant properties of random projections (further details can be found in [31]). These properties will be useful in understanding the remaining part of this section and the security discussion (Section 5). It must be noted that we assume a valid Lipschitz mapping R whose elements are i.i.d normally distributed with mean $\mu = 0$ and variance σ^2. Some properties of interest that R exhibits are:

1. In high dimensional space, vectors with random directions are almost orthogonal, i.e. $\mathsf{R}\mathsf{R}^T = \mathsf{R}^T\mathsf{R} \propto I$.
2. $E[\mathsf{R}^T\mathsf{R}] = k\sigma^2 I$ and $E[\mathsf{R}\mathsf{R}^T] = d\sigma^2 I$ where R has dimensions $k \times d$.
3. For row-wise projections, let $\mathbf{X}^{d\times n_1}$ and $\mathbf{Y}^{d\times n_2}$ are transformed by $\mathsf{R}^{k\times d}$ to, $\mathbf{U} = (1/\sqrt{k}\sigma)\mathsf{R}\mathbf{X}$ and $\mathbf{V} = (1/\sqrt{k}\sigma)\mathsf{R}\mathbf{Y}$ then, $E[\mathbf{U}^T\mathbf{V}] = \mathbf{X}^T\mathbf{Y}$. Similarly for column wise projections: $E[\mathbf{U}\mathbf{V}^T] = \mathbf{X}\mathbf{Y}^T$.
4. Each entry $\epsilon_{i,j}$ of matrix product $\mathsf{R}^T\mathsf{R}$ is approximately Gaussian with $E[\epsilon_{i,i}] = d\sigma^2$, $Var[\epsilon_{i,i}] = 2d\sigma^4$, $\forall i$ and $E[\epsilon_{i,j}] = 0$, $Var[\epsilon_{i,j}] = d\sigma^4$, $\forall i,\ j | i \neq j$.
5. The error $(\mathbf{u}^T\mathbf{v} - \mathbf{x}^T\mathbf{y})$ of the inner product matrix generated by Gaussian random projections and original data matrices has the statistical properties: $E[\mathbf{u}^T\mathbf{v} - \mathbf{x}^T\mathbf{y}] = 0$ and $Var[\mathbf{u}^T\mathbf{v} - \mathbf{x}^T\mathbf{y}] = (1/k)\left(\sum_i x_i^2 \sum_i y_i^2 + (\sum_i x_i y_i)^2\right)$.
6. In case when elements of R are chosen from an i.i.d $\mathbb{N}(0,1)$ or from $\mathbb{U}(-1,1)$, then

$$P(|\mathbf{u}^T\mathbf{v} - \mathbf{x}^T\mathbf{y}| \geq \epsilon) \leq 4 \times \exp\left(-\frac{k}{4}(\epsilon^2 - \epsilon^3)\right)$$

After reduction of number of features of original data by random projections R, the statistical dependencies among the observations will be maintained (from properties 3 to 6). The other way around, if the data owner compresses the observations, the relationship between the features of two signatures will be preserved (from properties 1 and 2). We can directly apply biometric template matching techniques on the perturbed data **U** and **V** without knowing the original sensitive biometric information. If intruder has only the perturbed data **U** or **V**, it cannot determine the values of the original data values in **X** or **Y**. This is due to the reason that the system of equations constituted in this case is an under-determined system with infinite possible solutions. As the amount of dimension reduction $(d-k)$ is decreased, alternatively increasing k, the amount of error introduced by the projections decreases (see properties 5 and 6). Therefore there exists a trade off between system performance and security level.

It is worth mentioning that there is a close relationship between JL-lemma and Restricted Isometric Property (RIP) through which an intruder can make use of the sparsity of biometric signal. In case, when a valid JL transform $f(\cdot)$ is an operation that projects data onto random subspace using random matrix $\mathsf{R}^{k\times d}$, we can define RIP as in [27].

Definition 2. A matrix $\mathsf{R} : \mathbb{R}^d \to \mathbb{R}^k$ is said to possess $(t,\epsilon)-RIP$ of order t and level $\epsilon \in (0,1)$ if for all t-sparse $x \in \mathbb{R}^d$ their exists the following relation:

$$(1-\epsilon)\|x\|_2^2 \leq \|\mathsf{R}x\|_2^2 \leq (1+\epsilon)\|x\|_2^2$$

The intruder can make use of RIP which resolves the problem of finding solution to a system of under-determined linear equations, $\mathbf{u} = \mathsf{R}\mathbf{x}$, where $\mathbf{x}$ is sparse. This is because the NP hard ℓ_0 minimization problem turns into a basis pursuit compressed sensing problem when RIP holds. This t-sparse solution is given by[1]

$$\hat{x} = \underset{\mathsf{R}z = u}{\operatorname{argmin}} \|z\|_1$$

ℓ_1 minimization is a convex optimization problem and can be efficiently solved using linear programming methods. Gaussian and Bernoulli matrices have $(t,\epsilon)-$RIP with high probability if $k \geq t \times \log(d)/\epsilon^2$. It can be shown that if the matrix R satisfies concentration inequality for JL-Lemma then it is highly probable that it would also satisfy (t,ϵ)-RIP for $t < c'\epsilon^2 k/\log(d)$ [5]. This concentration inequality can be expressed as

$$Pr\left((1-\epsilon)\|x\|_2^2 \leq \|\mathsf{R}x\|_2^2 \leq (1+\epsilon)\|x\|_2^2\right) \geq 1 - 2\exp(-ck\epsilon^2)$$

In our case, this relation is satisfied for R whose elements are chosen identically and independently from $\mathbb{N}(0,\sigma^2)$. The same is true for error between two vectors projected using R with elements having $\mathbb{N}(0,\sigma^2)$ distribution [31].

Krahmer and Ward [27] have proved a converse result that given R satisfying RIP, it can be shown that it is possible to embed it into a low dimensional space by applying JL lemma and taking into account some bounds [27]. This allows the application of theoretical results from compressed sensing to the JL low dimensional embeddings. When the signals are sparse, there exists a possibility of reconstruction from a few samples that may not be able to reconstruct the original signal in naive sense. Furthermore, *using random projections alone may partially leak biometric information* in case of an attack (this scenario is discussed in detail in Section 5).

3.2.3. Arithmetic hashing

To solve the above-mentioned security issues with biometric templates, we have employed an 'easy to compute' and 'difficult to invert' one way function. Given a function f, there exists an algorithm $\mathcal{A}$ that takes an input x, computes it for reasonable finite time T and outputs the result $f(x)$. Suppose there is another algorithm $\mathcal{B}$ that takes $f(x)$ as input, computes it for finite amount time T' and tries to guess the correct output i.e. $f'(f(x)) = x$. For a one way function, the probability of guessing x should be negligibly small so that correct inversion would be a rare event [44]. For a very large number of runs 'n', the probability of occurring correct inversion x is very small:

$$Pr(f'(f(x)) = x) < \frac{1}{n}$$

[1] $\|\cdot\|_1$ is the ℓ^1 norm in Banach space and $\|\cdot\|_2$ is the ℓ^2 norm in Lebesgue space.

The one way function we have employed is a first order difference followed by a decimation operation in which every second element is dropped. So effectively this operation becomes equivalent to the difference operation on consecutive pairs such that no pair is overlapped and hence can be termed as '*curtailed difference operation*'. The intuition of this technique lies in the fact that signals do not loose discrimination ability when their rate of change is calculated, rather such a calculation is often helpful in increasing the discriminating ability of signals. However, a derivative step by no way increases the security of original signal since a simple integration (summation) step can recover the original signal. The decimation step is put next to difference so that the links between pairs are dropped and the original signal cannot be fully recovered. Note that the factor by which we decimate the randomly projected biometric signal is also not known to the intruder.

For the case of quickly varying time series signals (such as randomly projected handwritten signature), AH function avoids the exact recovery of original signal by an intruder. Moreover, this operation preserves the discriminative ability of signals and the verification performance is not degraded (see Section 6.5.3 for results). The main reason why performance remains unaffected is the distance preserving transformation (Section 3.2.1) followed by the differential and decimation (low-pass) filters which keep the distinctive features of time-varying signals. An example of AH function applied to signature data and the resulting recovered signal is shown in Fig. 3. For the security analysis, Fig. 4 shows the error distribution for the signal recovered after an AH operation. We consider two cases to simulate signal recovery. For the first case, it is assumed that the attacker knows the operations involved in AH but do not know the exact parameters e.g., decimation rate. For this scenario, we take 200 genuine signatures from each of the three signature datasets (SVC'04, SUSig'07 and SigComp'11) and try to recover them with different possible choices of parameters. For each signal, we use an interpolation factor in the range (0, 20), samples used for interpolation in the range (2, 20) with steps of 2 and normalized cutoff frequency in the range (0.25, 0.75) with steps of 0.05. This makes a total of 1.26×10^6 runs and the distribution of mean square error (MSE) distribution is shown in Fig. 4(a). For the second case, we assume that the attacker knows all details about the AH function. We now try to recover the original signal for all the genuine signatures in the three signature datasets. The resulting MSE distribution is shown in Fig. 4(b). Note that the error is measured in comparison to the randomly projected signatures and the intruder will still have to recover the randomly projected data even after cracking the AH function.

4. Architecture of bi-stage two-factor user authentication framework based on KRP−AH scheme

Based on the proposed KRP−AH scheme for secure template generation, we now present a complete framework for two-factor user authentication. The framework performs its operation in two separate stages: the *enrollment phase* and *verification phase*.

4.1. Enrollment phase

During the enrollment phase a user presents his/her biometric data which is acquired in the form of a matrix, $\mathbf{D}$. We can express it as a random matrix because its elements may assume any probability distribution $p_{\mathbf{D}}(\mathbf{D})$ depending on the nature of biometric involved and the type of user. This data is then passed through a feature extraction module $\mathcal{F}_{feat}(\cdot)$ that converts raw data into useful information. The resulting processed data in feature space is $\mathbf{P} = \mathcal{F}_{feat}(\mathbf{D})$. For the protection of these feature vectors, they are passed on to secure biometric module $\mathcal{F}_{sec}(\cdot)$ that projects it onto random subspace. These random projections are dependent on the seed value provided by the password based key derivation function PBKDF2 ($\mathcal{F}_{kdf}(\cdot)$). This function takes the key/password ($\mathbf{k}$), cryptographic salt, number of iteration (n_{iter}) and desired derived key length (ℓ_{dk}) as an input to generate a derived key ($\mathbf{h}$). So,

$$\mathbf{h} = \mathcal{F}_{kdf}(\mathbf{k}, salt, n_{iter}, \ell_{dk})$$
$$\mathbf{S} = \mathcal{F}_{sec}(\mathbf{P}; \mathbf{h})$$

It can be assumed that the function $\mathcal{F}_{kdf}$ is non-invertible or at least it is difficult to do so. However, the security of $\mathbf{S}$ is partially dependent on $\mathbf{h}$. In case $\mathbf{k}$ is compromised, the bio-metric template will not be fully exposed, rather only the minimum norm solution

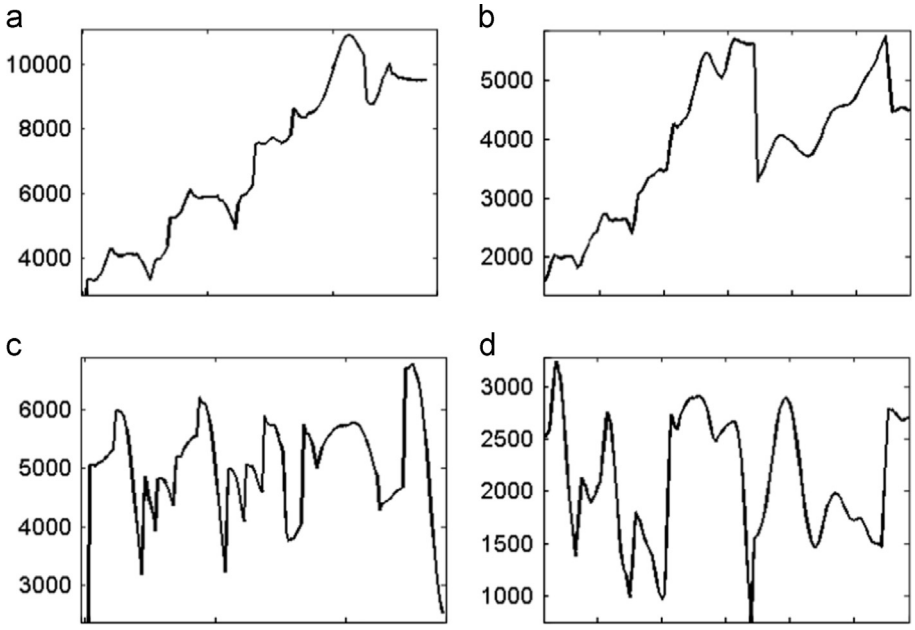

Fig. 3. Arithmetic hashing hinders the recovery of original signal: the left column shows original signals and the right column shows signals recovered by interpolation (up-sampling) followed by integration of the output from AH function. Handwritten signature for demonstration is taken from sample data in SVC dataset (a) *x*-axis data of signature, (b) signal (a) recovered after AH, (c) *y*-axis data of signature and (d) signal (b) recovered after AH.

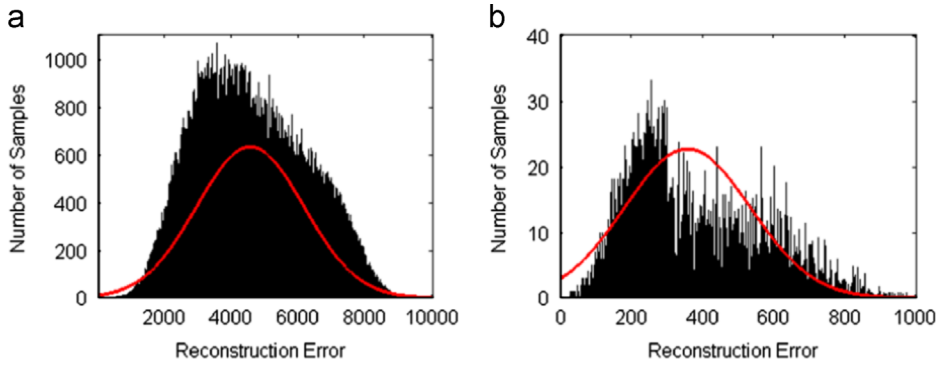

Fig. 4. The MSE distribution for three signature datasets (SVC'04, SUSig'07 and SigComp'11). We compare Gaussian distributions fitted over data (shown in *red*) with the respective histograms (shown in *black*). The error is measured after the normalization and re-scaling to match height and width of signals and to remove any DC component. (a) The reconstruction error distribution when attacker has partial information about AH and (b) the reconstruction error distribution when attacker has full information about AH. (For interpretation of the references to color in this figure caption, the reader is referred to the web version of this article.)

will be released. From this solution a partial leak of biometric information is possible. To solve this problem, an arithmetic hash AH() operation is introduced which is easy in computation and from which recovery of original biometric data is almost impossible (details of which will be discussed in Section 5). This enhancement in security level comes with a corresponding decrease in performance. We will show in Section 6.5 that this associated loss in performance is not significant in case of handwritten dynamic signature verification.

The vector $\mathbf{S}$ is secured through AH() to generate $\mathbf{S}_*$. This secured data $\mathbf{S}_*$, derived key $\mathbf{h}$ along-with the specifics required in $\mathcal{F}_{kdf}$ are composed in the form of a template:

$$\mathcal{T} = \{\mathbf{S}_*, \mathbf{h}, salt, n_{iter}, \ell_{dk}\}$$

This template is either stored in memory or sent to a remote location as per requirement, while the data used in intermediate steps ($\mathbf{D}$, $\mathbf{P}$, $\mathbf{S}$) is securely discarded.

4.2. Verification phase

When a query is made by the same user, a similar series of operations are performed as in enrollment. A set of raw data values $\mathbf{D}'$ of the same biometric are provided again by the user for authentication. We can assume that this data belong to some probability distribution $p_{\mathbf{D}'}(\mathbf{D}')$. This data is then passed through the feature extraction module $\mathcal{F}_{feat}(\cdot)$ which outputs the processed vector in feature space $\mathbf{P}' = \mathcal{F}_{feat}(\mathbf{D}')$. Next, this feature vector is secured by projecting it onto random space by the function $\mathcal{F}_{sec}(\cdot)$. These random projections take the derived key $\mathbf{h}'$ produced by the function $\mathcal{F}_{kdf}(\cdot)$ as the seed value and outputs a secured version $\mathbf{S}'$. A second level of security is added by applying AH(·) to generate $\mathbf{S}'_*$ from $\mathbf{S}'$. Again, the actual, feature and secured data ($\mathbf{D}'$, $\mathbf{P}'$, $\mathbf{S}'$) are discarded while a template $\mathcal{T}'$ is retained.

Biometrics of different users can be modeled as statistically independent variables such that given data of two users – $\mathbf{D}_1$ and $\mathbf{D}_2$ – joint probability can be expressed as $p_{\mathbf{D}_1,\mathbf{D}_2}(\mathbf{D}_1, \mathbf{D}_2) = p_{\mathbf{D}_1}(\mathbf{D}_1)\, p_{\mathbf{D}_2}(\mathbf{D}_2)$. In contrast, when a second sample $\mathbf{D}'$ of same biometric from same user is provided, we can write joint probability distribution function as $p_{\mathbf{D}',\mathbf{D}}(\mathbf{D}', \mathbf{D}) = p_{\mathbf{D}',\mathbf{D}}(\mathbf{D}'|\mathbf{D})p_{\mathbf{D}}(\mathbf{D})$. Here $p_{\mathbf{D}',\mathbf{D}}(\mathbf{D}'|\mathbf{D})$ accounts for the variation of second sample of biometric data $\mathbf{D}'$ from the originally provided biometric $\mathbf{D}$. When $\mathcal{F}_{sec}(\cdot)$ is applied on data, we want to retain this inevitable variation between genuine biometric samples within reasonable bounds ($|p_{\mathbf{D}',\mathbf{D}}(\mathbf{D}'|\mathbf{D}) - p_{\mathbf{S}',\mathbf{S}}(\mathbf{S}'|\mathbf{S})| < \epsilon$) such that the inter-user variability remains exploitable by the template matching techniques. This condition is ensured by the JL-lemma which is discussed earlier in Section 3. Therefore, instead of dealing with $p_{\mathbf{D}',\mathbf{D}}(\mathbf{D}', \mathbf{D})$ we will be concerned with $p_{\mathbf{S}',\mathbf{S}}(\mathbf{S}', \mathbf{S})$. For legitimate users we will have a joint probability distribution defined by $p_{\mathbf{S}',\mathbf{S}}(\mathbf{S}', \mathbf{S}) = p_{\mathbf{S}',\mathbf{S}}(\mathbf{S}'|\mathbf{S})p_{\mathbf{S}}(\mathbf{S})$.

The matching function $\mathcal{F}_{mat}(\cdot)$ performs a comparison between $\mathcal{T}$ and $\mathcal{T}'$. For successful authentication, the user provided key/password ($\mathbf{k}'$), cryptographic salt, number of iterations (n'_{iter}) and desired derived key length (ℓ'_{dk}) must strictly match with their corresponding copies stored in the original template. Along with this, there must exist a close match between copies of secured biometric data i.e. $p_{\mathbf{S}'_*,\mathbf{S}_*}(\mathbf{S}'_*|\mathbf{S}_*) \approx 1$ and $\mathbf{h}' = \mathbf{h}$. In this way, a highly secured TFA scheme, combining knowledge and inherence factor, is successfully implemented.

5. Attack scenarios and security analysis of proposed scheme (KRP−AH)

In this section, we enumerate some important attack scenarios and conduct a security analysis against these attacks. This analysis helps us to understand better how the proposed KRP−AH is resistant to security and privacy leaks even when highly critical partial information is leaked. Note that the security level is proportional to the ability to recover the actual biometric signal. A successful security mechanism will protect the privacy of a genuine subject by concealing its original biometric data from an intruder as well as the verification server.

5.1. Key is disclosed along-with random projections

Consider a system configuration such that the randomly projected data is denoted by $\mathbf{U} = \mathsf{R}\mathbf{X}$. For now, suppose that the biometric security system does not involve a one way arithmetic operation (AH). As an example, Fig. 5 shows dynamic signatures when mapped from $d = 39$ dimensional space to lower dimensional space of $k = 20$. It can be seen that actual signature data has got obscured under such a mapping.

Given an event of key compromise (secured by $\mathcal{F}_{kdf}$), an adversary will be able to know the actual realization of random matrix R. This encompass the notion that the dimensionality of R and its probability distribution is also known to eavesdropper. When R is fat i.e. the number of rows in R is less than the number of its columns ($\mathsf{R}^{k\times d} : k < d$) for every vector $\mathbf{x} \in \mathbf{X}$ and $\mathbf{u} \in \mathbf{U}$, we have an under-determined system of linear equations $\mathbf{u} = \mathsf{R}\mathbf{x}$ which has infinitely many solutions. To find the complete solution we start from '*minimum norm solution*' that seeks to find solution $\mathbf{x}^*$ such that $\|\mathbf{x}^*\|_2$ is minimized. We have $\mathbf{x}^* = \mathsf{R}^T\mathbf{w}$, where $\mathbf{w}$ is the solution of a solvable system $\mathbf{w} = (\mathsf{R}\mathsf{R}^T)^{-1}\mathbf{u}$. Here, $(\mathsf{R}\mathsf{R}^T)^{-1}$ is a non-singular matrix of full rank (k) because of the independence of rows in R. The minimum norm solution is given by $\mathbf{x}^* = \mathsf{R}^\dagger\mathbf{u}$, with $\mathsf{R}^\dagger$ being the pseudo-inverse of full rank, fat R. In the system

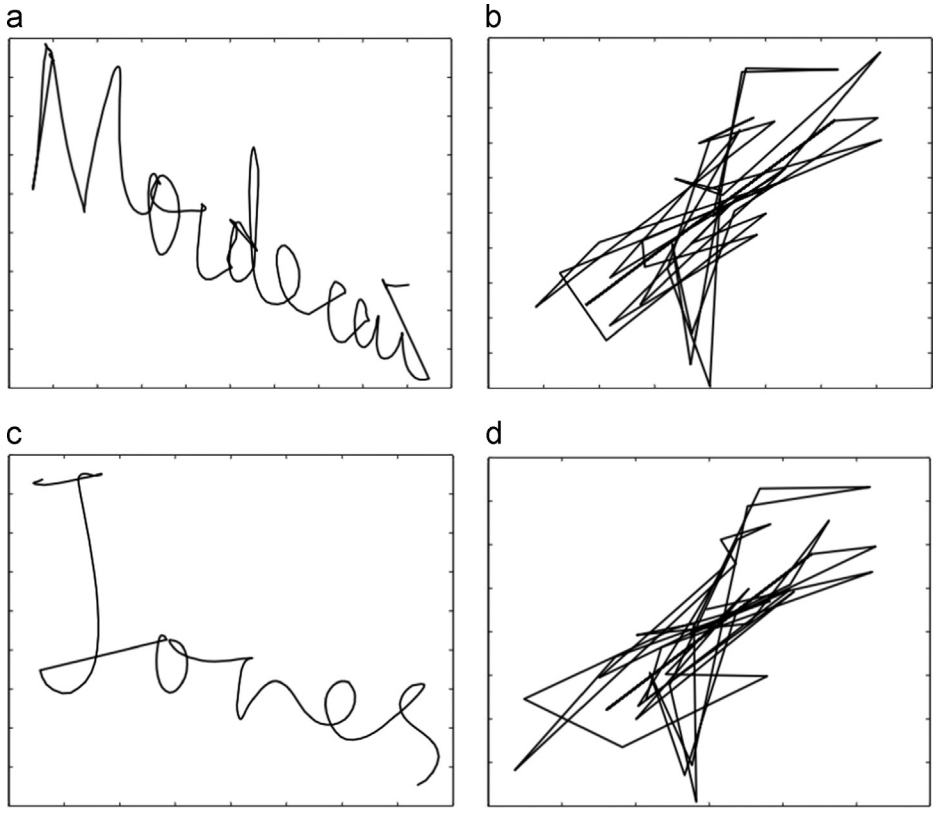

Fig. 5. Obfuscation of original signature data through random projection. (a) Original signature, (b) random projection of (a), (c) original signature and (d) random projection of (c).

of linear equations $\mathbf{u}=\mathsf{R}\mathbf{x}$ any solution of $\mathbf{x}$ will have the form $\mathbf{x}^*=\mathbf{x}_0-\mathbf{y}^*$ such that $\mathbf{y}^*$ belongs to null space of R, $\mathcal{N}(\mathsf{R})$ i.e. $\mathsf{R}\mathbf{y}^*=\mathbf{0}$ which has $\dim(\mathcal{N}(\mathsf{R}))=d-k$ degrees of freedom [46]. This implies that for any vector $\mathbf{z}$, the product $\mathbf{z}\cdot\mathsf{R}\mathbf{y}^*=\mathbf{z}\cdot\mathbf{0}=\mathbf{0}$. As mentioned in [31], it proves that if an adversary gets knowledge of the random matrix R, it is not possible to know exactly each of the value in vector $\mathbf{x}$, for each system of linear equations $\mathbf{u}=\mathsf{R}\mathbf{x}$.

Biometric signals can be represented in the sparse form, for example as a product of training dictionary matrix and the residual sparse signal i.e. $\mathbf{u}=\mathbf{A}\boldsymbol{\alpha}$ or performing an ℓ^1 regularization [45]. If an intruder gets access to a large number of genuine secured templates then a training dictionary $\mathbf{A}$ can be formed easily. Finding sparse solution to such a problem is a well founded problem in compressed sensing [11]. It must be noted that in the given case, the ℓ_2 norm solution that gives pseudo-inverse is not feasible because it usually does not lead to sparse solution. The sparsest solution (ℓ_0 normalization) is non-deterministic polynomial-time (NP) hard. RIP described in Section 3.2 helps in finding a stable sparse solution of an ill-posed system of linear equations. When RIP is satisfied, minimum ℓ_1 norm solution of an under-determined system of linear equations is also the sparsest solution [9]:

$$\hat{\boldsymbol{\alpha}}=\underset{\boldsymbol{\alpha}}{\operatorname{argmin}}\|\boldsymbol{\alpha}\|_1$$

Algorithms like greedy search and convex relaxation techniques are usually used to solve such problems. Donoho et al. [10] have recently proposed a stage-wise orthogonal matching pursuit (OMP) method for general sparse solution. However, such methods play with the sparsity of signals, which is usually absent in biometric signals (especially in the case of handwritten signatures).

Actual biometric data usually does not contain feature vectors containing many strict zeros. As discussed earlier, template protection using random projections for biometrics like facial images of sparse nature is not a secure method. The intruder can maintain a dictionary of training samples from a number of users to correctly identify the unique user and obtain original biometric when dimension of random projections and user specific key are known. To resolve this issue, the simple hash function (AH) is proposed by us which is used to obtain an irreversible template that can be adequately used for verification purposes. The performance of two-factor verification system using AH is not much undermined as evaluated in Section 6.5.3. Having said that this analysis is valid in the case when hashed key is compromised. When key is secure, it does not matter whether data is sparse or not because it will be secured in either case [48].

5.2. Characteristics of random projections are disclosed

Another important question from security point of view is the case of partial leak of information regarding the type of random projections. Suppose the adversary gets knowledge of the dimensions $k\times d$ of R, and the probability distribution from which the elements of R are chosen independently. On the basis of this knowledge another random matrix $\tilde{\mathsf{R}}$ can be generated. By inverting the $\tilde{\mathsf{R}}$ (i.e. finding pseudo inverse $\tilde{\mathsf{R}}^\dagger$) and multiplying with the randomly projected vector $\mathbf{u}$, an estimate of original biometric data $\mathbf{x}$ can be made. When R is a full row rank matrix, $\mathsf{R}^\dagger$ can be defined by left inverse. Otherwise, Singular Value Decomposition (SVD) is used to find $\mathsf{R}^\dagger$. In further discussion we will be in need of the characteristics of pseudo inverse ($\mathsf{R}^\dagger$).

Lemma 1. *Given a random matrix $\mathsf{R}^{k\times d}$ whose elements come from an independent and identically distributed normal pdf with mean 0 and variance $\sigma^2:\mathbb{N}(0,\sigma^2)$, then the pseudo inverse $\mathsf{R}^\dagger$ of R will have the statistical distribution: $\mathbb{N}(\mu_{r^\dagger},\sigma_{r^\dagger})$, where*

$$\mu_{r^\dagger}=0,\quad \sigma_{r^\dagger}^2=\frac{\sigma^2}{\left(\|\mathbf{r}_i\|^2\right)^2}$$

Proof. For $\mathsf{R}^\dagger$ to be a valid pseudo inverse of R, it must satisfy the four Penrose conditions:

$$\mathsf{R}\mathsf{R}^\dagger\mathsf{R}=\mathsf{R}, \mathsf{R}^\dagger\mathsf{R}\mathsf{R}^\dagger=\mathsf{R}^\dagger \tag{1}$$

$$(\mathsf{R}\mathsf{R}^\dagger)^T=\mathsf{R}\mathsf{R}^\dagger, \quad (\mathsf{R}^\dagger\mathsf{R})^T=\mathsf{R}^\dagger\mathsf{R} \tag{2}$$

Let $\mathbf{r}_i \in \mathsf{R}$ then from Eq. (1), the pseudo inverse $\mathbf{r}_i^\dagger$ is given by

$$\mathbf{r}_i^\dagger=\frac{\mathbf{r}_i^T}{\langle \mathbf{r}_i,\mathbf{r}_i\rangle}=\frac{\mathbf{r}_i^T}{\|\mathbf{r}_i\|^2}$$

where $\langle \mathbf{r}_i,\mathbf{r}_i\rangle$ is the dot product,

$$\|\mathbf{r}_i\|^2=\sum_{j=1}^{d} r_{ij}^2$$

The expected value of $\mathbf{r}_i^\dagger$ is

$$E[\mathbf{r}_i^\dagger]=0, \quad \because E[\mathbf{r}_i]=0$$

and the effect of linear transformation of $\mathbf{r}_i$ on variance is

$$var(\mathbf{r}_i^\dagger)=\frac{1}{\left(\|\mathbf{r}_i\|^2\right)^2}\cdot\sigma^2 \qquad \square$$

Corollary 1. *Alongside the Moore–Penrose pseudo inverse, Lemma 1 also holds for the case of generalized inverse and reflexive generalized inverse of matrix* R.

Proof. This result comes directly from the fact that both the generalized inverse and reflexive generalized inverse satisfy first relation in Eq. (1). $\square$

Lemma 2. *Given a random matrix* $\mathsf{R}^{k\times d}$ *whose elements come from an independent and identically distributed standard normal pdf:* $\mathbb{N}(0,1)$*, then the pseudo-inverse* $\mathsf{R}^\dagger$ *of* R *will have the statistical distribution:* $\mathbb{N}(0,\sigma_{r^\dagger}^2)$*, where* $\sigma_{r^\dagger}^2$ *can be approximated by*

$$\sigma_{r^\dagger}^2\approx\frac{1}{d^2}, \quad d>k$$

for significantly large values of d.

Proof.

$$E\left[\|\mathbf{r}_i\|^2\right]=E\left[\sum_{j=1}^{d} r_{ij}^2\right]=d\sigma^2=d \quad \because \sigma^2=1\left(\|\mathbf{r}_i\|^2\right)^2\approx d^2 \qquad \square$$

If $\tilde{\mathsf{R}}=\mathsf{R}$, left multiplication of the pseudo inverse $\tilde{\mathsf{R}}^\dagger$ with $\mathbf{u}$ will produce $\mathbf{I}$. We will like to investigate the case when $\tilde{\mathsf{R}}\neq\mathsf{R}$.

$$\mathbf{u}=\mathsf{R}\mathbf{x}, \quad \tilde{\mathsf{R}}^\dagger\mathbf{u}=\tilde{\mathsf{R}}^\dagger\mathsf{R}\mathbf{x}$$

If we define δ_{mn} as the $\{m,n\}$th element of $\tilde{\mathsf{R}}^\dagger\mathsf{R}$ then,

$$\delta_{mn}=\sum_{i=1}^{k}\tilde{r}_{mi}^\dagger r_{in} \quad \forall m,n, \quad 1\le m\wedge n\le d$$

The estimate of $\mathbf{x}$ denoted by $\tilde{\mathbf{x}}$ equals,

$$\tilde{x}_m=\sum_{n=1}^{d}\delta_{mn}x_n, \quad 1\le m\le d$$

$$\mu_{\tilde{\mathbf{x}}}=E[\tilde{x}_m]=\sum_{n=1}^{d}E[\delta_{m,n}x_n]=0$$

which is due to the fact that δ_{mn} and x_n are independent $E[\delta_{mn}\mathbf{x}_n]=E[\delta_{mn}]E[\mathbf{x}_n]$. Here, $E[\delta_{mn}]=0$ because $\tilde{\mathsf{R}}^\dagger$ and R are independent with zero mean.

Variance of $\tilde{\mathbf{x}}$ can be expressed as

$$Var[\tilde{\mathbf{x}}]=E[(\tilde{\mathbf{x}}-\mu_{\tilde{\mathbf{x}}})^2]=E[(\tilde{\mathbf{x}})^2] \quad \because \mu_{\tilde{\mathbf{x}}}=0$$

$$E[(\tilde{\mathbf{x}})^2]=E[\tilde{\mathbf{x}}\cdot\tilde{\mathbf{x}}]=E[\tilde{\mathbf{x}}^T\tilde{\mathbf{x}}]=E\left[\left(\sum_{i=1}^{d}x_i\delta_{i,n}\sum_{j=1}^{d}\delta_{m,j}x_j\right)\right]$$

$\tilde{\mathsf{R}}^\dagger\mathsf{R}$ is a square matrix with dimension $d\times d$. Therefore $E[(\tilde{\mathbf{x}})^2]=0$ when $i\neq j$ and

$$E[(\tilde{\mathbf{x}})^2]=k\sigma^2\sigma_{r^\dagger}^2\sum_{i=1}^{d}x_i^2$$

when $i=j$.[2] Substituting the value of variance of pseudo inverse R, $\sigma_{r^\dagger}^2=\sigma^2/\left(\|\mathbf{r}_i\|^2\right)^2$, we have

$$E[(\tilde{\mathbf{x}}_m)^2]=\frac{k\sigma^4}{\left(\|\mathbf{r}_i\|^2\right)^2}\sum_{i=1}^{d}x_i^2,$$

where, $\left(\|\mathbf{r}_i\|^2\right)^2\approx d^2$ and $d>k$ which leaves the $\tilde{\mathbf{x}}$ with all values close to zero.

Remark 1. When the characteristics of random projection are disclosed, an intruder can try to recover the original biometric using the pseudo inverse $\mathsf{R}^\dagger$. However, our mathematical analysis (Lemmas 1 and 2) shows that the recovered signal will only have all approximately zero values.

5.3. Brute force attack

We have discussed the strengths and vulnerabilities of random projections in detail. Now, we will see how the security scenario shape up when the transformation AH() is applied on **S**. This transformation can be expressed as

$$\mathsf{AH}(\mathbf{S})=[\mathsf{AH}(\mathbf{s}_1)\ldots\mathsf{AH}(\mathbf{s}_\ell)\ldots\mathsf{AH}(\mathbf{s}_k)]^T$$

$$s_\ell^{*(i+1)}=\mathsf{AH}(\mathbf{s}_\ell^{2i+1})=s^{2i+1}-s^{2i+2} \quad \forall i\in[0,n]$$

The transformation AH() operates on the output of random projection block and computes result that is half of the number of data points in input data. Let the number for data points in all $\mathbf{s}_\ell$, where $\ell\in[1,k]$, is n. Each data value is t digit wide. So, if we want to reconstruct the correct $\mathbf{s}_\ell$ from it's transformed version $\mathbf{s}_\ell^*$, we have infinite equally probable options. We can express this as the case when an intruder gains information about the $\mathbf{s}_\ell^*$ and would like to reconstruct actual data so that some values of genuine biometric $\mathbf{x}_\ell$ may be found. For a successful attack vector $\mathbf{s}_\ell$ must be present on the attacker's dictionary of possible secured biometric vectors. We consider the worst case that the attacker has gained access to every thing stored in the memory i.e. **h**, R and the characteristics of $\mathcal{F}_{feat}$, $\mathcal{F}_{kdf}$, $\mathcal{F}_{sec}$, AH. The adversary then employs an algorithm $\mathcal{A}$ to built a dictionary of possible outcomes given $\mathbf{s}_\ell^*$:

$$\mathcal{D}=\mathcal{A}(\mathbf{s}_\ell^*,\mathbf{h},\mathsf{R},p_{\mathbf{x}},p_{\mathbf{y}},\mathcal{F}_{sec}(\cdot),\mathcal{F}_{feat}(\cdot),\mathcal{F}_{kdf}(\cdot),\mathsf{AH}(\cdot))$$

For every entry in the $\mathcal{D}$ we have a chance of $10^{-2t\times n}$ for guessing correctly $\mathbf{s}_\ell$ i.e. the probability of existence of $\mathbf{s}_\ell$ in $\mathcal{D}$ will be as low as $10^{-2t\times n}$ and the probability of existence of all feature vectors k in $\mathcal{D}$ is $(k*10^{2t\times n})^{-1}$.

5.4. Birthday attack and effect on performance

Although the AH(·) function increases security, it is associated with a corresponding decrease in accuracy. We want to analyze what opportunities does it offer to an intruder to break the systems security. This scenario can be described by posing a question: given the near non-invertibility of AH(·), can the attacker deceive the biometric verification system using some other than the original biometric template as the query template? This can be assessed by calculating the probability of output collision for the

[2] For two independent random variables **x** and **y** we have $var(\mathbf{xy})=var(\mathbf{x})var(\mathbf{y})+var(\mathbf{x})E[\mathbf{y}]^2+var(\mathbf{y})E[\mathbf{x}]^2$ and for an i.i.d distribution $var(\sum_i\mathbf{x}_i)=\sum_i var(\mathbf{x}_i)$.

hash function AH(·). This type of vulnerability is known as the birthday attack due to its inherent similarity with the statistical problem of finding people in a group having identical birth dates.

If t is the digit length of each sample of the vector outcome of AH(·) then there are $q=10^t$ possible values for every sample $s_\ell^{*(i)}$. After r instances of hash values, the probability of no collision will be

$$P_{no\_coll}=\frac{q(q-1)(q-2)\ldots(q-(r-1))}{q^r}=\frac{q!}{q^r(q-r)!}$$

The higher values of q and lower r make the event of collision highly rare. The probability of atleast one collision among r instances is

$$P_{one\_coll}=1-\frac{q!}{q^r(q-r)!}$$

This relation can be expanded as $(1-x)$ factors that are related to their exponential form as $(1-x)\le e^{-x}$. Hence,

$$P_{one\_coll}>1-\exp\left(-\frac{1}{2q}(r\times(r-1)\right)$$

For any value p of P_{one_coll} we have number of instances given by

$$r=\sqrt{2\times q\times\ln\left(\frac{1}{1-p}\right)}$$

In our case, collision of one value by no means suffices the need of attacker. Rather the whole correct sequence of $\{s_\ell^i\}$ must be generated so that the desired sequence $\{\mathbf{s}_\ell\}$ can be obtained. This is implied as representing the possible outcomes as $q=10^{t\times n\times\eta}$. Here η is the strictness factor that decides the level of match between actual secured biometric and the item on the intruder's dictionary. Again, from the attacker's point of view the task is not yet finished. In order to generate all feature vectors the process in obtaining each $\mathbf{s}_\ell$ will have to be repeated k times, so the corresponding number of instances required (r) will be expressed as

$$r=\left(\sqrt{2\times q\times\ln\left(\frac{1}{1-p}\right)}\right)^k$$

As an example if we choose η to be 75%, $n=3\times10^2$, $t=5$, $k=20$ then $q\approx1\times10^3$ and $r\approx10^{650}$ [44].

5.5. Linkage attacks

Biometric template security systems can also become a victim of linkage attacks [37]. In this case, the adversary makes use of the leaked information when two different templates generated from the same biometric are compared. This comparison can be made either with or without (i.e. in $\mathbf{x}$ domain or in $\mathbf{s}^*$ domain respectively) inversion of the secured template. If only random projections are applied, partial recovery of original biometric data is possible and the intruder may enhance his/her knowledge by comparing partially recovered data ($\hat{\mathbf{x}}_1$ and $\hat{\mathbf{x}}_2$) from two instances of secured biometric ($\mathbf{s}_1^*$ and $\mathbf{s}_2^*$). However, after the application of AH(·) recovery of original data is highly infeasible, as shown in the security analysis of previous section. Therefore a comparison can be undertaken only in the transformed domain of $\mathbf{s}_\ell^*$ vectors. Since the transformed domain does not retain original biometric data, the best an intruder can get is a check to ascertain whether both templates belongs to the same user or not,

$$P(\mathcal{M}(\mathbf{s}^*,\hat{\mathbf{s}}^*)<\epsilon)$$

where $\mathcal{M}(\cdot)$ is the matching function and ϵ is the margin of permissible dissimilarity.

6. Case study: using dynamic handwritten signatures as biometric in KRP−AH framework

We have presented a secure authentication template generation scheme (KRP−AH) and built a TFA framework around it. We have also discussed possible attack situations and the performance of our system. In this section, we perform empirical validation of our claim that our proposed framework does not significantly undermine the discriminating features of genuine and forged signatures. To establish that the generated secure biometric templates are still highly usable for authentication purposes, we evaluate the proposed framework in a TFA setup using user passwords and dynamic handwritten signatures. Unlike the traditional feature transformation techniques, our system preserves the important biometric information even when the user specific password is compromised. We have identified a number of local and global features related to dynamic signatures for template generation, and we use Dynamic Time Warping and Mahalanobis Distance for matching of secure templates. We have evaluated the performance of the framework over two publicly available dynamic handwritten signature datasets. The results show that our proposed framework does not undermine the discriminating features of genuine and forged signatures.

6.1. Geometric normalization

To achieve good classification performance, all signatures are preprocessed to reduce the impact of undesired deviations (in geometry, size and spatial translation of different signature instances) on verification results. We have applied normalization by removing the spatial translation and angular rotation. The center of mass of signature contours are aligned as follows:

$$COM=\{x_{mean},y_{mean}\}=\frac{1}{N}\sum_{n=1}^{N}\{x_n,y_n\}$$

$$\{x_{shif},y_{shif}\}=\{x_n-x_{mean},y_n-y_{mean}\}\quad\forall n\in[1,N]$$

where N is the number of samples of signature data and x and y are the coordinates in cartesian plane. The average path tangent angle of complete signature contour is calculated and the amount of rotation is removed. In this way, the axis of least inertia gets aligned and average path tangent angle becomes zero:

$$\theta_{avg}=\frac{1}{N}\sum_{n=1}^{N}\tan^{-1}(\dot{y}_n/\dot{x}_n)$$

Here, $\dot{y}_n$ and $\dot{x}_n$ are the first order time derivatives of sequences $\{y_n\}_{1\times N}$ and $\{x_n\}_{1\times N}$ respectively.

6.2. Feature extraction

Signature verification can be considered as a two-class pattern recognition problem, where the authentic user is one class and all the forgers conform the second class. Feature extraction maximizes the discriminative capability of both classes. The features that we have extracted can be grouped into two major types: (i) local features and (ii) global features. The features in which a value is extracted for each sample point in the input domain are called as *local features*. *Global features* are the ones in which feature value is extracted for a whole signature, based on all sample points in the input domain [50,22].

6.2.1. Local features

The signatures used in our study are sampled at 100 Hz using a WACOM Intuos tablet (SVC2004 Dataset) or Interlink Electronics ePad-ink tablet (SUSig 2007 Dataset) and at 200 Hz using WACOM Intous3 tablet (SigComp 2011 Dataset). The local features are

Table 1
Local features: they capture dynamical information about handwritten signature signals. Top *five* rows list self-evident local features while the last four rows show features (*left column*) along with their definition (*right column*).

Time stamp (t)	Spatial co-ordinates ($\{x_n, y_n\}_{N\times 2}$)
Absolute speed ($\lvert s_n\rvert$)	Directional speed (s_n^x, s_n^y)
Absolute acceleration ($\lvert a_n\rvert$)	Directional acceleration (a_n^x, a_n^y)
Pen pressure (p_n)	Pressure deviation ($P_{max}-P_{min}$)
Azimuth angle (az_n)	Pen elevation (el_n)
Tangential acceleration	$\lvert a_{tn}\rvert = \dot{s}_n = dif\left(\sqrt{\dot{x}_n^2+\dot{y}_n^2}\right)$
Centripetal acceleration	$\lvert a_{cn}\rvert = s_n.\dot{\theta}_n, \quad \forall n \in [1,N]$
Path tangent angle	$\theta_n = \tan^{-1}\left(\frac{\dot{y}_n}{\dot{x}_n}\right) \quad \forall n \in [1,N]$
Log radius of curvature	$\delta_n = \log\left(\frac{s_n}{\dot{\theta}_n}\right) \quad \forall n \in [1,N]$

extracted at 100 Hz sampling frequency, which are listed in Table 1. In addition to these features, we also include first and second order time derivatives in the feature set. Derivatives are of paramount importance when the need is to capture distinctive characteristics of dynamic signals [50]. Instead of simple difference calculation for discrete signals, we have used second order regression to find derivatives [15]:

$$\dot{o}_n = \frac{\sum_{i=1}^{2} i(o_{n+i} - o_{n-i})}{2\cdot\sum_{i=1}^{2} i^2}. \tag{3}$$

6.2.2. Global features

Thirty five global features are calculated for each signature. These are listed in Table 2. The global feature 'Average Jerk' is the averaged rate of change of acceleration da/dt:

$$jerk_{avg} = \frac{1}{N}\sum_{n=1}^{N} \dot{a}_n \quad \forall n \in [1,N].$$

6.3. Distance measurement

The authentication decision is made by calculating two separate distance measures from local and global feature vectors of authentic and probe templates. It is necessary to treat the local and global feature vectors separately during distance measurement since local features are time varying signals in which each sample has a relation with adjacent samples. Therefore normal distance measurements like Euclidean, Manhattan, etc. cannot be applied for local features.

These distance measures are then fed to a random forest classifier that predicts the class to which the probe biometric belongs i.e. a genuine signature or an attempt of forgery. The choice of forest classifier is made due to its realtime performance and high accuracy. Fig. 6 shows this procedure as an access request scenario, where either the requested access is granted or denied depending upon the authenticity of the presented biometric. We now briefly discuss both distance calculation algorithms.

6.3.1. Dynamic time warping

DTW is based on dynamic programming and allows us to find a 'best path' that maximizes the local match between two aligned times series. The resulting similarity index calculated by the technique gives us a measurement that signifies the quality of match. DTW effectively minimizes the shifting in time and elastically transforms the time axis. Since we have time varying signature signals, we can use DTW as a metric to decide whether to accept or reject the query signature.

Table 2
Global features: they capture holistic information of handwritten signature signals. Each box contain a single feature definition.

Number of data points (N)	Average velocity
Avg. x velocity	Avg. y velocity
Max velocity	Avg. vel./max. vel.
Signature height (H)	Signature width (W)
Spread ratio (N/W)	Aspect ratio (W/H)
Variance of velocity	Variance of x velocity
Variance of y velocity	Sign changes in dx/dt
Sign changes in dy/dt	Average jerk
Max x velocity	Max y velocity
Average acceleration	Average x acceleration
Average y acceleration	Variance of acceleration
Variance of x acceleration	Variance of y acceleration
Average pressure	Average azimuth
Average elevation	Maximum pressure
Variance of pressure	Point of max. pressure
Max. acceleration	Pen up samples (N_u)
No. of points with positive x-velocity/N_u	
No. of points with negative y-velocity/N_u	
Deviation in pressure ($P_{max}-P_{min}$)	

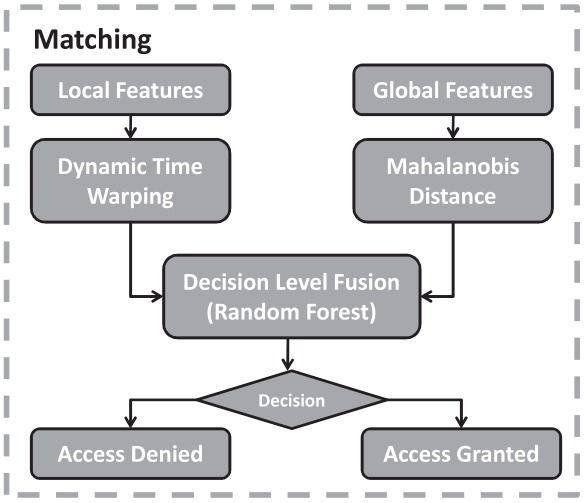

Fig. 6. Matching module.

If we have two random vectors which represent time series belonging to two different signature instances, $\mathbf{X} = [\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_F]^T \in \mathbb{R}^{d\times N_x}$ and $\mathbf{Y} = [\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_F]^T \in \mathbb{R}^{d\times N_y}$ where d is the total number of local dynamic features, N_x and N_y are the number of data points in equally sampled $\mathbf{X}$ and $\mathbf{Y}$ respectively. A distance matrix $\mathbf{U}$ is built to store local pairwise distances between $\mathbf{X}$ and $\mathbf{Y}$.

$$\mathbf{U} \in \mathbb{R}^{N_x\times N_y} : u_{ij} = \lVert \mathbf{x}_i^T - \mathbf{y}_j^T \rVert$$

where $i \in [1 : N_x]$, $j \in [1 : N_y]$. DTW warps $\mathbf{X}$ and $\mathbf{Y}$ such that the cost or distance function is minimized over alignment path (see Fig. 7):

$$\mathbf{P} = \mathcal{F}_{DTW}(\mathbf{X},\mathbf{Y}) = \underset{\mathbf{p_m}}{\operatorname{argmin}}\left(\sum_{m=1}^{M} \lVert \mathbf{x}_{p_m^x}^T - \mathbf{y}_{p_m^y}^T \rVert\right)$$

The warping path $\mathbf{P} = [\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_M]^T$ is calculated that consists of a pair of path vectors $\mathbf{p}_m = [p_m^x, p_m^y] \in \mathbb{R}^{M\times 2}$, where $p_m^x \in [1 : N_x]^{m\times 1}$ and $p_m^y \in [1 : N_y]^{m\times 1}$. The steps $m \in [1 : M]$ and M are the number of steps that are required to align two sequences in the minimum distance sense. $\mathbf{X}$ and $\mathbf{Y}$ can be aligned in a number of ways, exponential in N_x and N_y, however dynamic programming provides an efficient approach ($O(N_xN_y)$) to reach the desired minimum cost path using Bellman equations.

The warping path $\mathbf{P}$ must start and end with the bounded points of two signatures. During alignment steps, time ordering of

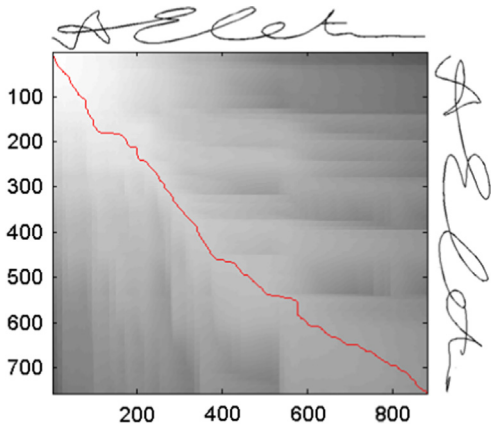

Fig. 7. Local pairwise distances between two secure signatures templates.

sequences is retained and jumps are taken in accordance with some predefined policy $\xi(\cdot)$. We have tested the system with two types of policy functions: unconstrained policy (ξ_u) and greedy policy (ξ_g). ξ_u encompasses 5 steps:

$$\xi_u : \{(i+1,j),(i,j+1),(i+1,j+1),(i+2,j+1),(i+1,j+2)\}$$

while the ξ_g consists of 3 steps:

$$\xi_g : \{(i+1,j+1),(i+2,j+1),(i+1,j+2)\}$$

Equal weights are assigned to all movements in both ξ_u and ξ_g. We tested with both policy functions and found them identical in relation to the verification performance.

6.3.2. Mahalanobis distance

This distance measure is used for distance calculation between global feature vector of each signature. This choice is based on the premise that different global features are distributed with different statistical properties (variances and means). For each user k we have,

$$\mathbf{G}_i = [\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_k, \ldots, \mathbf{g}_K], \quad \text{where } k \in [1, K]$$

Distance calculation is based on correlations between variables and is scale invariant as desired in our application,

$$d_k^{ij} = \sqrt{(\mathbf{g}_k^i - \mu_k)^T \sigma_k^{-2} (\mathbf{g}_k^j - \mu_k)}$$

An averaging function is applied on distance vector; $\mathbf{d^{ij}} = [d_1^{ij}, d_2^{ij}, \ldots, d_K^{ij}]$ which does not create a bias in verification decision due to normalization characteristic of Mahalanobis distance,

$$\Lambda_{ij} = \sum_{k=1}^{K} d_k^{ij}/K, \quad i,j \in [1, \text{ no. of users}], \; k \in [1, K].$$

6.4. Decision making

A decision level fusion of both distance measurement algorithms (DTW for local and Mahalanobis distance for global features) is performed using a Random Forest classifier (RFC). This classification algorithm creates an ensemble of trees and then decides the input class using the votes from each tree. RFC provides us with very fast ($\sim$2.8 ms for each signature on average) decision support and works well when enough signature samples are available for training.

6.5. Performance evaluation

Now, we present the empirical results of our case study. First, we describe the datasets used in our experiments. Then, we define the performance metrics used for evaluation. Afterwards, we present the actual performance evaluation results in term of the performance metrics.

6.5.1. Datasets

For the purpose of evaluation of our scheme, we have run tests on three publicly available dynamic signature datasets. On the whole, these datasets comprise of $\sim$8100 signatures, of which there are $\sim$3600 forged and $\sim$4500 are genuine signatures. The important statistics of these datasets are briefly described below.

SVC 2004: This dataset was collected as a part of First International Signature Verification Competition (SVC), 2004. The data set contains signatures for two tasks, each containing data for 100 users. However, the data of only 40 users is released publicly for each of the two tasks. Each user data is further divided into 20 genuine and 20 skilled forgeries. For first task, data of only x and y coordinates, pen-up/pen-down and time stamp are included. The second task data contains some extra dynamic information including pressure, elevation and azimuth angles indicating pen orientation. SVC 2004 is a widely used benchmark database for testing on-line signature verification systems [57].

SUSig 2007: The SUSig dataset contains signatures of 100 different users. Among them, there are 29 female and 71 male subjects. This dataset is divided into two parts, visual sub-corpus and blind sub-corpus. There are 20 genuine signatures collected from each user in visual sub-corpus while 10 forgeries are also included for each user. In blind sub-corpus, 10 genuine and 10 forgeries are there for each user. Data for each signature include $x-y$ co-ordinates, pressure and pen-up/pen-down events with time stamp. To collect skilled forgeries, an animated signing simulation module is used [24].

SigComp 2011: This dataset was released as part of Signature Verification Competition (SigComp 2011) for online skilled forgeries. It consists of two sub-corpses, containing Chinese and Dutch handwritten signatures respectively. The dynamic signature data includes x, y and z coordinates and do not contain pressure signal. Chinese dataset contains 1339 online signatures in total while 2356 signatures are present in dutch datset. Chinese subcorpus includes data from 20 users and dutch subcorpus includes data from 64 users. All signatures are collected at 200 Hz using WACOM Intuos3 A3 Wide USB Pen Tablet [32].

6.5.2. Performance metrics

We can define measures of performance in probabilistic terms. The probability of FAR is

$$P_{FAR} = Pr[\{\mathsf{AH}(\mathcal{F}_{sec}(\mathcal{F}_{feat}(\mathbf{Y}))), \mathcal{F}_{kdf}(\mathbf{k_Y})\} \approx \{\mathsf{AH}(\mathcal{F}_{sec}(\mathcal{F}_{feat}(\mathbf{X}))), \mathcal{F}_{kdf}(\mathbf{k_X})\}]$$

where $\mathbf{Y}$ and $\mathbf{X}$ are copies of same biometric from two different users. When we have a second copy $\hat{\mathbf{X}}$ of same bio-metric trait from the same user, we may define FRR as

$$P_{FRR} = Pr[\{\mathsf{AH}(\mathcal{F}_{sec}(\mathcal{F}_{feat}(\hat{\mathbf{X}}))), \mathcal{F}_{kdf}(\mathbf{k}_{\hat{\mathbf{X}}})\} \neq \{\mathsf{AH}(\mathcal{F}_{sec}(\mathcal{F}_{feat}(\mathbf{X}))), \mathcal{F}_{kdf}(\mathbf{k_X})\}]$$

We choose the *Equal Error Rate (EER)* point as the operating point of our framework. As the name suggests, EER is the point on Receiver Operating Characteristic (ROC) curve where FAR and FRR rates are equal. The performance results of our framework are presented using this metric.

6.5.3. Experiments and verification results

On both of these datasets, training is performed on 5 genuine signatures. The best signature is chosen as a reference signature depending upon the minimum distance with all other genuine

Table 3
Evaluation of authentication performance.

Datasets	k	KRP (·)	AH (·)	EER (%)
SVC 2004	30	✓	×	3.40
		✓	✓	4.84
	20	✓	×	4.37
		✓	✓	6.21
SUSig 2007	30	✓	×	3.68
		✓	✓	4.47
	20	✓	×	4.15
		✓	✓	5.05
SigComp 2011	30	✓	×	5.26
		✓	✓	6.03
	20	✓	×	6.69
		✓	✓	7.28

signatures in the training set. During the testing phase, performance is evaluated against only skilled forgeries. Each of the signature from probe bio-metric set is matched with the reference genuine signature and the decision about its authenticity is made. We have used 10-fold cross validation to assess how the predictive model will perform in actual practice, irrespective of the type of training set.

The results for our experiments on SVC, SUSig and SigComp datasets are shown in Table 3. The system is tested with different values of k (accounting for the amount of dimensionality reduction) to observe how the level of compression affects verification results. A decrease in performance is noted when the amount of compression is increased, which is consistent with the results found in [52]. However the level of degradation is not much significant when compared to the amount of dimension reduction (i.e. 77% and 51% in case of $k=30$ and $k=20$ respectively). The effect of applying AH(·) is also studied while evaluating system performance. Due to the trade-off between security and performance levels, a decrease in system efficiency is expected after the arithmetic hashing. However, the decline is not large if we keep in view the benchmark results reported on these data-sets (SVC: EER averaged on both tasks; $6.2 \pm 8.59\%$ [51], SUSIG: EER equals $4.08 \pm 19.1\%$ [23] and SigComp: EER avergaed on both Chinese and Dutch sub-corpses; 5.24 [32]). The ROC curves are plotted in Fig. 8.

We observe that the EER of our system is maximum when both KRP and AH are used. However even for low value of $k=20$, the maximum EER is comparable to the previous state-of-the-art results on signature datasets. This low error rate demonstrates that unlike the traditional feature transformation techniques, our system preserves the important biometric information even when the user specific password is compromised. This validates our hypothesis that KRP−AH framework does not significantly undermine the discriminating features of genuine and forged signatures.

Table 4 reports the comparisons when different transformation functions are used in place of AH. For *Discriminability Preserving Transform* (DPT) [13], each feature is divided into 3 windows (w). The verification accuracy is reported by matching signatures using normalized hamming distance. For Convolution Function Transform (CFT) [35], 120 distinguishing points (d) are chosen for each signature and matching for transformed signatures is performed using DTW. It turns out that when DPT and CFT are used in place of AH, the verification accuracy is severely degraded.

7. Discussion

There are a plethora of biometric verification schemes used in industry. We specifically focus on the security of handwritten signatures because they are widely acceptable, easily revocable and are now more suitable than ever due to the increasing availability of touch screen (or stylus) based computing devices. However, it turns out that there are very few industrial methods which provide mechanisms for securing biometric templates of handwritten signatures. In the following discussion, we outline some industrial solutions and provide a comparison with our scheme:

1. American Health Information Management Association (AHIMA) outlines the use of online hand-written signatures but does not give any hint about whether and how the biometric template security will be ensured. Rather they recommend cryptographic signature (a digital/electronic key) as a good alternative to handwritten signature due to its security strength [2].
2. Malik et al. [36] report an industrial solution to the problem of on-line signature verification using Anoto digital pen. Their approach extracts a number of features and employ GMM for classification. The signature templates in the form of GMM descriptions are stored on the electronic cards and thus provide secure storage. However, at the test time a genuine signature is directly used for comparison and is thus vulnerable to attacks. Moreover, their approach is not robust to birthday attacks where they can reach to similar GMM descriptions (esp. when the number of Gaussians is low) with different feature values.
3. WonderNet [43] is an online service which enables users to sign documents using handwritten signatures. However, no mechanism to secure biometric templates is mentioned.
4. Right Signature [40] is another signature service which is integrated with EverNote to digitally sign documents. Because, they focus on authenticating documents and not on verifying users based on their signatures, no template level security is provided. They use standard cryptographic techniques such as 256 bit EV SSL encryption. Note that we want to do signature level matching for which standard encryption techniques are not suitable because they do not retain intra-person variations (Section 1). Other similar services available include DocuSign [39], Silanis e-Signatures [41]. However, none of them provide template level security for handwritten signatures.
5. SOFTPRO [42] provides a signature verification service based on DTW, which is similar to local feature matching part of our verification framework. However, they also do not mention any security measure to protect biometric data against any possible data leak.
6. A recent system [53] uses simple dynamical features of on-line signatures and handwriting for verification purposes. But again, no security measures are discussed to protect signature templates.

In comparison to the above-mentioned methods, our approach provides template-level security for handwritten signatures and proposes a verification scheme to validate query biometrics in the transformed domain. Regarding the authentication set-up, our approach can be used to validate personal cards (e.g. smart cards) that provide crucial functions (e.g. financial transactions) or carry data worthy of protection (e.g. private medical data). The transformed genuine biometric template will be stored on the card to ensure security. Note that such biometric information is already in use (e.g., Spanish police uses handwritten signature biometrics stored on National ID cards to verify person's identity; Henniger and Müller [18] report extensive real life card matching experiments using handwritten signatures). However unlike our approach, the stored biometric templates are not secured and an attacker can recover original signature from stored features.

Finally, our approach is also perfectly suitable to be deployed as a software based service (SaaS) on cloud. In this way, enterprises

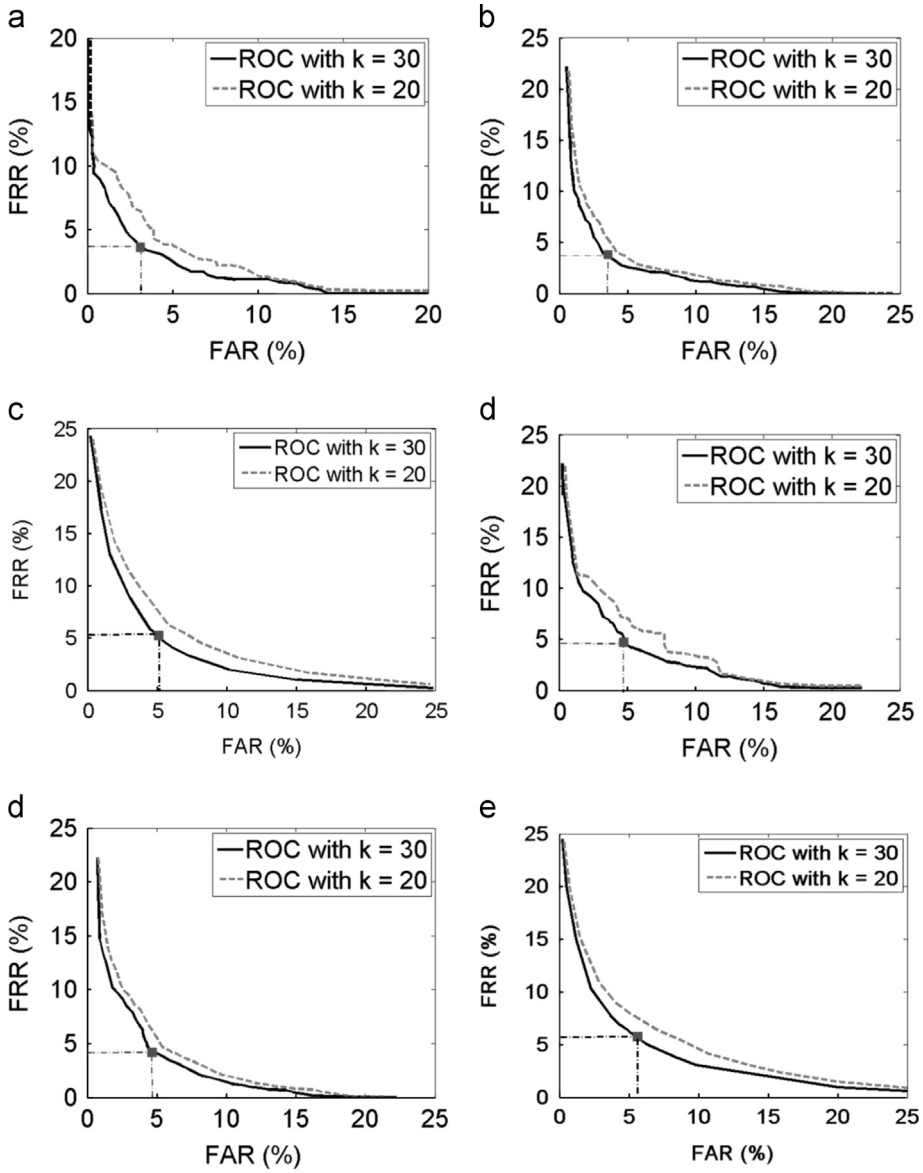

Fig. 8. ROC results for the SVC'04, SUSIG'07 and SigComp'11 datasets. (a) Using KRP (SVC), (b) using KRP (SUSig), (c) using KRP (SigComp), (d) using KRP-AH (SVC), (e) using KRP-AH (SUSig) and (f) using KRP-AH (SigComp).

Table 4
Comparison of verification accuracy on SVC 2004 dataset when different transformation functions are used.

Transform	KRP $k=30$	KRP-AH $k=30$	KRP-DPT [13] $d=120$	KRP-CFT [35] $w=3$
EER (%)	3.40	4.84	18.99	15.23

will be able to store and authenticate private data of their clients in a secure manner.

8. Conclusion

In this paper, we have presented a secure and efficient framework that employs a novel scheme comprising random projections of biometric data (inherence factor) using secure keys derived from passwords (knowledge factor) to generate inherently secure, efficient and revocable/renewable biometric templates for user verification. We have discussed the security strength of the framework against possible attacks. We perform a case study of the proposed framework in a TFA setup using user provided passwords and dynamic handwritten signatures. Unlike the traditional feature transformation techniques, our system preserves the important biometric information even when the user specific password is compromised. We have evaluated the performance of the framework over three publicly available signature datasets. The results show that our proposed framework does not significantly undermine the discriminating features of genuine and forged signatures.

Conflict of interest

None declared.

Acknowledgments

The work presented in this paper is supported by the National ICT R&D Fund, Ministry of Information Technology, Government of Pakistan. The information, data, comments, and views detailed

herein may not necessarily reflect the endorsements of views of the National ICT R&D Fund.

References

[1] T. Ahmad, J. Hu, S. Wang, Pair-polar coordinate-based cancelable fingerprint templates, Pattern Recognit. 44 (2011) 2555–2564.
[2] American Health Information Management Association, Electronic Signature, Attestation and Authorship: Appendix c, 2009.
[3] K.J. Anil, N. Karthik, N. Abhishek, et al., Biometric template security, EURASIP J. Adv. Signal Process. (2008), http://dx.doi.org/10.1155/2008/579416.
[4] E. Argones Rua, E. Maiorana, J. Alba Castro, P. Campisi, Biometric template protection using universal background models: an application to online signature, IEEE Trans. Inf. Forens. Secur. 7 (2012) 269–282.
[5] R. Baraniuk, M. Davenport, R. DeVore, M. Wakin, A simple proof of the restricted isometry property for random matrices, Construct. Approx. 28 (2008) 253–263.
[6] J. Brodkin, Dropbox Confirms It Got Hacked, Will Offer Two-Factor Authentication, 2013, ⟨http://arstechnica.com/security/2012/07/dropbox-confirms-it-got-hacked-will-offer-two-factor-authentication/⟩, Online (accessed 18.11.13).
[7] R. Cappelli, A. Lumini, D. Maio, D. Maltoni, Fingerprint image reconstruction from standard templates, IEEE Trans. Pattern Anal. Mach. Intell. 29 (2007) 1489–1503.
[8] S. Dasgupta, A. Gupta, An elementary proof of a theorem of Johnson and Lindenstrauss, Random Struct. Algorithms 22 (2002) 60–65.
[9] D. Donoho, For most large underdetermined systems of linear equations the minimal 1-norm solution is also the sparsest solution, Commun. Pure and Appl. Math. 59 (2006) 797–829.
[10] D. Donoho, Y. Tsaig, I. Drori, J. Starck, Sparse solution of underdetermined systems of linear equations by stagewise orthogonal matching pursuit, IEEE Trans. Inf. Theory 58 (2012) 1094–1121.
[11] D.L. Donoho, Compressed sensing, IEEE Trans. Inf. Theory 52 (2006) 1289–1306.
[12] R. Dragusin, Data Breach at IEEE. org: 100k Plaintext Passwords, 2013, ⟨http://ieeelog.com⟩, Online (accessed 18.11.13).
[13] Y. Feng, P. Yuen, A. Jain, A hybrid approach for generating secure and discriminating face template, IEEE Trans. Inf. Forens. Secur. 5 (2010) 103–117.
[14] FFIEC, Ffiec Releases Guidance on Authentication in Internet Banking Environment, 2005, ⟨http://www.ffiec.gov/press/pr101205.htm⟩.
[15] J. Fierrez, J. Ortega-Garcia, D. Ramos, J. Gonzalez-Rodriguez, Hmm-based on-line signature verification: feature extraction and signature modeling, Pattern Recognit. Lett. 28 (2007) 2325–2334.
[16] P. Frankl, H. Maehara, The Johnson–Lindenstrauss lemma and the sphericity of some graphs, J. Comb. Theory, Ser. B 44 (1988) 355–362.
[17] S. Gina, 450k Yahoo Passwords Online Now: Is Yours?, 2013, ⟨http://www.techrepublic.com/blog/security/450k-yahoo-passwords-online-now-is-yours/8097⟩, Online (accessed 18.11.13).
[18] O. Henniger, S. Müller, Handwritten signature on-card matching performance testing, in: Biometric ID Management and Multimodal Communication, Springer, Berlin Heidelberg, 2009, pp. 268–275.
[19] A.K. Jain, K. Nandakumar, Biometric authentication: system security and user privacy, IEEE Comput. 45 (2012) 87–92.
[20] S. Jassim, H. Al-Assam, H. Sellahewa, Improving performance and security of biometrics using efficient and stable random projection techniques, in: Proceedings of 6th International Symposium on Image and Signal Processing and Analysis (ISPA 2009), IEEE, Salzburg, Austria, 2009, pp. 556–561.
[21] P. Kamp, P. Godefroid, M. Levin, D. Molnar, P. McKenzie, R. Stapleton-Gray, B. Woodcock, G. Neville-Neil, Linkedin password leak: salt their hide, Queue 10 (2012) 20.
[22] S. Khan, Z. Khan, F. Shafait, Can signature biometrics address both identification and verification problems?, in: 12th International Conference on Document Analysis and Recognition (ICDAR), 2013, pp. 981–985.
[23] A. Kholmatov, B. Yanikoglu, Realization of correlation attack against the fuzzy vault scheme, in: Electronic Imaging 2008, International Society for Optics and Photonics, San Jose (CA) United States, 2008, pp. 68190O–68190O.
[24] A. Kholmatov, B. Yanikoglu, Susig: an on-line signature database, associated protocols and benchmark results, Pattern Anal. Appl. 12 (2009) 227–236.
[25] Y. Kim, A.B.J. Teoh, K.A. Toh, A performance driven methodology for cancelable face templates generation, Pattern Recognit. 43 (2010) 2544–2559.
[26] A. Kong, D. Zhang, M. Kamel, Three measures for secure palmprint identification, Pattern Recognit. 41 (2008) 1329–1337.
[27] F. Krahmer, R. Ward, New and improved Johnson–Lindenstrauss embeddings via the restricted isometry property, SIAM J. Math. Anal. 43 (2011) 1269–1281.
[28] H. Lee, C. Lee, J. Choi, J. Kim, J. Kim, Changeable face representations suitable for human recognition, Adv. Biom. (2007) 557–565.
[29] L. Leng, J. Zhang, M. Khan, X. Chen, M. Ji, K. Alghathbar, Cancelable palmcode generated from randomized Gabor filters for palmprint template protection, J. Sci. Res. Essays 6 (2011) 784–792.
[30] M.H. Lim, A.B.J. Teoh, K.A. Toh, An efficient dynamic reliability-dependent bit allocation for biometric discretization, Pattern Recognit. 45 (2012) 1960–1971.
[31] K. Liu, H. Kargupta, J. Ryan, Random projection-based multiplicative data perturbation for privacy preserving distributed data mining, IEEE Trans. Knowl. Data Eng. 18 (2006) 92–106.
[32] M. Liwicki, M.I. Malik, C.E. van den Heuvel, X. Chen, C. Berger, R. Stoel, M. Blumenstein, B. Found, Signature verification competition for online and offline skilled forgeries (sigcomp2011), in: International Conference on Document Analysis and Recognition (ICDAR), IEEE, Beijing, China, 2011, pp. 1480–1484.
[33] D. Maio, A.K. Jain, Handbook of Fingerprint Recognition, Springer, Berlin Heidelberg, 2009.
[34] E. Maiorana, Biometric cryptosystem using function based on-line signature recognition, Expert Syst. Appl. 37 (2010) 3454–3461.
[35] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, A. Neri, Template protection for hmm-based on-line signature authentication, in: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW'08), IEEE, Anchorage, Alaska, USA, 2008, pp. 1–6.
[36] M.I. Malik, S. Ahmed, A. Dengel, M. Liwicki, A signature verification framework for digital pen applications, in: 10th IAPR International Workshop on Document Analysis Systems (DAS), IEEE, Queensland, Australia, 2012, pp. 419–423.
[37] A. Nagar, K. Nandakumar, A. Jain, Biometric template transformation: a security analysis, in: Proceedings of the SPIE, Electronic Imaging, Media Forensics and Security, 2010.
[38] B. News, Twitter: Account Hack Affects 250,000 Users, 2013, ⟨http://www.bbc.co.uk/news/technology-21304049⟩, Online (accessed 02.10.13).
[39] Online, 2014a. Docusign, URL: ⟨https://www.docusign.com.au/⟩.
[40] Online, 2014b. Right Signature: Easy Online Document Signing, URL: ⟨https://rightsignature.com/⟩.
[41] Online, 2014c. Silanis e-Signatures, URL: ⟨http://www.silanis.com/⟩.
[42] Online, 2014d. Softpro: The Signature Professionals, URL: ⟨http://www.softpro.de/en/⟩.
[43] Online, 2014e. Wondernet: Authentic e-Signatures, URL: ⟨http://www.wondernet.co.il/⟩.
[44] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, Physical one-way functions, Science 297 (2002) 2026–2030.
[45] V. Patel, R. Chellappa, M. Tistarelli, Sparse representations and random projections for robust and cancelable biometrics, in: 11th International Conference on Control Automation Robotics and Vision (ICARCV), IEEE, 2010, pp. 1–6.
[46] A. Peressini, F. Sullivan, J. Uhl Jr., The Mathematics of Nonlinear Programming, Springer-Verlag, New York, Inc., 1988.
[47] F. Quan, S. Fei, C. Anni, Z. Feifei, Cracking cancelable fingerprint template of ratha, in: International Symposium on Computer Science and Computational Technology (ISCSCT'08), IEEE, Shanghai, China, 2008, pp. 572–575.
[48] Y. Rachlin, D. Baron, The secrecy of compressed sensing measurements, in: 46th Annual Allerton Conference on Communication, Control, and Computing, IEEE, Monticello, IL, USA, 2008, pp. 813–817.
[49] N. Ratha, S. Chikkerur, J. Connell, R. Bolle, Generating cancelable fingerprint templates, IEEE Trans. Pattern Anal. Mach. Intell. 29 (2007) 561–572.
[50] J. Richiardi, H. Ketabdar, A. Drygajlo, Local and global feature selection for on-line signature verification, in: Proceedings of the Eighth International Conference on Document Analysis and Recognition, IEEE, Seoul, South Korea, 2005, pp. 625–629.
[51] SVC, Signature Verification Competition, 2004, ⟨http://www.cse.ust.hk/svc2004/results.html⟩.
[52] A. Teoh, A. Goh, D. Ngo, Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs, IEEE Trans. Pattern Anal. Mach. Intell. 28 (2006) 1892–1901.
[53] P. Thumwarin, J. Pernwong, T. Matsuura, Fir signature verification system characterizing dynamics of handwriting features, EURASIP J. Adv. Signal Process. 2013 (2013) 1–15.
[54] U. Uludag, S. Pankanti, S. Prabhakar, A. Jain, Biometric cryptosystems: issues and challenges, Proc. IEEE 92 (2004) 948–960.
[55] A. Vetro, S.C. Draper, S. Rane, J. Yedidia, Securing biometric data, Distrib. Source Coding (2009) 293–323.
[56] S. Wang, J. Hu, Design of alignment-free cancelable fingerprint templates via curtailed circular convolution, Pattern Recognit. 47 (2014) 1321–1329.
[57] D. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto, G. Rigoll, Svc2004: first international signature verification competition, Biom. Authent. 5 (2004) 179–208.

Salman H. Khan is a Ph.D. candidate at the School of CSSE, The University of Western Australia, Crawley WA 6009. He obtained his bachelor's in Electrical Engineering from College of EME, National University of Sciences and Technology (NUST), with high distinction. He was awarded several prestigious scholarships such as the Fulbright Scholarship for Master Studies and the International Postgraduate Research Scholarship at UWA. He worked with several research groups including Research laboratory of Communications and Networking (CoNNekT) at School of Electrical Engineering and Computer Science (SEECS), NUST; Human Systems Laboratory, School of Mechanical and

Manufacturing Engineering (SMME), NUST and Next Generation Intelligent Networks Research Center (nexGIN RC), Islamabad. His research interests include biometrics, visual scene understanding and bionic vision.

M. Ali Akbar received his B.E. degree in Electrical Engineering from National University of Sciences and Technology (NUST), Pakistan, in 2008. He worked on VoIP security for 3 years at Next Generation Intelligent Networks Research Center (nexGIN RC), Islamabad, Pakistan. He completed his M.S. in Computer Science with specialization in Computer Security from Columbia University, NY, in 2011. He also worked on penetration testing of a number of smartphone applications at Cigital NY. He is now working as an Information Security Consultant and Smartphone Development Manager at nexGIN RC, Islamabad, Pakistan. He has over 4 years of experience in the fields of software development, mobile application development, and penetration testing of web and smartphone applications. He loves reviewing code for security vulnerabilities and breaking applications through penetration testing. His research interests include information and communications security, privacy and anonymity, wireless communication, machine learning, smartphone security, information assurance, and security aware web and mobile applications design (Web: http://www.muhammadakbar.com).

Farrukh Shahzad received his BCS (Honors) degree from Hamdard University Karachi, Pakistan, in 1999, He completed his M.S. degree in Computer Engineering (CE) from the University of Engineering and Technology Taxila, Pakistan, in 2006. He got his Ph.D. in Electrical Engineering (EE) from National University of Computer and Emerging Sciences (FAST-NUCES) Islamabad, Pakistan, in 2014. In 2000, he joined Elixir Technologies Pvt. Ltd., Pakistan as a software engineer and worked in the areas of Enterprise database applications and printing streams based applications for heavy duty printers. From 2004 to 2008, he worked as team lead and software architect for Interactive Group Pvt. Ltd., Pakistan – in the area of multimedia applications design and development. In 2008, he joined Next Generation Intelligent Networks Research Center (nexGIN RC), Islamabad as a project manager, software architect and researcher. Currently, he is working as Principal Researcher in Ebryx (Pvt) Ltd. Pakistan. His research area encompasses non-signature base, intelligent and self-healing security solutions for smart phones and desktop operating systems, data mining and evolutionary algorithms.

Mudassar Farooq received his B.E. degree in Avionics Engineering from National University of Sciences and Technology (NUST), Pakistan, in 1996. He completed his M.S. in Computer Science and Engineering from University of New South Wales (UNSW), Australia, in 1999. He completed his D.Sc. in Informatics from Technical University of Dortmund, Germany, in 2006. In 2007, he joined the National University of Computer and Emerging Sciences (NUCES), Islamabad, Pakistan, as an associate professor. Currently, he is working as Dean, Institute of Space Technology (IST) and Director of Next Generation Intelligent Networks Research Center (nexGIN RC) at IST. He is the author of the book "Bee-inspired Protocol Engineering: from Nature to Networks" published by Springer in 2009. He has also has co-authored two book chapters in different books on swarm intelligence. He is on the editorial board of Springer Journal of Swarm Intelligence. He is also the workshop chair of European Workshop on Nature inspired Techniques for Telecommunication and Networked Systems (EvoCOMNET) held with EuroGP. He also serves on the PC of well-known EC conferences like GECCO, CEC, ANTS. He is the guest editor of a special issue of Journal of System Architecture (JSA) on Nature inspired algorithms and applications. His research interests include agent based routing protocols for fixed and mobile ad hoc networks (MANETs), nature inspired applied systems, natural computing and engineering and nature inspired computer and network security systems, i.e. artificial immune systems.

Zeashan Khan received his Ph.D. in Automatic Control from University of Grenoble, France in 2010. Since then, he is actively collaborating in research as well as working as a full-time faculty at Department of Electrical Engineering, Faculty of Engineering and Applied Sciences, Riphah International University, Islamabad, Pakistan. His research interests include Image Processing, Computer Vision, Soft Computing, Cyber Physical Systems, Fault detection and Fault tolerant control etc. He has published several research papers in IEEE Conferences and international journals. He is a member of IEEE (USA) and SEE (France).