IEEE TRANSACTIONS ON
EMERGING TOPICS
IN COMPUTING

Received 22 February 2018; revised 30 July 2018; accepted 5 August 2018.
Date of publication 22 October 2018; date of current version 3 March 2021.

Digital Object Identifier 10.1109/TETC.2018.2865345

Automatic Signature Verification in the Mobile Cloud Scenario: Survey and Way Ahead

DONATO IMPEDOVO, (Senior Member, IEEE) AND GIUSEPPE PIRLO, (Senior Member, IEEE)

The authors are with the Department of Computer Science, University of Bari, Bari 70125, Italy.
CORRESPONDING AUTHOR: D. IMPEDOVO (donato.impedovo@uniba.it)

ABSTRACT On-line signature verification is typically carried out with the use of digitizing tablets specifically designed for the aim. So far, stand-alone systems have been mainly inspected, but the current distributed/cloud scenario and the amount of mobile devices in everyday life is calling for a new challenge. Within this scenario, signatures are acquired around the world with different kinds of devices and processed on multiple platforms in order to be verified. Through the paper, the different phases of the signature verification process in the new scenario are presented and the most valuable results are discussed considering the following aspects: accessibility and usability, interoperability, security and performance. Achievements as well as weakness are focused to highlight promising directions for further research and technology development.

INDEX TERMS Biometrics, handwritten signature verification, mobile applications, acquisition devices, cloud computing, interoperability, signature template security

I. INTRODUCTION

Handwritten signature is a well-established mean for personal identification the use of which is well recognized by administrative and financial institutions [98]. Nowadays, digital signature devices, specifically designed for the aim, are increasingly used in the commercial and banking sector, with the aim to facilitate payments and transactions, as well as in many other sectors, e.g., e-government, healthcare, education and express courier.

General state-of-the-art papers dealing with handwritten signature verification have been published in 1989 [74], in 2000 [76] and 2008 [39]. Within these works, signatures have been considered acquired by means of digitizing tablets, provided with *ad hoc* pen stylus, specifically designed for the aim. At the same time, stand-alone verification systems have been mainly inspected. In the last 10 years the contour technologic scenario is changed, and the field of handwriting signature verification cannot avoid considering the cloud (distributed) computing and the amount of mobile devices used in everyday life. Within this scenario, signatures can be acquired around the world with different kinds of devices (specifically devoted and/or mobile) and processed at different stages on multiple and distributed platforms to be verified. In fact, even if Narayanaswamy *et al*. [64] were among the first in 1999 to consider signature verification on mobile phones, it is only in the last years that the technological development and sustainable costs have enabled a wide spread of such devices. This paper intends to describe the signature verification process within this new challenging scenario: mobile devices and cloud (distributed) computing.

It must be argued that an on-line signature verification within this scenario is quite different from the traditional one and the application of already known solutions (in the form they are) will result in many fails. In fact, in this context, the signature is also intended to be part of a remote authentication process (similar to retina scan authentication or even $\mathrm{username} + \mathrm{password}$). In other words, the signature has the aim of demonstrating the willing of the writer in signing the document as well as her/his identity.

Given the previous, general issues regarding biometric authentication, template protection and secure infrastructure can be considered [77], [86]. On the other hand, signature verification raises specific issues here discussed. Handwritten signature is placed within the set of behavioural biometrics: the acquisition device measures the result of an action (i.e., signing process) performed by the user. Three major components are conveyed within the signing process:

- Physiologic component: the writing system (i.e., arm, wrist, hand, fingers, etc.);
- Learned component: signature is personalized over time and it embeds many aspects related to schooling, culture and habits;

2168-6750 © 2018 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications/rights/index.html for more information.

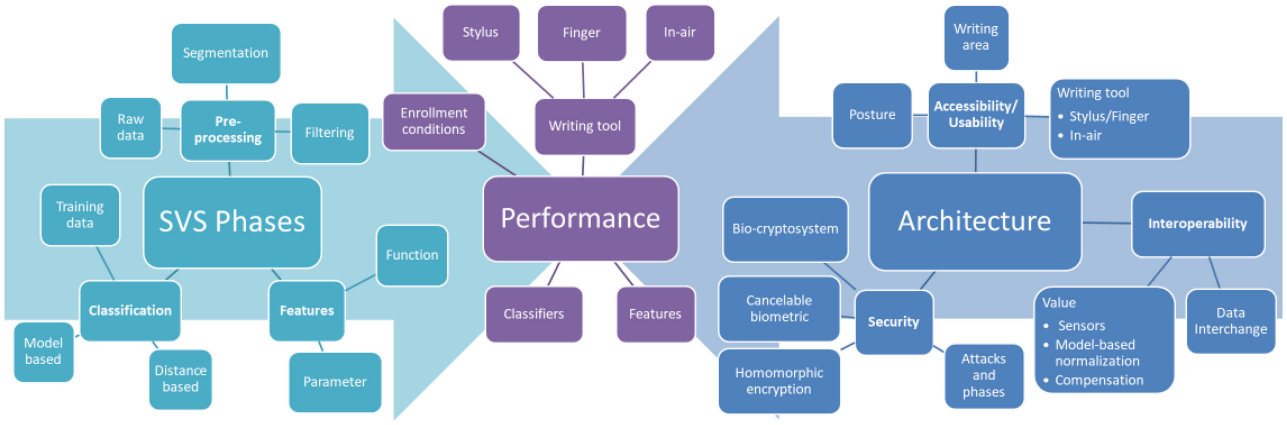

FIGURE 1. **Taxonomy and organization of the paper.**

- Contour contingent component: given the above, some noise is introduced due to the writing device, posture, spatial constrains, number of the signature written the specific session and emotional state.

The mobile signature issue mainly deals with the last aspect. In fact, mobile devices have, in general, very variable input area (i.e., screen size), a poor sampling frequency if compared to specifically devoted pad devices (e.g., 60Hz for a smartphone vs. 200Hz for a specific designed device) as well as spatial pixel density (e.g., 150dpi in the case of a smartphone vs. 1000dpi in the case of a professional device). Different sensing technologies must be considered: capacitive (e.g., most part of smartphones and tablets), resistive (in general less sensitive than a capacitive one), optical, infrared (no more used) and electromagnetic (adopted by professional signature pads). Moreover, only specifically devoted pads and a very reduced set of mobile devices are provided with a stylus, so that signatures are written using a finger.

The posture plays an important role: when using a specifically designed pad, the user is expected to be sitting or to standing. A mobile scenario includes many other possibilities: signing while moving, or while hand-holding the device at different angles and orientations [2], [83], [84].

The aim of this work is to provide a comprehensive research and technologic view of the field, developing a perspective on the area. Reviewed papers have been categorized according the taxonomy reported in Figure 1 which also reflect the organization of the paper. The SVS Area takes into account the typical phases of a signature verification system: data acquisition and pre-processing, feature extraction and classification. This has been specialized in the direction of the scenario of interest and it is reported in Section II. The Architecture area reflects new structural aspects of the signature verification process: accessibility/usability of acquisition devices, interoperability of systems at different stages and security of data (signature). Those aspects are discussed in Section III. Topics of these two areas intersect each other many times. For example, security can be performed at feature level by means of non-invertible features or at model level, some features are influenced by usability aspects (e.g., velocity feature is influenced by the signing area), etc.. Both the previous areas strongly determine performance of the system which are discussed in Section IV. Finally, Section V concludes the paper summarizing directions for further research in the field.

II. THE PROCESS OF DYNAMIC SIGNATURE VERIFICATION

On-line automatic signature verification involves three main phases: data acquisition and pre-processing, feature extraction and verification [75]. The acquisition device produces electronic signals named raw data, representative of the signature and captured during the writing process. In the pre-processing phase, the enhancement of the input data is generally based on filtering, noise reduction, smoothing and signature normalization. Function features or parameter features are extracted in the feature extraction phase, so that specific characteristics of the signature can be described. Verification is used to evaluate the authenticity of the test signature by matching its features against those stored in the knowledge base and developed during the training stage. A standard all-in-one application has the execution of the three phases on the same device being a self-consistent system. Within the cloud scenario, the three fundamental steps must be further decomposed and placed on a distributed architecture. The overall process is depicted in Figure 2. Each one of the different steps reported in Figure 2 can be (theoretically) performed and/or located on different devices and/or servers. More specifically, light blue colored boxes are expected to be performed on the acquisition device (mobile or specifically devoted pads), lilac colored boxes can be performed on the acquisition device and/or on the server depending upon the specific pre-processing step. Grey colored boxes are typically performed on a server, however modules (feature extraction, training, etc.) could be also deployed on a distributed architecture.

A. DATA ACQUISITION AND PREPROCESSING

The current technology makes available a multitude of devices for data acquisition providing immediate visual feedback to the writer. The dynamic signature data is generally

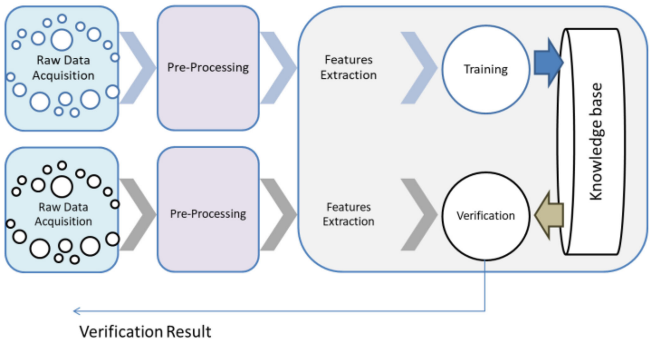

FIGURE 2. Process of automatic signature verification.

acquired using devices like digitizing tablets or through the touch screen technologies provided on Tablet PCs, PDAs or smartphones. The dominant attributes captured in the mobile scenario are *X* and *Y* pen positions and their timestamps [37], [49], [56]–[58]. On the other hand, specifically devoted pads are able to acquire a wider set of data than the pen trajectory, namely pen orientation (azimuth and altitude) and pen pressure. Moreover, pen tablets also detect the pen trajectory when the tip is not in contact with the surface [39]. Smart pens embedding an accelerometer, a gyroscope and a pen grip pressure sensor have been also considered [50]. The treatment of signatures acquired using different devices poses several interoperability problems. Moreover, within the mobile scenario, specific issues arise on the quality of signature specimens, due to the small size of the writing area and the non-standard posture of the signer. In fact, the available writing area strongly influences features [40], [71], [73].

The pre-processing phase generally concerns filtering and noise reduction techniques, as well as signature normalization and segmentation [38], [39]. Some segmentation techniques consider a signature as a sequence of writing units, the "regular" parts of the signature, delimited by abrupt interruptions, the "singularities" of the signature. Signatures can also be segmented in accordance with perceptually important points or derived from the analysis of direct matching points [17], [70].

The cloud scenario poses issues related to the part of the infrastructure on which pre-processing should be performed. For example, if the ISO/IEC 19794-7 International Standard for the Biometric Signature interchange format is adopted [42], it requires the evaluation of many parameters (e.g., scaling factor, minimum, max, average and standard deviation of channels) before the transmission occurs.

B. FEATURE EXTRACTION

Function and parameter features can be considered [39]. In the first case signatures are characterized by time functions. Examples of function features are: position in terms of (x,y), velocity, acceleration, pressure, force and direction of pen movements, speed and angular acceleration. When parameter features are used, the signature is characterized as a vector of elements: in this case indexes of the vector are not referred to a time sequence. Typical global parameter features are the total signature duration, the number of pen lifts (pen-down/pen-up), the pen lift time ratio and other parameters derived from the analysis of direction, curvature and moments of the signature trace. Well-known parameters are also the average, root mean square, maximum and minimum values of position, displacement, speed and acceleration. Coefficients derived from Fourier Transform and Wavelet Transform have also been considered as parameter features. In general, it is worth noting that parameter features are evaluated from time function features by means of a transformation. The transformation can be invertible or not: the original function feature can be recovered only in the first case.

Parameter features can be considered at global level, i.e., for the whole signature, or at local level, i.e., for specific regions (segments) of the signature. Global features reflect the holistic characteristics of a signature while local features describe very specific characteristics of a signature region [38], [75]. Global and local features have been frequently combined [91], [93].

The use of a generic feature set over the entire population has demonstrated to be not effective, and many studies have been devoted to the selection of the most suitable features on a signer basis [33], [39], [70], [75], [105].

TABLE 1. Verification Techniques.

Technique	Algorithm	Reference
Distance based	DTW	[5], [6], [8], [9], [11], [15], [32], [49], [56], [57], [91], [93], [94], [97]
Model based	ANN	[106]
	HMM/GMM	[6], [19], [26], [35], [55], [92]
	SVM	[57], [58], [87], [90]

C. TRAINING-VERIFICATION

The authenticity of a test signature is evaluated by comparing its features against those stored in the knowledge base and developed during the enrolment (training) stage [39]. The result is generally provided as a Boolean value (acceptance or rejection) however, a float value can also be provided when a confidence value, concerning the decision, is required. In general, two matching approaches can be considered: distance-based and model-based [75]. The most used in the cloud-mobile scenario are reported in Table 1.

Distance-based approaches provide the verification response based on the distance between the test signature and one or more reference signatures. Model-based approaches verify the test signature by estimating fitness on the signature reference model of the user. Dynamic Time Warping (DTW) [67] is the most exploited distance-based technique as it allows the time axis of two-time sequences representing a signature to be compressed or expanded locally to obtain the minimum of a given distance value. To make matching more cost-effective, advanced DTW strategies have been proposed for data reduction based on genetic algorithms, principal or minor component analysis and linear regression. When

parameters are considered, both Euclidean and Mahalanobis distances have been used for distance-based matching, as well as similarity measures, split-and-merge strategies and string-matching [15]. Support Vector Machines (SVMs) have also been used for signature matching, since they are able to map input vectors to a higher dimensional space, in which clusters may be determined by a maximal separation hyper-plane [90]. Model-based techniques for signature comparison mainly concern artificial neural networks (ANNs), multi-layer perceptrons, time-delay neural networks, backpropagation networks and self-organizing maps. Hidden Markov Models (HMMs) have also been successfully used for signature matching; since they are highly adaptable to personal variability, they can support effective signature modelling techniques [19], [26].

Note that when model-based classifiers such as ANNs, HMMs, SVMs, etc., are considered, the problem of the size of the training dataset arises [101]: within a real cloud scenario there is a first cold start problem that is the reduced number of available signatures and/or their quality. Many researchers agree about the number of genuine and good quality signatures can be acquired within a single training session is between 3 and 5 specimens (based on the number of samples used for training). A higher number will result in very poor execution. In fact, it is quite easy to have a nominal good number of available samples (just think about the number of signatures required when a credit card is issued); unfortunately, these specimens are often very poor in execution quality. On the other hand, it must be considered that the initial reduced set can be enlarged by using synthetically generated signatures [27], as well as that the amount of available signature increases with the use of the system: it has been showed that a re-training process considering new samples results in improved performance [81].

Automatic signature verification produces two types of errors: False Rejection Rate (FRR), concerning the false rejection of genuine signatures; and False Acceptance Rate (FAR), which concerns the false acceptance of forged signatures. The threshold that provides the best trade-off between FRR and FAR depends upon the specific application and it represent a non-trivial problem. For example, in the case of a high security application, the FAR should be as low as possible, while in the case in which the probability to have an attack would be very low, FAR can be a higher value. It must be also underlined that FAR and FRR are strictly related one to the other, so that (in general) every effort to reduce one of them results in the increase of the other one. Usually, for comparison aims, the DET (Detection Error Trade-off) curve is considered plotting the FRR vs. FAR so that the performance of the system can be evaluated at various values of the threshold. Many works have also demonstrated that a globally applied threshold is not effective, so that in a real scenario, the user-based threshold assessment should be also administered. Another very common parameter is the Equal Error Rate (EER) defined as the point of the DET where $\mathrm{FRR} = \mathrm{FAR}$. In this paper, unless otherwise specified, performances are expressed in terms of EER [39]. It is a fair choice to adopt EER here for comparison since it is the most common parameter reported in the most part of reviewed papers.

III. THE MOBILE-CLOUD ARCHITECTURE

Dynamic signature verification on mobile cloud scenario must be considered along three different directions:

- Accessibility and usability,
- Interoperability,
- Security.

A. ACCESSIBILITY AND USABILITY

The final user is expected to mainly interact with the system in an unsupervised way (i.e., on mobile devices). Dissatisfaction generates performance degradation, misuses and, in the worst case, the rejection of the technology. The signing process within the application must be easy to use (e.g., 2017 Apple Pay FACE ID is equivalent to take a selfie). The signing process should not require more time than the one needed to "sign the signature" [12].

Usability experiments have been performed considering different devices, platforms and technologies as well as various posture scenarios [8], [10], and [83]. Although the signing process is often considered to be an automatic one, the visual feedback plays a crucial role: signing without a visual feedback is completely un-natural [9].

The signing box size, typically adopted on identity cards, bank checks and credit/debit cards, is (approximatively) $70\text{x}15$ mm [73], in fact the smallest screen size adopted by professional solutions is (approximatively) $95\text{x}50$ mm which include the area for the signature and other essential info (e.g., the amount and the currency). In order to reproduce the same conditions, mobile devices should have a screen of at least 5 inches. Of course, the signing area can be smaller, but it should be clear that constrains on the writing area strongly influence the result of the signing process since fine motor control is involved. The influence is not only in terms of size (i.e., the disappearance of elements or compressed/poor specimens) but also in terms of velocity. It has been observed that velocity seems to be very dependent on the writing area size whereas acceleration and pressure do not change significantly. In fact, when parameter features are considered, the signature area is the characteristic most dependent by spatial constraints: height and width oscillate, whereas ascendants and descendants do not seem to be affected [40], [71], and [73]. So that, the problem of two signatures acquired on two different writing areas cannot be coped with a simple a-posteriori normalization in terms of spatial dimension.

The most part of smartphones and tablets currently available is not provided with a stylus; even if some object could be used and/or adopted to the aim (based on screen technology), it is clear that a pen with a rigid thin tip is desirable for improving the user experience and comfort [57]. However, the instinctive solution in absence of stylus is the use of a finger [11], [81]. In this case it is important to understand that the interaction mode with the device is different: touch

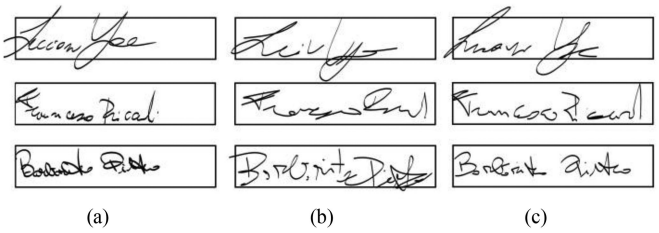

FIGURE 3. Dynamic signatures (a) stylus, (b) finger first attempt, (c) finger after some trials. Signatures are acquired on the same device and on the same writing area.

vs. pen. The user is already confident with the finger-touchscreen interaction, but the task to be performed is "new". Leaving aside the signature (for a while), it has been already showed that the interaction with the touchscreen results in different patterns (e.g., swipe or touch dynamics) can be used for user identification aims [23], [88]. In general, high intra-class variability due to time, emotional state, change of the part of the screen which has been touched and task performed has been observed [23]. From this perspective, a signature could reduce the variability amount, but it should be clear that the signature written by means of the finger should call for a new set of features to be considered: each one use her/his own finger. Up to this date all works dealing with finger-based signatures have considered the same set of features for both pen and finger -based systems, but the result (signature) obtained in the two cases is different (see Figure 3). This is mainly due to:

- the unusual use of the finger compared to the pen;
- the perception that the user has of the finger size compared to the one of the pen normally used;
- the non-rigidity of the finger;
- the friction between the screen and the finger which is quite different from the one between the pen tip and the screen;
- the changing of the screen-finger contact point while signing as well as the different size of the contact area.

Differences are not only in the (x,y) coordinates domain but also in velocity (due to a different friction), pressure, contact area, etc..

Figure 3 points out that finger-based signatures get closer to pen-based in the (x,y) domain while the user became confident with the task. Signing time also decreases revealing that users do not stop perfecting the signing process [9]. However, in general, users feel more comfortable when a stylus is used [10]. The acquisition mode (pen or finger) should be considered as a meta-feature and must be taken into account within the system adopting a multiple reference sets strategy [41].

As previously mentioned, the common set of pen-based features has been generally considered also in the case of finger-based signatures. The use of signature-based features in order to identify people by swipe (finger-made) on touchscreen has been also considered [23]. Although a swipe cannot be compared to a signature in terms of complexity (e.g., the number of strokes, geometry, changes in directions and velocity, etc.), it is interesting to consider that horizontal gestures obtained better performance than vertical one. Another interesting result is that, in landscape orientation (the one on which the signature is expected to be written) the performance for the inter-session scenario are better than that in portrait one [23]. Even if these results can be transposed to the signature domain only to some extent, they call for stability evaluation of different strokes of the signature in the finger mode scenario: results could be completely different from those already observed on the stylus domain [70].

Regarding posture, two possibilities must be considered:

- the mobile device is placed on a table or support;
- the user is handling the mobile device.

The first scenario is quite close to standard signing conditions, in fact, the use of stylus outperforms (in terms of EER) finger-based signatures [10]. On the other hand, finger-based approach results in improved performance when the user handle the device without support, in fact the weight and the size of the device strongly influences the signing process [10].

Finally, the mobile device has been also considered within an authentication procedure consisting in making the signature in the air while holding the device in the hand [6], [32]. In this case: the movement is performed in the air instead of on a surface, so it should be harder to copy the 3-D gesture. Of course, the device must embed an accelerometer to obtain the acceleration values of the movement. The amount of works in literature is not enough to state something about real performance, but of course this is an interesting area of investigation.

B. INTEROPERABILITY

The mobile cloud scenario intends signatures of the same user acquired with different devices and cross-used (enrolment vs. classification). Two major issues deal with interoperability:

1. Data interchange format;
2. Data normalization.

The first problem is solved by the International Standard ISO/IEC 19794-7 which specifies data formats for signatures [42]. A deep insight on this standard is out of the aims of this paper; however it must be argued that the standard takes into account raw data and parameters reported in Table 2 that are named "channels". Only channels considered by the standard can be interchanged: if the system needs to evaluate a wider set of features (e.g., parameter features, etc.), these have to be computed after the transmission has occurred.

The main problem found in this direction is that the standard does not provide a conformance tool test, although it provides sample files, so that, data interchanging problems are evident just when they occur. In fact, in an unpublished interoperability test involving different vendors, no files where immediately and directly readable from third-party software. The test pointed out problems to be solved, so that at the end of the second round there was a full interchangeability.

When data normalization is considered, the first issue deals with the tactile sensor used by the acquisition device since different technologies capture signals in different manners. The following technologies can be considered [16]:

TABLE 2. ISO/IEC 19794-7 Second Edition (2014-02-01) - Features.

Channel
X coordinate
Y coordinate
Z coordinate
Velocity in the x direction
Velocity in the y direction
Acceleration the x direction
Acceleration in the y direction
Time stamps
Time difference
Pen tip force
Button status
Tilt along x
Tilt along y
Azimuth
Elevation
Rotation

- Capacitive sensor can be made very small allowing the construction of dense sensor arrays; moreover, they are also very robust; most part of smartphones and tablets adopts capacitive sensors.
- Resistive sensors have resistance values depending on the contact point and the applied force: they are, in general, less sensitive than capacitive. A small set of mobile devices and of signature pads adopts this technology.
- Optical sensor can be also considered for screen technology as well as for the pen (e.g., camera based pen); in general an optical pad can also measure pressure. A very reduced set of mobile devices adopt optical sensors.
- Electromagnetic sensors have many advantages if compared to other technologies: high sensitivity, good dynamic range, no measurable mechanical hysteresis, linear response and physical robustness. This solution is the one adopted (under various patents) by specifically devoted signature acquisition pads.

Table 3 reports acquisition details (as stated by producers) of some signature pads currently available on the market. It can be observed that devices are different in terms of sampling frequency, spatial resolution, accuracy and pressure levels. Regarding pressure, it is worth noting that the difference it is not only in terms of quantization levels, but also in terms of force range. Another issue is the calibration in terms of sync of the pencil with the pad which results in an offset between the screen cursor and the position of the pen on the screen. Many specifically devoted pad vendors provide a calibration procedure, which is not available on others and on mobile devices. Variations due to differences in sampling, quantization, sensing technology, writing area, posture, etc., are reflected in features. Variation in features results in mismatch and in very increased EERs [9]. Although the ISO/IEC 19794-7 offers the possibility to specify details dealing with the capture device (i.e., vendor identifier, device ID and screen technology) unfortunately these fields are almost never filled, principally due to the lack of encoded data. This info, coupled with those related to channels (i.e., values range, mean, etc.) plays a crucial role within an inter-device normalization process. The problem is already known in many other biometric scenarios [80], but, to date, it has only been addressed indirectly (and to some extent) within the field of signature verification [4], [73], [84]. Two strategies can be adopted in order to cope with the problem:

1. The use of specific template/models given the acquired signature sample to be tested;
2. Values normalization/compensation;

The first solution intends a set of models (references) stored into the knowledge base obtained by different acquisition devices. So that at each verification submission, the corresponding device-based model can be considered. It is a practical and viable solution due to the fact that a person does not change his/her mobile device on day basis and that the amount of signature pads is less than twenty. Moreover, the downscaling of this idea to specific corporate scenario is

TABLE 3. Main Acquisition Characteristics of Professional Signature Pads. Legend: Electromagnetic Resonance (EMR), Resistive Technology (RES), Capacitive Technology (CAP).

Product	Writing area W × H [mm]	Technology	Pressure Levels	Force range [N]	Sampling Freq. [Hz]	Spatial resolution	Accuracy of repetition in X,Y,Z measurements	Data encription
1	154 × 86	EMR	1024	na	Na	2540 lpi	+/ − 0.4 mm	3DES 168 bit
2	223 × 126	EMR	1024	[0.3;5]	Na	1000 lpi	+/ − 0.5 mm	3DES 168 bit
3	217 × 136	EMR	2048	[0.3;5]	Na	2540 lpi	Na	AES-256
4	95 × 47	CAP	na	na	Na	Na	Na	DES, 3DES, RSA
5	150 × 85	CAP	na	na	Na	Na	Na	DES, 3DES, RSA
6	3, 5″	RES	na	na	Na	Na	Na	Na
7	95 × 47	RES	1024	na	500	1121 × 2243 ppi	+/ − 1, 5%	AES-256 / RSA-2048
8	100 × 75	RES	1024	na	500	1040 × 1387 ppi	+/ − 1, 5%	AES-256 / RSA-2048
9	108 × 65	EMR	2048	na	500	2400 × 2909 ppi	+/ − 0, 4 mm	AES-256 / RSA-2048
10	95 × 53	EMR	512	[1;10]	500	1000 lpi	+/ − 0.1 mm	RSA 2048
11	100 × 29	EMR	512	[1;10]	500	1000 lpi	+/ − 0.1 mm	RSA 2048
12	114 × 85	EMR	512	[1;10]	500	1000 lpi	+/ − 0.1 mm	RSA 2048
13	96 × 60	EMR	1024	na	200	2540 lpi	+/ − 0.5mm	AES-256 / RSA-2048
14	108 × 65	EMR	1024	na	200	2540 lpi	+/ − 0.5mm	AES-256 / RSA-2048
15	108 × 65	EMR	1024	na	200	2540 lpi	+/ − 0.5mm	TLS

quite easy, it would result in low cost implementation and reduced EER.

However, it is quite clear that the previous solution can be applied only to some extent: values normalization shall be considered. A signal processing approach suggests to take into account two phases:

- Resampling of time signals (function features) and values interpolation to obtain missing elements;
- Range values normalization (e.g., within a pre-defined range, typically [0,1]).

For example, in [9] raw signals were linear interpolated to obtain 256-point vectors, values were normalized by using their mean and standard deviation (z-score). A very similar approach has also been adopted in [81] and [93]. Even if the z-score has been applied, there is no evidence it is able to outperform other well-known normalization techniques or more sophisticated approaches able to take into account the statistical estimates of value distribution of parameters over the specific device [72]. This is a domain of great importance. A set of experiments has been made to measure intra-device, intra-modality (only a single modality stylus/pen is allowed) and inter-modality (signatures acquired using both a stylus and the fingertip) performance [9], [93]. It has been showed that most of the EERs obtained in the inter-modality experiments were comparable to the intra-modality ones [9], however this result could be related to the specific devices and setup (in particular writing area) used in the particular experiments.

Resampling and value normalization has been coupled with features selection [91], [93]. More specifically, the Sequential Forward Feature Selection (SFFS) algorithm has been adopted using as optimization criteria the reduction of ERR (of all the possible devices matching cases) to obtain a subset of global and local features. Experiments, performed on the BioSecure DS2 and DS3 dataset, showed EER improvements if compared to the baseline system, moreover further improvements have been observed by combining local and global features [93].

C. SECURITY

Numerous advantages are offered by cloud computing, at the same security issues arise. These issues deal with confidentiality, integrity, and availability of data (signatures) [31]. The security issue arises since (in case of disclosure), solutions typically adopted with standard authentication technologies (e.g., change the password) cannot be adopted in the biometric scenario: it is almost impossible to modify the biometric (human characteristic) trait. In order to improve readability, the security issue is discussed taking into account two different points of view: a technological and a research one.

1) TECHNOLOGY ISSUES

Eight potential vulnerable points can be considered within a generic biometric system [22], [45], and [78]; however the cloud mobile signature verification scenario calls for specialization. In particular, assuming that the ISO/IEC 19794-7

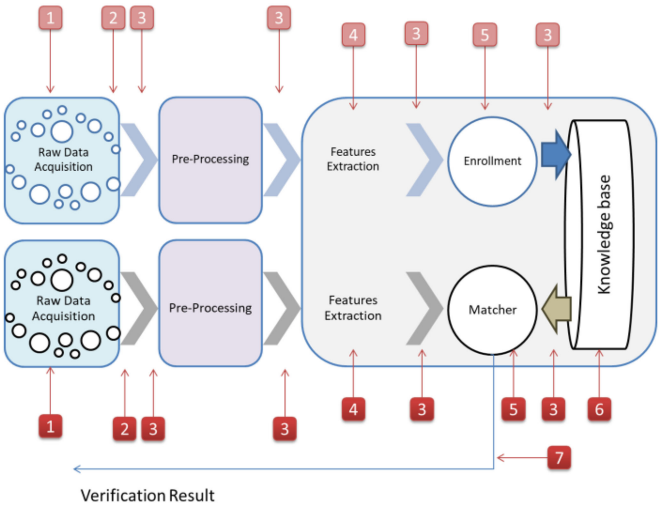

FIGURE 4. Possible vulnerable points within a mobile scenario (adapted from [45]).

standard is applied for raw data (channels) interchange, the baseline distributed application intends:

A. signature acquired on a device,
B. signature channels transmitted to a server(s) adopting the ISO/IEC 19794-7 over a secure transport/network layer,
C. supplementary features extraction, matching phase and decision taken on the server(s),
D. decision, with the allow/denial of required service, transferred from the server to the mobile device over a secure transport/network layer.

Given the above, possible attacks deal with elements reported in the following and depicted in Figure 4.

1. Sensor. Three main presentation attacks can be considered concerning the sensor: *Random Forgeries* (an impostor tries to verify the identity of a signer by using a random signature); *Simple Forgery* (the forger knows the writer's name, but has no access to samples of the signature) and *Skilled Forgeries* (the impostor is able to reproduce the target signature with a certain degree of similarity) [39]. Different skilled forgeries can be taken into account based on the knowledge that he/she has of the genuine signature (e.g., static representation of the signature and/or the writing dynamics). It is quite clear that the error rates increase with the experience of the forger, however it has been showed that the ability of the forger to remember the target signature over time is a crucial point, so that the error rates can decrease since details are forgotten over time [85]. Presentation attacks can be compared only to some extent to those already known in other biometrics [28], in fact in the case of skilled forgery, a previous and complex elicitation attack is required to take details of the target signature. It is interesting to consider that, while a traditional presentation attack in physiological biometrics (e.g., face) involves the use of some physical artifact (e.g., mask and/or make-up) to override the sensor, signature

forgery attacks are performed in terms of mimicry. In this case the interaction with the acquisition device is the same of the genuine user (they both use the hand and the device). This attack does not involve any manipulation, overriding or hacking of the system. This means that, at present, it seems not to be possible to design anti-spoofing systems at the sensor device level (e.g., as in the case of fingerprint). This type of protection could be a great challenge since at this stage the evaluation of is entrusted to other parts of the system.

Within a real distributed scenario, also a *coercive attack* must be considered (i.e., a genuine user is forced to sign by an attacker). The system should be able to detect coercion without endangering lives.

2. Raw data extractor module of the device. In this case the impostor is able to tamper raw data acquired by the device (e.g., x, y, pressure, etc.) and to provide a different set. This kind of attack is performed, in general, by means of buffer manipulation, pointer manipulation and input data manipulation.
3. Network/Channel attack. It involves the network and it has the aim to intercept, read, stole and/or modify the exchanged data. It can be referred to mobile->server, server1->server2 and server->mobile transmissions. It can be performed by means of interception, protocol manipulation, traffic injection and obstruction.
4. Features extractor module. Here the assumption is that the system evaluates a new feature set taking as input those received by the device (compliant to ISO/IEC 19794-7). In general, this is a software module, so that attacks on this issue range from excavation to code injection.
5. Matcher. The impostor is able to tamper the matcher in order to forge the result (or score). Attacks to this module are similar to those of the previous point.
6. Signature Templates. The stored signature template or model is modified. The model is expected to be stored within a database, attacks mainly deal with it.
7. Final decision. The impostor is able to override the final decision.

Depending on the role and skills of the impostor an attack can be easier that another. In general, based on many cybersecurity reports, the most part of successful attacks deal, in order, with human errors (the user provides data in a non-conscious manner to the impostor), spying and extortion.

Under this light, it must be clear that enrollment is also vulnerable at points 1-5 [62]. If enrollment is allowed under non-supervised session(s), then probabilities of failures increase.

The assessment of a system within a real scenario must consider the above reported issues and implement them in com pliance with ISO/IEC 24745 standard [44] which deals with the protection of biometric information under the requirements of:

- Confidentiality of information and their protection against unauthorized access or disclosure;
- Integrity of the system, "property of safeguarding the accuracy and completeness of assets"
- Renewability and revocability to prevent the attacker from future (or continued) unauthorized access".
- Irreversibility of stored data (i.e., raw data function features cannot be stored):
- Un-linkability of the stored biometric references across applications or databases.
- Confidentiality of the biometric references.

It appears quite clear that interoperability of protected data and the fulfillment of all the previous requirements are quite hard to be satisfied in the cloud mobile scenario. To date, it must be observed that, in order to protect signature data (features, template, etc.) at different stages, standard kay release cryptography have been adopted [46]. In fact, specifically devoted and market available devices and applications typically adopt ISO/IEC 19794-7 standard for biometric signature exchange and standard cryptographic algorithm for the transfer of data (e.g., AES 256 bit encryption and RSA 2048 bit key exchange, see Table 3). Only in very few cases the application is declared to be compliant to the ISO/IEC 27001 (information-security) [43] while no state about ISO/IEC 24745.

2) RESEARCH ISSUES

Research activities cover a huge scenario, the complete set of open research issues related to security and privacy in mobile cloud computing can be found in [61]. This work just concerns with handwritten signatures, so that general issues are here specialized: the biggest issue deals with template security. In fact, the problem of using standard symmetric encryption algorithms is that the matching phase (comparison of the questioned signature against the claimed template stored into the knowledge base) is not allowed in the encrypted domain thus leaving the template exposed during every verification attempt [79] violating requirements of ISO/IEC 24745. It is worth noting that, within a cloud scenario, this could be performed on multiple and potentially non-secure platforms.

Three different strategies can be considered as summarized in Table 4: Homomorphic Encryption, Cancelable Biometric and Bio-cryptosystem (note that the last two terms have been frequently mixed within the biometric field) [102].

Homomorphic and asymmetric encryption allow the comparison (matching) in the encrypted domain. The use of this technique results in no degradation of performance (if compared to the matching in the non-encrypted domain) and it is a viable practical solution in the mobile cloud scenario since it also allows to meet requirements on biometric information protection of ISO/IEC 24745 [7], [29], [107]. It is worth noting that, in general, signatures to be compared could have a different length (e.g., in terms of samples), so that variable length data comparisons techniques have been also proposed within the homomorphic encryption schema [30], [31]. A crucial point within this direction is that the set of processing allowed in the encrypted domain is restricted, and some state-of-the-art approaches could not be applied as they are [29], [63]. In order to overcome this limitation, signature could be gathered with other biometrics (e.g., fingerprint)

TABLE 4. Signature Security Strategies.

Name	Working Modality	Impact on erformance	Compliant to ISO/IEC 24745 requirements	Ref.
Homomorphic Encryption	Matching allowed in the encrypted domain	No degradation if compared to the non-encrypted domain	YES	[31], [29]
Cancelable biometric	Biometric data is irreversibly transformed, verification is performed in the transformed domain	Degradation depends upon the specific transformation	Not Evaluated Not Evaluated To some extent	[107] [33], [34], [81], [99] [53], [54], [104]
Bio-Criptosystems	Encryption schema where the kay is generated directly from the signature	Higher performance degradation	Not Evaluated	[20], [25], [52]

thus obtaining a multibiometric system placed within a homomorphic encryption schema [29].

Cancelable biometric transforms are designed by means of non-invertible features: the computation of the original raw data acquired by the device should be computationally hard. In case of feature disclosure, a new set of cancelable features must be assessed. The simplest approach is to consider standard non-invertible parameter features (e.g., total duration, number of pen ups, sign changes in velocity and acceleration, average jerk, number of local minima, etc.) [39]. A pioneering work in this direction is the one by Vielhauer *et al.* [99] where an interval matrix was used to obtain a hash vector from raw features.

In general, within this direction, any non-invertible transformation can be considered made up of several steps [53], [54], [104]. A Symbolic representation of signatures based on global features (in the form of interval-valued data) has been also proposed [34], as well as this approach could be also coupled with user-dependent feature selection [33]. Similarly, histograms able to describe raw features statistics can be considered [81].

A growing interest has been observed on bio-cryptographic systems. In this case the idea is to have a combination of signature and cryptography with a key binding mode: the kay is generated directly from the signature so that it is not explicitly stored within the knowledgebase [46]. The problem is that, due to the intrinsic intra-class variation of signature samples, it is impossible to obtain exactly the same key (with a bit precision) at each submission. Intra-class variations must be small enough, to successfully enable the decryption process. A tolerance threshold must be administered: the most used approach in the biometric field is based on Fuzzy Vault (FV) construction of the bio-cryptographic system. FV has been also applied to signature verification under different schema and implementations [20], [25], [52]: high error rates have been generally observed.

In general, EERs performance obtained with non-invertible features as well as with bio-cryptographic systems are not able to equal those obtained by the baseline system. Moreover, their direct application into a real contemporary technological scenario will result in the failure of other parts of the system. In fact, just for instance, in order to be secure, the transform should be performed on the acquisition device by an ad-hoc embedded system [51].

IV. PERFORMANCE EVALUATION

Performance evaluation is a crucial point, in fact error rates in the mobile cloud scenario are significantly higher than the one observed in end-to-end solutions [5], [35]–[37] [56], [57], [106]. Table 5 summarizes performances of some of the most relevant approaches discussed in the following.

Obviously, the simplest approach to the mobile scenario is the application of pre-existing systems. To the aim, as a first attempt, the MCYT database has been modified to simulate signatures acquired by a mobile device considering capacitive and resistive screen technologies [58]. Simulations on the resistive screens yielded lower EERs than those obtained simulating capacitive screens. This result has been also confirmed taking into account a real (non-simulated) mobile scenario [57]. In this case five different devices have been used: four smartphones/tablets with a capacitive or a resistive screen, and a traditional digital pen tablet (considered as the baseline). A DTW-base system outperformed a SVM-based one. Moreover, it has been observed that the use of a template trained using a specific device coupled with specimens acquired by mean of other devices results in strong performance decay (about 10 percentage points).

Concerning features, it has been showed that dynamic features (speed and acceleration) have lower discrimination capability than geometric features (which are able to represent the 2D signature image) [55]. The need of specifically designed systems has been demonstrated by means of signature verification competitions. The BMEC'2007 Signature Competition [13] has been the first evaluation campaign involving mobile devices: BioSecure DS3 dataset has been considered. A multi-classifier system adopting several (seven) Gaussian Mixture Model (GMM)-based classifiers achieved the best performance when tested on both skilled and random forgeries ($\mathrm{EER} = 13.43$ percent and $\mathrm{EER} = 4.03$ percent, respectively). Five classifiers were based on local features, while the others on global features. Successively the BioSecure Signature Evaluation Campaign (BSEC'2009) [36] had, among the others, the aim to evaluate the influence of acquisition conditions (digitizing tablet or PDA) on systems' performance. In

TABLE 5. Systems' performances. Legend: Genuine Signatures (GS), Random Forgeries (RF), Skilled Forgeries (SF), Artificial Neural Network (ANN), Dynamic Time Warping (DTW), Longest Common Subsequence (LCS), Gaussian Mixture Model (GMM), Hidden Markov Model (HMM), Support Vector Machine (SVM).

Matching technique	Main Features	Database	EER	Reference
ANN	Time, X and Y coordinates, pressure	SG-NOTE, SVC: 5 users × (20(GS) + 20(SF)	0.127% (RF)	[106]
DTW	Time, X and Y coordinates	21 users	0.21% (RF)	[8]
	Time, speed, acceleration, direction, X and Y coordinates	SG-NOTE: 25 users- × 2 sessions × 10(GS)	0.525% (RF)	[49]
	Time, X and Y coordinates	43 users × 60(GS) × 8 devices	0.19% (RF)	[11]
	Global features	BioSecure DS2 and DS3 of 120 users, SG-NOTE	2.1% (RF)	[56]
	X and Y coordinates, pressure	BioSecure DS2 and DS3 of 120 users	2.0% (RF) 6.2% (SF)	[93]
	X and Y coordinates, pressure	e-BioSign: 3640(GS) + 2730(SF) collected from 5 devices and 65 users in 2 sessions	Stylus: 0.05% (RF) 6.35% (SF) Finger: 0.36% (RF) 13.23% (SF)	[97]
	Time	e-BioSign	0.1% (RF) 6.4% (SF)	[94]
	X and Y coordinates, pressure	e-BioSign	0.5% (RF) 23.9% (SF)	[91]
	Time, X, Y, velocity, acceleration, pressure, entropy, global features	MOBISIG	4.62 (RF) 10.72% (SF)	[5]
	Pressure	11 users × 8 devices (using stylus and finger) × 3 sessions × (20(GS) + 20(SF))	1.27% (RF) 7.99% (SF)	[9]
	Acceleration	96 users × (8(GS) + 7(SF))	2.12% (RF) 4.58% (SF)	[6]
DTW, SVM	Pressure	5 databases (for 5 devices) each one consisting of 25 users × (28(GS) + 28(SF))	1.58% (RF) (DTW) 4.03% (RF) (SVM)	[57]
DTW, LCS	Acceleration	50 users × (7(GS) + (6 impostors × 5(SF))	2.80% (DTW) 3.34% (LCS)	[32]
HMM	Time, speed, acceleration, direction, X and Y coordinates	BioSecure DS2 and DS3 of 120 users × (20(GS) + 20(SF)) × acquisition device (pen tablet, DS2, and PDA, DS3)	4% (RF) 11.9% (SF)	[55]
	Speed, acceleration	PDA-64 (64 users), BioSecure DS3 (210 users)	16.02% (SF) (PDA-64), 9.95% (SF) (DS3)	[35]
	X and Y coordinates, pressure	Extended version of the Signature Long-Term database: 29 users × (46(GS) + 10(SF))	0.0% (RF) 1.4% (SF)	[92]
Model-free non-invertible system	Histogram-based features	MCYT, SUSIG: 94 users × 2 sessions × (20(GS) + 10(SF)), a mobile dataset of 180 users signing with the finger	2.67% (RF) on the mobile dataset	[81]
SVM	Speed, acceleration	Modified MCYT emulating mobile devices: 100 users × (25(GS) + 25(SF))	3%	[58]
	Displacement, velocity, acceleration, duration, direction	50 users, >100 pen based signature per user, >100 finger based signature per user 10 users used to produce 10 fake trials of 32 genuine users	Stylus: 0.52% Finger: 1.63%	[87]

fact, the BioSecure DS2 dataset contains the same writers of DS3, but signatures are acquired on a digitizing tablet. It is important to note that DS2 and DS3 were collected in two sessions separated in time by several weeks thus giving the possibility to evaluate intra-class variability over time. Even in this case, performances obtained with signatures acquired with the specifically devoted pad are globally better than those related to signature acquired on the mobile platforms. Moreover, the new competition, if compared to BMEC'2007, resulted in EER improvements: 4.97 and 0.55 percent on skilled and random forgeries, respectively. In this case, systems able to perform better than others adopted local features and a DTW-based score computation. The BioSecure Signature Evaluation Campaign (ESRA'2011) [37] has intended to evaluate the impact of mobile devices and skilled forgery considering coordinate function features. This choice is of interest since even if many function features could be typically considered with a specifically devoted pad (e.g., pressure, azimuth and

altitude), these are not provided by the most part of mobile devices. Once more it has been observed that signatures acquired by a digitizer tablet were able to outperform results obtained on the mobile scenario, moreover the ranking of systems in terms of performance was different when considering the use of additional function features. Among the others, one of the main reason for performance degradation within the mobile scenario has been considered to be the absence on in-air features, moreover it has been also observed that global features present a more robust behavior than local features [49], [56].

The amount of genuine signatures to be used for the training issue, within a real scenario, increases as the application is used. Under this light and in the consideration that an update process of the template stored within the knowledge-base must be administered, it has been empirically showed that EER decrease when the classifier is trained using samples from the preceding session [81]. Although this result is very interesting, it could be biased (to some extent) by the dataset adopted, moreover this approach can be adopted only under a restricted set of circumstances, in fact a mobile distributed scenario implicitly deals with the acquisition of signatures in un-controlled, not trusted and un-supervised settings: this results in the problem of the selection of signature to be used for the training phase. The enrolment of specimens acquired within an unsupervised scenario (even if considered to be genuine by the system) arises many lawfulness and security issues given the possibility to introduce, within the knowledge base, fake trials (i.e., specimens by random, simple and skilled forgeries). Probably signatures evaluated as genuine but acquired within an unsupervised scenario should be conveyed within a different "non-trusted" training set. However results obtained by the pattern recognition community within the re-training process (in semi-supervised scenarios) haven't been studied within this specific field, so that it must be considered to be a challenging open issue [47]. Some results can be referred to HMM and GMM [92], (even if in this case signature where acquired only by means of a single platform): the standard case of having an HMM-based system with a fixed configuration and an HMM-based and a GMM-based system with optimized configurations in function of the training signatures available at enrolment stage. The approach has been able to let the system achieves an average absolute improvement of 4.6 percent (2.7 percent) in terms of EER, with respect to the baseline system, for the skilled (random) forgery cases. These results highlight the importance of configuration optimization when the number of training signatures increases.

Shahzad *et al.* [87] considered signature acquired considering both stylus and finger. In the case of finger based signatures, the centroid of the touching area was considered. Due to the limited touch resolution of the capacitive screen, a low pass filter was adopted to remove high frequency noise in the time series of coordinate values. Excellent EERs were observed, however it must be argued that the acquisition protocol intended users to be sit and the device placed on a table, as well as 25 training samples were considered, as well as many other test conditions.

When the smartphone has been considered to be handled in order to write the signature in the air [6], [32], Longest Common Subsequence (LCS) and DTW have been used to align acceleration signals, and to evaluate distance. The algorithms based on DTW obtained better EER results than those based on LCS (2.80 vs. 3.34 percent) [32]. In this case DTW has outperformed HMMs and Bayes classifiers, moreover the approach seems to be robust against spoofing attacks [6].

V. CONCLUSION AND OPEN ISSUES

Signature verification has attracted great interest over the last forty years. The current industrial scenario principally involves bank and commercial transactions. Of course, these transactions are within a distributed cloud scenario which calls for interoperability. Moreover, each one of us has mobile devices and more and more often we carry out transactions with mobile device. To date, the security of these transactions is entrusted to the knowledge of some secret code even if new biometric services are being used (e.g., 2017 Apple Pay FACE ID). In this perspective, this report addresses to a systematic review of the literature on handwritten signatures in the mobile cloud scenario. Along the different sections the most interesting results have been reported. Although some specific open issues have been already pointed out, in the following the most relevant are briefly discussed.

A. DATASET

Two datasets are currently available: BioSecure [13] and BioSign [51]. The DS2 subset of e-BioSecure contains two sessions acquired on a specifically devoted pad two weeks apart. The DS3 subset is acquired using a mobile device, it contains two sessions acquired 4-5 weeks apart. DS2 and DS3 contain signatures of the same users. E-BioSign database contains signature acquired by using 3 specifically devoted pads (all belonging to the same vendor) and two tablets. Two sessions acquired 3 weeks apart are available.

It is quite clear that there is the lack of an extended dataset public available. The missing dataset would include signatures acquired by means of multiple tools of different vendors since inter-vendor compatibility is a crucial point. Different screen size mobile devices should be considered, in fact this aspect, as already described, involves issues not present in traditional devices specifically conceived for the aim. Mobile devices are typically characterized by a small input area which is large enough (in the case of 5" screen size) if the signature is going to be written by means of a stylus, but it is too small if the signature is going to be written by finger. This aspect affects user interaction and leads to large intra-class variability. The data acquisition should be performed over multiple time spanned acquisition sessions in order to evaluate aging. The dataset should also include soft-biometrics dealing with contour acquisition conditions [14], [65].

B. FINGER AND STYLUS

Up to date, the same set of features has been considered whenever the signature has been written by using a finger or a stylus. Some features have been removed in order to allow comparison. However features considered where those related to the stylus domain. The finger scenario offers the possibility to take into account features from the keystroke and touch dynamics domain [48], [59], [82], and able to describe tapping behaviour [108] or swipes [23]. Just for instance, the touch size and the shape of the contact area have never been considered, as well as the fact that mobile screens allow multi-touches. In fact it has been shown that touch analytics can be used to recognize users [24].

C. INTEROPERABILITY

As the number of devices increases, device interoperability is a very relevant issue that needs further specific research. Signature signals can change significantly depending on the type and characteristics of the acquisition device. At this stage no inter-sensor calibration model has been proposed even considering specifically devoted devices, as for instance it has been done so far on fingerprint [80]. Some preliminary research has showed that velocity is more influenced than acceleration and pressure [40]. Also feature selection has been taken into account in order to face the problem of interoperability; however it should be specialized within the per-user direction since it has been demonstrated that a features set universally applied is not effective.

D. SECURITY

This issue principally concerns the implementation of the so-called *bio-cryptographic* systems [96] able to fulfils requirements of ISO/IEC 24745 while offering acceptable EER if compared to the baseline system. Bio-cryptographic systems may find application in the emerging mobile cloud computing field [18]. Another interesting research aspect is the administration of the selection of a new non invertible feature set when the previous one is disclosure as well as performance evaluation and parameter amount.

E. MULTIBIOMETRICS

Okabe and Yamazaki [66] were among the first to propose a multimodal system taking into account the usage environment. The authors focused on both face and handwriting as they can be acquired by mobile devices. Moreover, nowadays, many devices are also equipped with a fingerprint sensor. Nevertheless also keystroke dynamics and behavioural and cognitive aspects could be coupled.

At present, common dynamic signature verification systems intend the signature written by means of a pen or of a finger. Non-contact modalities can be also investigated: Guerra-Casanova *et al*. [32], Bailador *et al*. [6] and Fang *et al*. [21] considered in-air signatures. In this direction it is quite interesting to consider that the hand-waving behavior (the way in which the mobile device is handled) can be used to distinguish users [89], [103]. A continuous mobile-based authentication process could be also taken into account by considering touch dynamics and data provided by embedded sensors (e.g., gyroscope, accelerometer, etc.) [1]. In fact in this case sensors could be able to provide contour information related to the signing process as, for example, the posture of the writer (sitting, standing, walking). Signature verification could be coupled with other continuous user authentication on mobile devices [68] so that the impostor could be detected before signing [69].

Very interesting overviews can be found in [3] and [60] which also discuss how to implement the multimodal authentication.

F. REAL SCENARIO

Least but not last, real scenario test conditions should be considered in order to propose and evaluate feasible solutions. Examples of such conditions are:

- No real impostor trials are available at training;
- The reduced set of signature available at the very first training session, and in case of more than 5-6 samples, the evaluation of their quality;
- The possibility to perform supervised as well un-supervised training and/or verification;
- Template selection and update given the increasing of available samples as the system is deployed [95], [23];
- Practical forgery attacks and countermeasures (e.g., adding features [100] or combining with standard technologies).

REFERENCES

[1] Z. Akhtar, A. Buriro, B. Crispo, and T. H. Falk, "Multimodal smartphone user authentication using touchstroke, phone-movement and face patterns," in *Proc. IEEE Global Conf. Signal Inf. Process.*, 2017, pp. 1368–1372.

[2] W. Akram and M. A. Shah, "Online signature verification: A survey on authentication in smartphones," in *Proc. Ubiquitous Netw.*, 2017, pp. 471–480.

[3] A. Alzubaidi and J. Kalita, "Authentication of smartphone users using behavioral biometrics," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1998–2026, Jul.-Sep. 2016.

[4] F. Alonso-Fernandez, J. Fierrez-Aguilar, and J. Ortega-Garcia, "Sensor interoperability and fusion in signature verification: A case study using tablet PC," in *Proc. Int. Workshop Biometric Person Authentication*, 2005, pp. 180–187.

[5] M. Antal and A. Bandi, "Finger or stylus: Their impact on the performance of on-line signature verification systems," in *Proc. 5th Int. Conf. Recent Achievements Mechatron. Autom. Comput. Sci. Robot.*, 2017, pp. 11–22.

[6] G. Bailador, C. Sanchez-Avila, J. Guerra-Casanova, and A. de Santos Sierra, "Analysis of pattern recognition techniques for in-air signature biometrics," *Pattern Recognit.*, vol. 44, no. 10, 2011, pp. 2468–2478.

[7] M. Barni, G. Droandi, and R. Lazzeretti, "Privacy protection in biometric-based recognition systems: A marriage between cryptography and signal processing," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 66–76, Sep. 2015.

[8] R. Blanco-Gonzalo, L. Diaz-Fernandez, O. Miguel-Hurtado, and R. Sanchez-Reillo, "Usability evaluation of biometrics in mobile environments," in *Proc. 6th Int. Conf. Hum. Syst. Interactions*, 2013, pp. 123–128.

[9] R. Blanco-Gonzalo, O. Miguel-Hurtado, A. Mendaza-Ormaza, and R. Sanchez-Reillo, "Handwritten signature recognition in mobile scenarios: Performance evaluation," in *Proc. IEEE Int. Carnahan Conf. Security Technol.*, 2012, pp. 174–179.

[10] R. Blanco-Gonzalo, R. Sanchez-Reillo, O. Miguel-Hurtado, and J. Liu-Jimenez, "Usability analysis of dynamic signature verification in mobile environments," in *Proc. Int. Conf. BIOSIG Special Interest Group*, 2013, pp. 1–9.

[11] R. Blanco-Gonzalo, R. Sanchez-Reillo, O. Miguel-Hurtado, and J. Liu-Jimenez, "Performance evaluation of handwritten signature recognition in mobile environments," *IET Biometrics*, vol. 3, no. 3, 2014, pp. 139–146.

[12] R. Blanco-Gonzalo, R. Sanchez-Reillo, C. Sanchez-Redondo, and J. L. Alonso-Aguilera, "Accessibility evaluation of a mobile biometric recognition system," in *Proc. IEEE Int. Conf. Identity Security Behavior Anal.*, 2016, pp. 1–6.

[13] A. Mayoue, B. Dorizzi, L. Allano, G. Chollet, J. Hennebert, D. Petrovska-Delacretraz, and F. Verdet, "BioSecure multimodal evaluation campaign 2007," *Guide to Biometric Reference Systems and Performance Evaluation*. D. Petrovska-Delacrétaz, B. Dorizzi, and G. Chollet, Eds. pp. 327–371, 2009.

[14] N. Bouadjenek, H. Nemmour, and Y. Chibani, "SVM Combination for an enhanced prediction of Writers' soft biometrics," *Hybrid Intelligence for Image Analysis and Understanding*, Hoboken, NJ, USA: Wiley, 2017, pp. 103–125.

[15] Y. Chen and X. Ding, "On-line signature verification using direction sequence string matching," in *Proc. 2nd Int. Conf. Image Graph.*, 2002, pp. 744–749.

[16] R. S. Dahiya, G. Metta, M. Valle, and G. Sandini, "Tactile sensing—From humans to humanoids," *IEEE Trans. Robot.*, vol. 26, no. 1, pp. 1–20, Feb. 2010.

[17] G. Dimauro, S. Impedovo, and G. Pirlo, "On-line signature verification by a dynamic segmentation technique," in *Proc. 3rd Int. Workshop Frontiers Handw. Recognit.*, 1993, pp. 262–271.

[18] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Commun. Mobile Comput.*, vol. 13, no. 18, pp. 1587–1611, 2013.

[19] J. G. A. Dolfing, E. H. L. Aarts, and J. J. G. M. van Oosterhout, "On-line verification signature with hidden Markov models," in *Proc. 14th Int. Conf. Pattern Recognit.*, 1998, pp. 1309–1312.

[20] G. S. Eskander, R. Sabourin, and E. Granger, "Improving signature-based biometric cryptosystems using cascaded signature verification-fuzzy vault (SV-FV) approach," in *Proc. 14th Int. Conf. Frontiers Handwriting Recognit.*, 2014, pp. 187–192.

[21] Y. Fang, W. Kang, Q. Wu, and L. Tang, "A novel video-based system for in-air signature verification," *Comput. Electr. Eng.*, vol. 57, pp. 1–14, 2017.

[22] H. Feng and C. C. Wah, "Online signature verification using a new extreme points warping technique," *Pattern Recognit. Lett.*, vol. 24, no. 16, pp. 2943–2951, 2003.

[23] J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally, and A. Morales, "Benchmarking touchscreen biometrics for mobile authentication," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2720–2733, Nov. 2018.

[24] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 1, pp. 136–148, Jan. 2013.

[25] M. Freire, J. Fierrez, M. Martinez-Diaz, and J. Ortega-Garcia, "On the applicability of off-line signatures to the fuzzy vault construction," in *Proc. 9th Int. Conf. Document Anal. Recognit.*, 2007, pp. 1173–1177.

[26] M. Fuentes, S. Garcia-Salicetti, and B. Dorizzi, "On line signature verification: Fusion of a hidden Markov model and a neural network via a support vector machine," in *Proc. 8th Int. Workshop Frontiers Handwriting Recognit.*, 2002, pp. 253–258.

[27] J. Galbally, M. Diaz-Cabrera, M.A. Ferrer, M. Gomez-Barrero, A. Morales, and J. Fierrez, "On-line signature recognition through the combination of real dynamic data and synthetically generated static data," *Pattern Recognit.*, vol. 48, no. 9, pp. 2921–2934, Sep. 2015.

[28] J. Galbally, M. Gomez-Barrero, and A. Ross, "Accuracy evaluation of handwritten signature verification: Rethinking the random-skilled forgeries dichotomy," in *Proc. IEEE Int. Joint Conf. Biometrics*, 2017, pp. 302–310.

[29] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryption," *Pattern Recognit.*, vol. 67, pp. 149–163, 2017.

[30] M. Gomez-Barrero, J. Fierrez, and J. Galbally, "Variable-length template protection based on homomorphic encryption with application to signature biometrics," in *Proc. 4th Int. Conf. Biometrics Forensics*, 2016, pp. 1–6.

[31] M. Gomez-Barrero, J. Galbally, A. Morales, and J. Fierrez, "Privacy-preserving comparison of variable-length data with application to biometric template protection," *IEEE Access*, vol. 5, pp. 8606–8619, 2017.

[32] J. Guerra-Casanova, C. S. Ávila, G. Bailador, and A. de-Santos-Sierra, "Time series distances measures to analyze in-air signatures to authenticate users on mobile phones," in *Proc. Carnahan Conf. Security Technol.*, 2011, pp. 1–7.

[33] D. S. Guru, K. S. Manjunatha, S. Manjunath, and M. T. Somashekara, "Interval valued symbolic representation of writer dependent features for online signature verification," *Expert Syst. Appl.*, vol. 80, pp. 232–243, 2017.

[34] D. Guru and H. Prakash, "Online signature verification and recognition: An approach based on symbolic representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 6, pp. 1059–1073, Jun. 2009.

[35] N. Houmani, S. Garcia-Salicetti, B. Dorizzi, and M. El-Yacoubi, "On-line signature verification on a mobile platform," in *Proc. Int. Conf. Mobile Comput. Appl. Serv.*, 2012, pp. 396–400.

[36] N. Houmani, *et al.*, "BioSecure signature evaluation campaign (BSEC'2009): Evaluating online signature algorithms depending on the quality of signatures," *Pattern Recognit.*, vol. 45, no. 3, pp. 993–1003, 2012.

[37] N. Houmani, *et al.*, "BioSecure signature evaluation campaign (ESRA'2011): Evaluating systems on quality-based categories of skilled forgeries," in *Proc. Int. Joint Conf. Biometrics*, 2011, pp. 1–10.

[38] K. Huang and H. Yan, "On-line signature verification based on dynamic segmentation and global and local matching," *Opt. Eng.*, vol. 34, no. 12, pp. 3480–3487, 1995.

[39] D. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," *IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.)*, vol. 38, no. 5, pp. 609–635, Sep. 2008.

[40] D. Impedovo, G. Pirlo, and F. Rizzi, "Characteristics of constrained handwritten signatures: An experimental investigation," in *Proc. 17th Biennial Conf. Int. Graphonomics Soc.*, 2015, pp. 1–4.

[41] D. Impedovo, R. Modugno, G. Pirlo, and E. Stasolla, "Handwritten signature verification by multiple reference sets," in *Proc. 11th Int. Conf. Frontiers Handwriting Recognit.*, Aug. 19-21, 2008, pp. 125–129, (ISBN: 1-895193-03-6).

[42] Information technology—Biometric data interchange formats—Part 7: Signature/sign time series data, ISO/IEC 19794-7, 2014.

[43] Information technology—Security techniques—Information security management systems, ISO/IEC 27001, 2013.

[44] Information Technology—Security Techniques—Biometric Information Protection. ISO/IEC 24745, 2011.

[45] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 2, pp. 125–143, Jun. 2006.

[46] A. Juels and M. Sudan, "A fuzzy vault scheme," *Proc. IEEE Int. Symp. Inf. Theory*, 2002, Art. no. 408.

[47] Z. Kalal, J. Matas, and K. Mikolajczyk, "P-N learning: Bootstrapping binary classifiers by structural constraints," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, 2010, pp. 49–56.

[48] G. Kambourakis, D. Damopoulos, D. Papamartzivanos, and E. Pavlidakis, "Introducing touchstroke: Keystroke-based authentication system for smartphones," *Secur. Commun. Netw.*, pp. 1–13, 2014.

[49] R. P. Krish, J. Fierrez, J. Galbally, and M. Martinez-Diaz, "Dynamic signature verification on smart phones," in *Proc. Int. Conf. Practical Appl. Agents Multi-Agent Syst.*, 2013, pp. 213–222.

[50] M. Lech and A. Czyżewski, "Handwritten signature verification system employing wireless biometric pen," *Intell. Methods Big Data Ind. Appl. Studies Big Data*, vol 40, pp. 307–319, 2019.

[51] M. López-Garcőa, R. Ramos-Lara, O. Miguel-Hurtado, and E. Cantó-Navarro, "Embedded system for biometric online signature verification," *IEEE Trans. Ind. Inf.*, vol. 10, no. 1, pp. 491–501, Feb. 2014.

[52] E. Maiorana and P. Campisi, "Fuzzy commitment for function based signature template protection," *IEEE Signal Process. Letters*, vol. 17, no. 3, pp. 249–252, Mar. 2010.

[53] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable templates for sequence-based biometrics with application to online signature recognition," *IEEE Trans. Syst. Man Cybern. - Part A: Syst. Hum.*, vol. 40, no. 3, pp. 525–538, May 2010.

[54] E. Maiorana, P. Campisi, J. Ortega-Garcia, and A. Neri, "Cancelable biometrics for HMM-based signature recognition," in *Proc. IEEE 2nd Int. Conf. Biometrics: Theory Appl. Syst.*, 2008, pp. 1–6.

[55] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia, "Towards mobile authentication using dynamic signature verification: useful features and performance evaluation," in *Proc. 19th Int. Conf. Pattern Recognit.*, 2008, pp. 1–5.

[56] M. Martinez-Diaz, J. Fierrez, R. P. Krish, and J. Galbally, "Mobile signature verification: Feature robustness and performance comparison," *IET Biometrics*, vol. 3, no. 4, pp. 267–277, 2014.

[57] A. Mendaza-Ormaza, O. Miguel-Hurtado, R. Blanco-Gonzalo, and F. J. Diez-Jimeno, "Analysis of handwritten signature performances using mobile devices," in *Proc. Carnahan Conf. Security Technol.*, 2011, pp. 1–6.

[58] A. Mendaza-Ormaza, O. Miguel-Hurtado, R. Sánchez-Reillo, and J. Uriarte-Antonio, "Analysis on the resolution of the different signals in an on-line handwritten signature verification system applied to portable devices," in *Proc. 44th Annu. IEEE Int. Carnahan Conf. Security Technol.*, 2010, pp. 341–350.

[59] Y. Meng, *et al.*, "Touch gestures based biometric authentication scheme for touchscreen mobile phones," in *Proc. Int. Conf. Inf. Security Cryptology*, vol. 7763, 2013, pp. 331–350.

[60] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1268–1293, Jul.-Sep. 2015.

[61] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *J. Netw. Comput. Appl.*, vol. 84, pp. 38–54, 2017.

[62] M. Muaaz and R. Mayrhofer, "Smartphone-based gait recognition: from authentication to imitation," *IEEE Trans. Mobile Comput.*, vol. 16, no. 11, pp. 3209–3221, Nov. 1, 2017.

[63] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 88–100, Sep. 2015.

[64] S. Narayanaswamy, J. Hu, and R. Kashi, "User interface for a PCS smart phone," in *Proc. IEEE Int. Conf. Multimedia Comput. Syst.*, 1999, pp. 777–781. e whole authentication system.

[65] K. Niinuma, U. Park, and A. K. Jain, "Soft biometric traits for continuous user authentication," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 771–780, Dec. 2010.

[66] R. Okabe and Y. Yamazaki, "Smart device-based multimodal biometric authentication with the function for environment recognition," in *Proc. 3rd Int. Symp. Comput. Netw.*, 2015, pp. 495–498.

[67] M. Parizeau and R. Plamondon, "A comparative analysis of regional correlation, dynamic time warping, and skeletal tree matching for signature verification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 12, no. 7, pp. 710–717, Jul. 1990.

[68] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," *IEEE Signal Process. Mag.*, vol. 33, no. 4, pp. 49–61, Jul. 2016.

[69] P. Perera and V. M. Patel, "Efficient and low latency detection of intruders in mobile active authentication," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1392–1405, Jun. 2018.

[70] G. Pirlo, V. Cuccovillo, M. Diaz-Cabrera, D. Impedovo, and P. Mignone, "Multidomain verification of dynamic signatures using local stability analysis," *IEEE Trans. Hum.-Mach. Syst.*, vol. 45, no. 6, pp. 805–810, Dec. 2015.

[71] G. Pirlo, M. Diaz, M. A. Ferrer, D. Impedovo, and F. Rizzi, "Behaviour of dynamic and static feature dependences in constrained signatures," in *Proc. 13th Int. Conf. Document Anal. Recognit.*, 2015, pp. 1278–1281.

[72] G. Pirlo and D. Impedovo, "Adaptive score normalization for output integration in multiclassifier systems," *IEEE Signal Process. Letters*, vol. 19, no. 12, pp. 837–840, Dec. 2012.

[73] G. Pirlo, F. Rizzi, A. Vacca, and D. Impedovo, "Interoperability of biometric systems: Analysis of geometric characteristics of handwritten signatures," in *Proc. Workshops New Trends Image Anal. Process.*, vol. 9281, 2015, pp. 242–249.

[74] R. Plamondon and G. Lorette, "Automatic signature verification and writer identification - the state of the art," *Pattern Recognit.*, vol. 22, no. 2, pp. 107–131, 1989.

[75] R. Plamondon, G. Pirlo, and D. Impedovo, "Online signature verification," in *Handbook of Document Image Processing and Recognition*, 2014, pp. 917–947.

[76] R. Plamondon and S. N. Srihari, "On-line and off-line handwriting recognition: A comprehensive survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 1, pp. 63–84, Jan. 2000.

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

[78] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proc. Int. Conf. Audio- Video-Based Biometric Person Authentication*, 2001, pp. 223–228.

[79] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Security*, vol. 2011, 2011, Art. no. 3.

[80] A. Ross and R. Nadgir, "A thin-plate spline calibration model for fingerprint sensor interoperability," *IEEE Trans. Knowl. Data Eng.*, vol. 20, no. 8, pp. 1097–1110, Aug. 2008.

[81] N. Sae-Bae and N. Memon, "Online signature verification on mobile devices," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 6, pp. 933–947, Jul. 2014.

[82] H. Saevanee and P. Bhattarakosol, "Authenticating user using keystroke dynamics and finger pressure," in *Proc. IEEE 6th Consum. Commun. Netw. Conf.*, 2009, pp. 1–2.

[83] R. Sanchez-Reillo, "Signature analysis in the context of mobile devices," *Image Vis. Comput.*, vol. 55, pp. 34–37, 2016.

[84] R. Sanchez-Reillo, R. Blanco-Gonzalo, O. Miguel-Hurtado, and A. Mendaza-Ormaza, "Migrating biometrics to mobile scenarios: Performance and usability evaluation," in *Proc. IBPC*, 2012, pp. 1–39.

[85] R. Sanchez-Reillo, H. C. Quiros-Sandoval, I. Goicoechea-Telleria, and W. Ponce-Hernandez, "Improving presentation attack detection in dynamic handwritten signature biometrics," *IEEE Access*, vol. 5, pp. 20463–20469, 2017.

[86] A. Shahzad and M. Hussain, "Security issues and challenges of mobile cloud computing," *Int. J. Grid Distrib. Comput.*, vol. 6, no. 6, pp. 37–50, 2013.

[87] M. Shahzad, A. X. Liu, and A. Samuel, "Behavior based human authentication on touch screen devices using gestures and signatures," *IEEE Trans. Mobile Comput.*, vol. 16, no. 10, pp. 2726–2741, Oct. 1, 2017.

[88] C. Shen, Y. Zhang, X. Guan, and R. A. Maxion, "Performance analysis of touch-interaction behavior for active smartphone authentication," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 498–513, Mar. 2016.

[89] B. Shrestha, N. Saxena, and J. Harrison, "Wave-to-access: Protecting sensitive mobile device services via a hand waving gesture," in *Proc. Cryptology Netw. Security*, 2013, pp. 199–217.

[90] J. Swanepoel and J. Coetzer, "Feature weighted support vector machines for writer-independent on-line signature verification," in *Proc. 14th Int. Conf. Frontiers Handwriting Recognit.*, 2014, pp. 434–439.

[91] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "Benchmarking desktop and mobile handwriting across COTS devices: The e-BioSign biometric database," *PloS One*, vol. 12, no. 5, 2017, Art. no. e0176792.

[92] R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia, and J. Fierrez, "Update strategies for HMM-based dynamic signature biometric systems," in *Proc. IEEE Int. Workshop Inf. Forensics Security*, 2015, pp. 1–6.

[93] R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia, and J. Fierrez, "Preprocessing and feature selection for improved sensor interoperability in online biometric signature verification," *IEEE Access*, vol. 3, pp. 478–489, 2015.

[94] R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia, and J. Fierrez, "Increasing the robustness of biometric templates for dynamic signature biometric systems," in *Proc. Int. Carnahan Conf. Security Technol.*, 2015, pp. 229–234.

[95] U. Uludag, A. Ross, and A. Jain, "Biometric template selection and update: A case study in fingerprints," *Pattern Recognit.*, vol. 37, no. 7, pp. 1533–1542, Jul. 2004.

[96] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proc. IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

[97] R. Vera-Rodriguez, R. Tolosana, J. Ortega-Garcia, and J. Fierrez, "e-BioSign: Stylus-and finger-input multi-device database for dynamic signature recognition," in *Proc. 3rd Int. Workshop Biometrics Forensics*, 2015, pp. 1–6.

[98] C. Vielhauer. Biometric User Authentication for IT Security—From Fundamentals to Handwriting. Boston, MA, USA: Springer, 2006.

[99] C. Vielhauer, R. Steinmetz, and A. Mayerhöfer, "Biometric hash based on statistical features of online signatures," in *Proc. Object Recognit. Supported User Interaction Serv. Robots*, vol. 1, 2002, pp. 123–126.

[100] M. Wolf, "Behavioral biometric identification on mobile devices," in *Proc. Int. Conf. Augmented Cognition*, 2013, pp. 783–791.

[101] Q. Z. Wu, I. C. Jou, and S.Y. Lee, "On-line signature verification using LPC cepstrum and neural networks," *IEEE Trans. Syst. Man Cybern. Part B (Cybern.)*, vol. 27, no. 1, pp. 148–153, Feb. 1997.

[102] K. Xi and J. Hu. "Bio-cryptography," *Handbook of Information and Communication Security*, Berlin, Germany: Springer, 2010, pp. 129–157.
[103] L. Yang, Y. Guo, X. Ding, J. Han, Y. Liu, C. Wang, and C. Hu, "Unlocking smart phone through handwaving biometrics," *IEEE Trans. Mobile Comput.*, vol. 14, no. 5, pp. 1044–1055, May 2015.
[104] W. K. Yip, A. Goh, D. C. L. Ngo, and A. B. J. Teoh, "Generation of replaceable cryptographic keys from dynamic handwritten signatures," in *Proc. Int. Conf. Biometrics*, 2006, pp. 509–515.
[105] M. Zalasinski and K. Cpalka, "A new method for signature verification based on selection of the most important partitions of the dynamic signature," *Neurocomputing*, vol. 289, pp. 13–22, 2018.
[106] F. J. Zareen and S. Jabin, "Authentic mobile-biometric signature verification system," *IET Biometrics*, vol. 5, no. 1, pp. 13–19, 2016.
[107] H. Zhang, X. Liu, and C. Chen, "An online mobile signature verification system based on homomorphic encryption," *Int. J. Innovative Comput. Inf. Control*, vol. 13, no. 5, pp. 1623–1635, Oct. 2017.
[108] N. Zheng, K. Bai, H. Huang, and H. Wang, "You are how you touch: User verification on smartphones via tapping behaviors," in *Proc. IEEE Int. Conf. Netw. Protocols*, 2014, pp. 221–232.

DONATO IMPEDOVO (M'08-SM'17) received the MEng degree cum laude in computer engineering and the PhD degree in computer engineering. He is associate professor with the Department of Computer Science of the University of Bari (IT). His research interests include field of signal processing, pattern recognition, machine learning and biometrics. He is co-author of more than 80 articles on these fields in both international journals and conference proceedings. He received the "distinction" award in May 2009 at the International Conference on Computer Recognition Systems (CORES – endorsed by IAPR), and the first prize of the first Nereus-Euroavia Academic competition on GMES in October 2012. He is also very involved in research transfer activities as well as in industrial research, he has managed more than 25 projects funded by public institutions as well as by private SMEs. He is IEEE Access associate editor and he serves as reviewer for many international journals including *IEEE Access*, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *Pattern Recognition* and many others. He was the general co-chair of the International Workshop On Artificial Intelligence With Application In Health (WAIAH2017), of the International Workshop on Emergent Aspects in Handwritten Signature Processing (EAHSP 2013) and of the International Workshop on Image-Based Smart City Application (ISCA 2015). He was a reviewer in the scientific committee and program committee of many international conferences in the field of computer science, pattern recognition and signal processing, such as the ICPR and ICASSP. He is IAPR and IEEE senior member.

GIUSEPPE PIRLO (M'92–SM'13) received the degree in computer science (cum laude) from the Department of Computer Science, University of Bari, Italy, in 1986. Since 1986, he has been carrying out research in the field of computer science and neuroscience, signal processing, handwriting processing, automatic signature verification, biometrics, pattern recognition and statistical data processing. Since 1991, he has been an assistant professor with the Department of Computer Science, University of Bari, where he is currently an full professor. He developed several scientific projects and authored more than 250 papers on international journals, scientific books and proceedings. He is currently an associate editor of the *IEEE Transactions on Human–Machine Systems*. He also serves as a Reviewer for many international journals including the *IEEE Transactions on Pattern Analysis and Machine Intelligence*, the *IEEE Transactions on Fuzzy Systems*, the *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, the *IEEE Transactions on Evolutionary Computation*, the *IEEE Transactions on Image Processing*, the *IEEE Transactions on Information Forensics and Security*, the *Pattern Recognition*, the *International Journal on Document Analysis and Recognition*, and the *Information Processing Letters*. He was the general chair of the International Workshop on Emerging Aspects in Handwriting Signature Processing, Naples, in 2013, the International Workshop on Image-based Smart City Applications, Genoa, in 2015, and the general co-chair of the International Conference on Frontiers in Handwriting Recognition, Bari, in 2012. He was a reviewer in the scientific committee and program committee of many international conferences in the field of computer science, pattern recognition and signal processing, such as the ICPR, the ICDAR, the ICFHR, the IWFHR, the ICIAP, the VECIMS, and the CISMA. He is also the editor of several books. He was an editor of the Special Issue Handwriting Recognition and Other PR Applications of the *Pattern Recognition* Journal in 2014 and the Special Issue *Handwriting Biometrics of the IET Biometrics* Journal in 2014. He was the guest editor of the Special Issue of the Je-LKS Journal of the e-Learning and Knowledge Society Steps toward the Digital Agenda: Open Data to Open Knowledge in 2014. He is currently the guest co-Editor of the Special Issue of the *IEEE Transactions on Human–Machine Systems on Drawing and Handwriting Processing for User-Centered Systems*. He is a member of the Governing Board of Consorzio Interuniversitario Nazionale per l'Informatica (CINI), a member of the Governing Board of the Società Italiana di e-Learning and the e-learning Committee of the University of Bari. He is currently the deputy representative of the University of Bari in the Governing Board of CINI. He is also the managing advisor of the University of Bari for the Digital Agenda and Smart Cities. He is the chair of the Associazione Italiana Calcolo Automatico-Puglia. He is also a member of the Gruppo Italiano Ricercatori Pattern Recognition, the International Association Pattern Recognition, the Stati Generali dell'Innovazione, and the Gruppo Ingegneria Informatica. He is a senior member of the IEEE.