Cognitive Computation (2020) 12:940–953
https://doi.org/10.1007/s12559-020-09755-z

Handwriting Biometrics: Applications and Future Trends in e-Security and e-Health

Marcos Faundez-Zanuy[1] · Julian Fierrez[2] · Miguel A. Ferrer[3] · Moises Diaz[4] · Ruben Tolosana[2] · Réjean Plamondon[5]

Received: 4 March 2020 / Accepted: 19 July 2020 / Published online: 12 August 2020

Abstract
Online handwritten analysis presents many applications in e-security, signature biometrics being the most popular but not the only one. Handwriting analysis also has an important set of applications in e-health. Both kinds of applications (e-security and e-health) have some unsolved questions and relations among them that should be addressed in the next years. We summarize the state of the art and applications based on handwriting signals. Later on, we focus on the main achievements and challenges that should be addressed by the scientific community, providing a guide for future research. Among all the points discussed in this article, we remark the importance of considering security, health, and metadata from a joint perspective. This is especially critical due to the risks inherent when using these behavioral signals.

Keywords Online handwriting · Biometrics · e-Security · e-Health · Privacy

Introduction

Online handwriting biometric systems belong to behavioral biometrics as they are based on actions performed by a specific subject [1]. This is complementary to morphological biometrics, which are based on direct measurements of physical traits of the human body [1, 2]. From a human behavior and health condition perspective, online handwriting biometrics are more appealing and informative than other popular biometrics traits such as fingerprints or iris [3, 4]. Although health applications based on online handwriting have not been explored in-depth yet, there is a considerable set of possibilities that will probably be developed in the near future, such as diagnosis/monitoring of depression, neurological diseases, and drug abuse [5]. It can be noted that nowadays, most of the published research in biometric signal processing is based on image and speech. This might be linked to the fact that these signals are simpler and cheaper to acquire compared with others such as online handwriting where specific digitizing tablets are needed. Fortunately, online handwriting signals are more present in our society than a few years ago due to the increasing popularity of tactile devices and their corresponding cost reduction [6]. Thus, the price of the acquisition device is no longer a drawback nowadays. Also, most commercial off-the-shelf (COTS) smartphone devices incorporate handwriting capabilities. As a result, we forecast a considerable

✉ Marcos Faundez-Zanuy
faundez@tecnocampus.cat

Julian Fierrez
julian.fierrez@uam.es

Miguel A. Ferrer
miguelangel.ferrer@ulpgc.es

Moises Diaz
moises.diaz@atlanticomedio.es

Ruben Tolosana
ruben.tolosana@uam.es

Réjean Plamondon
rejean.plamondon@polymtl.ca

[1] School of Engineering Tecnocampus, Pompeu Fabra University, Mataró, Barcelona, Spain

[2] School of Engineering, Universidad Autonoma de Madrid, Madrid, Spain

[3] Instituto Universitario para el Desarrollo Tecnológico y la Innovación en Comunicaciones, Universidad de Las Palmas de Gran Canaria, Las Palmas, Spain

[4] Universidad del Atlántico Medio, Las Palmas de Gran Canaria, Las Palmas, Spain

[5] Département de Génie électrique, Polytechnique Montréal, Montréal, Canada

growth in applications in this field. Indeed, in a near future, these pen-based handheld devices (tablets, phablets, cellphones, etc.) will help to protect people's sensitive data, for example, incorporating automatic signature verification and writer identification. Moreover, the same devices could be used to monitor user fine motor control to detect stress, aging, and health problems [5]. In this dual context, privacy issues will have to be seriously investigated. This will be especially important when the double use is possible. Ideally, samples acquired for security purposes (e.g., grant access to a facility or authorize a payment) should not be able to reveal health information of the user. Conversely, samples acquired for health monitoring should be anonymized and not convey user identity information [7]. Figure 1 shows an overview of the main application scenarios of biometric handwriting in both security and health fields. It is worth pointing out that this is not a biometric-specific problem. For instance, in [8], similar problems are discussed in relation to loyalty cards provided by supermarkets. The advantage for the customer is that he gets discounts and points that can be exchanged for prizes. The advantage for the company is that it can rationalize the products' distribution along the supermarket and take better care of their prices' politics, stock, etc. However, consumers are not aware about the risk of permitting that the supermarket stores this information. A secondary/double use could be other companies willing to pay for information about which kind of products is purchased by a given person (tobacco, alcohol, drugs, etc.), which kinds of videos are rented, how much money spends each month, etc. Doubtless, consumption habits are more personal and private than some biometric traits, and special care must be taken for this information, although the offers of the companies seem quite tentative.

The challenges and opportunities of handwriting biometrics for e-security and e-health outlined before are particularly well suited to be advanced in the framework of cognitive computing. Combined work considering at the same time both disciplines (biometrics and cognitive computing) can be seen in a few selected works in the past [9–12], but still many synergies between them are to be exploited in future research and development.

According to the Cognitive Computing Consortium, cognitive computing systems must have five key attributes, as listed below [13, 14]:

- Adaptive: Cognitive systems must be flexible enough to learn as information changes and as goals evolve. The systems must be able to make adjustments as the data and environment change, such as user stress.
- Interactive: Human-computer interaction (HCI) is a critical component in cognitive systems. Users must be able to

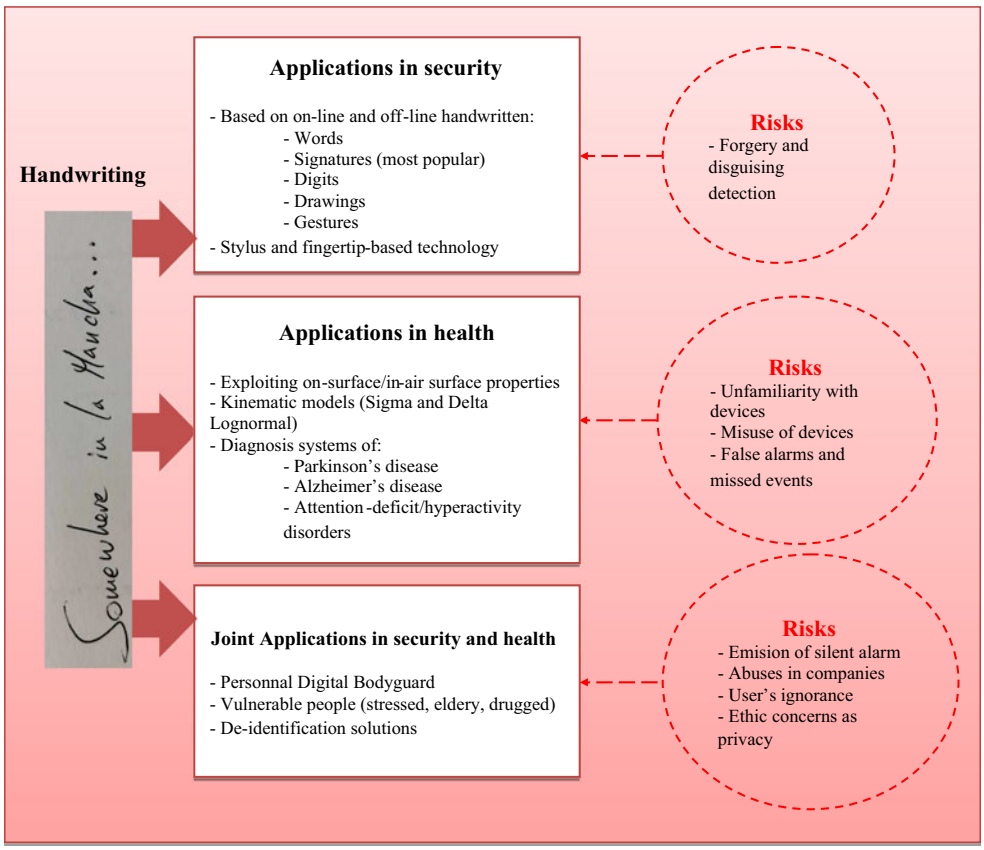

Fig. 1 Exploiting on-surface/in-air propierties for biometric handwriting

interact with cognitive machines and define their needs as those needs change, maybe due to aging or temporary health state.
- Iterative and stateful: Cognitive computing technologies can also identify problems by asking questions or pulling in additional data, if a stated problem is vague or incomplete.
- Contextual: Understanding context is critical in thought processes, and so cognitive systems must also understand, identify, and mine contextual data. They may draw on multiple sources of information present in a given handwriting task.

A handwriting biometric system should be aware and take advantage of the rich amount of information that can be extracted from a very simple handwriting task, as described in the next sections. This is because handwriting is a cognitive task in which synchronized neuromotor orders are fired from the cortex to carry out the planned action [15, 16]. Signal processing and pattern recognition techniques applied to analyze this procedure can reveal very useful information about the writer, including its identity and health state.

The present paper summarizes the current research in handwriting biometrics with applications to e-security and e-health under the umbrella of cognitive computing principles: adaptiveness, interactivity, iterativity, and context. We focus our discussion on the accuracy, performance, utility, application factors, and challenges of handwriting analysis in such application scenarios, also foreseeing trends and potential research lines for the future. More comprehensive surveys of the state of the art in handwriting analysis for security and health can be found elsewhere [3, 5 17–19].

The Biometric Data Behind Handwriting

The acquisition devices considered in online handwriting allow to capture various properties of the moving pen (or fingertip [20]) during the whole writing process in real time. These time-stamped sequences of points typically give the digital representation of the signal. For instance, digitizing tablets typically acquire the following information:

- Position of pen tip in X-axis
- Position of pen tip in Y-axis
- On-surface/in-air pen position information
- Pressure applied by the pen tip
- Azimuth angle of the pen with respect to the tablet's surface
- Altitude angle (a.k.a. tilt) of the pen with respect to the tablet's surface
- Timestamp

An example of this information is given in Fig. 2 for both healthy and unhealthy handwritings.

From this set of dynamic raw data, further information can be inferred or derived, which is usually more suitable for certain applications (e.g., handwriting velocity, duration, width, height) [22, 23]. Some digitizing devices such as Wacom Intuos tablet and Samsung Galaxy Note are able to track the pen tip movement even when it is not touching the surface (see Fig. 3). Thus, it is possible to record the X and Y coordinates of in-air movements when pressure is null. Unfortunately, this is only possible when the distance between the tip of the pen and the surface is less or equal to approximately 1 cm; otherwise, the tracking is lost. Nevertheless, the in-air time spent is still known because the acquisition device provides a timestamp for each sample [24]. In-air information cannot be obtained with "classic" off-line methods (scanning the ink-pen handwriting once the task is finished), and the timing information is also lost or very difficult to recover [24, 25].

An accurate complete recording of in-air information requires other 3D sensors. Possibly, the more appropriate for handwriting are the Motion Capture (MOCAP) sensors. These sensors are based on either video or inertial measurement units (IMUs), i.e., accelerometer, gyroscope, and magnetometer. The first ones, e.g., Vicon system (www.vicon.com), use the image from multiple cameras to calculate the 3D position of the target, which could be the tip of the pencil or a fingertip, where a marker is attached. The second ones are based on IMUs, such as neuronmocap (https://neuronmocap.com), which require a glove in which sensors are plugged in to track the 3D trajectory. In both cases, it is possible to sample the position of the marker or IMUs around 100 times per second (i.e., 100 Hz). The major problem of the first ones is the occlusion while the downside of the second is the offset drift of the accelerometers. Besides, the first one must be used in a fixed space while the second is portable. Anyway, both procedures are reliable systems for 3D tracking which, although not massively used in nowadays handwriting biometric applications, is a promising research line to be explored. We have everything in hand to design 2D and 3D systems from the acquisition hardware point of view. While 2D models and algorithms are a reality, the potential of 3D systems is yet to be explored.

Security Applications

According to [26], verification and recognition are two classical studies carried out with handwriting specimens. In the context of biometric security, applications based on handwriting tasks are mainly based on signatures. Several international competitions summarize the state of the art achieved by dozens of teams, such as BSEC [27], SVC [28], and

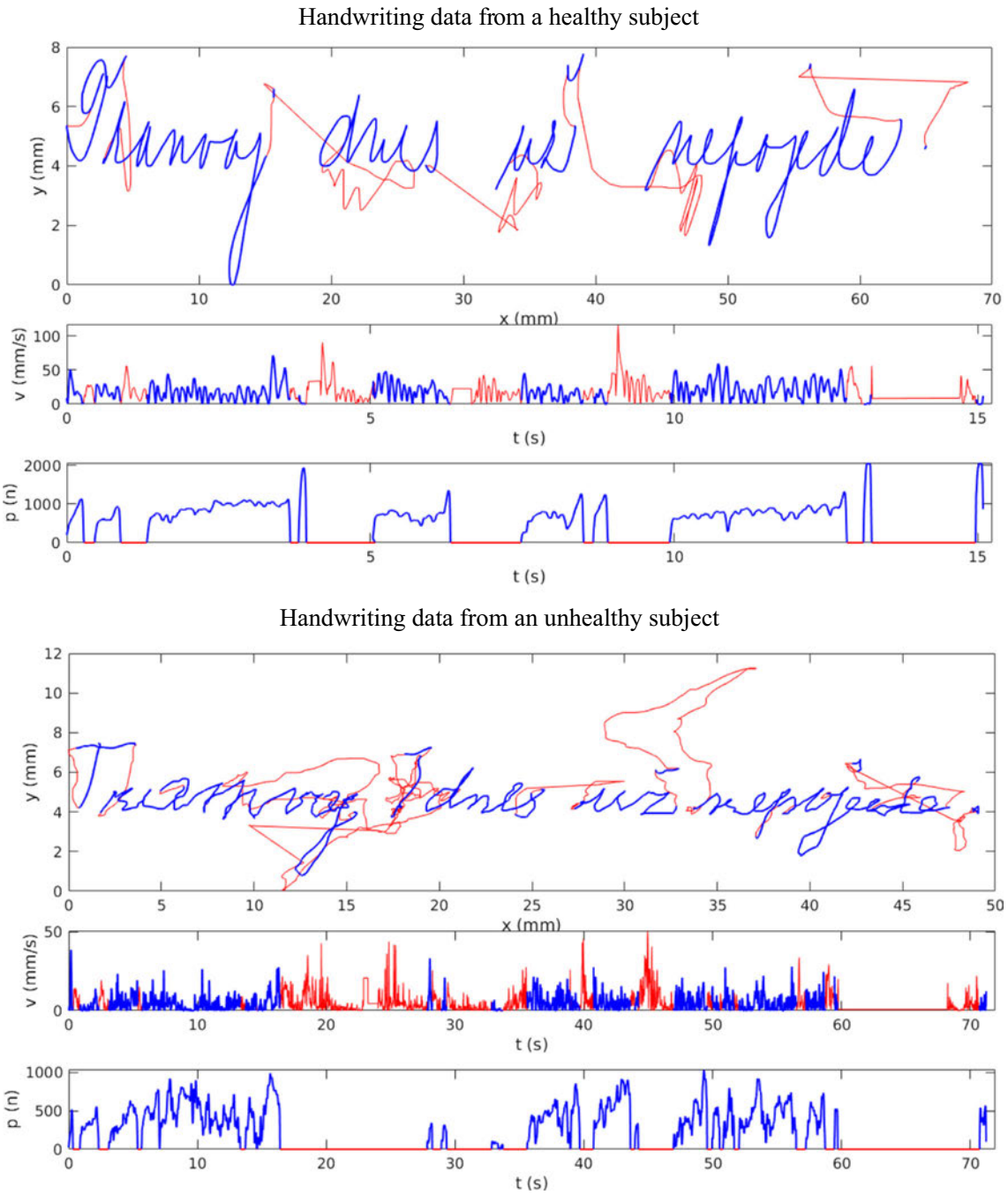

Fig. 2 Online handwriting from healthy and unhealthy subjects: in-air handwriting in solid red line and on-surface handwriting in solid blue line. (Figure extracted from PaWaH database [21])

SigWIComp [29]. Although less known, there are also some studies (e.g., [30–32]) where biometric recognition is based on handwritten text, either text dependent or independent.

Several authors have demonstrated the individuality of handwriting. It has been assessed in the offline case, for example, in [21]. These researchers collected a database of 1500 writers selected to be representative of the US population and conducted experiments on identification and verification. Regarding writer identification, they reached an accuracy of about 83% at the word level (88% at the paragraph level and 98% at the document level). These results allowed the authors to conclude that the individuality hypothesis, with respect to the target population, was true with a 95% confidence level. Another study [30] complemented the previous work of [32]. They analyzed the individuality of four handwritten words (*been*, *Cohen*, *Medical*, and *referred*) taken from 1027 US individuals who wrote each word three times. The combination of the

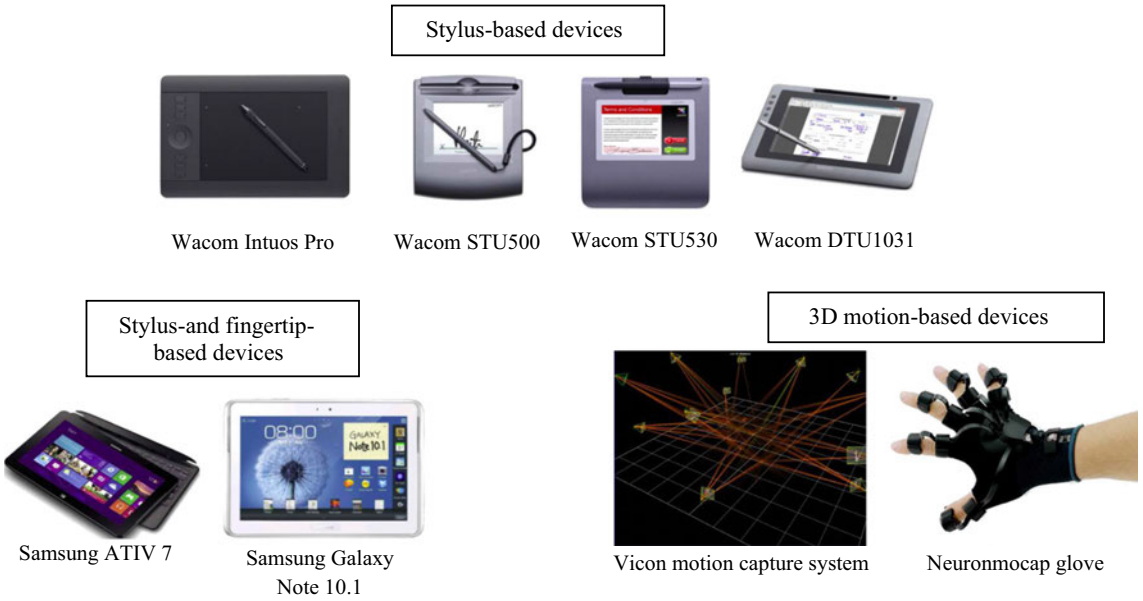

Fig. 3 Devices for capturing handwriting information. Illustration designed using figures extracted from: [6], https://thumb.pccomponentes.com/w-530-530/articles/5/59297/wacom-intuos-pro-small-1.jpg, www.virtualrealityreviewer.com/wp-content/uploads/2014/09/PERCEPTION-NEURON.jpg, and https://www.researchgate.net/profile/Ron_Wakkary/publication/221572400/figure/download/fig3/AS:305541982244866@1449858293504/Graphical-view-of-the-Vicon-motion-capture-system-Twelve-cameras-are-used-to-reconstruct.png

four words yielded an identification accuracy of about 83% and a verification accuracy of about 91%.

With regard to the online case, some authors have addressed the issue of the individuality of single words and short sentences. Hook et al. [31] showed that single words (the German words *auch*, *oder*, *bitte*, and *weit*) and the short sentence *Guten Morgen* exhibit both considerable reproducibility and uniqueness (i.e., equal items written by the same person match well while equal items written by different people do not match so well). They used a small database consisting of 15 writers that produced, in a single session, ten repetitions of each item captured by a prototype of a digitizing pen. In [33] the English words *February*, *January*, *November*, *October*, and *September* were used (25 repetitions of each word donated by 45 writers). The identification rate reached 95%. In [34] a writer identification rate of 92.38% and a minimum detection cost function of 0.046 (4.6%) were achieved with 370 users using just one word written in capital letters. Results were improved up to 96.46% and 0.033 (3.3%) when combining two words. In [35], signatures, initials, and keywords were compared.

More recently, in [20] writer verification rates of 96.2% were achieved for handwritten passwords consisting of 7 digits written with the fingertip over the touchscreen of COTS smartphones and 94.1% for 4-digit passwords. In a subsequent study, the same authors were able to obtain similar authentication accuracy for more challenging and realistic acquisition conditions (in the wild including cross-device comparisons over a diverse pool of COST smartphones consisting of 94 different models) by considering characters and symbols instead of only numerical digits to construct the passwords [36].

In a separate line of research, some authors have also explored handwriting information from drawings and other graphical information generated with stylus- or finger-based inputs for authentication [37], usually resulting in worse performance as compared to natural handwriting or signature data [38]. Anyway, the results obtained based on graphical inputs may be acceptable for some low-security applications or helpful as a second authentication factor (e.g., in smartphone login applications [39]).

It is also worth pointing out some forensic challenges approached mainly in offline handwriting. The two main tasks addressed by forensics are forgery detection and disguising. Forgeries refer to a writer imitating the handwriting of other writers while disguising means a writer trying to conceal his usual writing habits and to make the new writing as different as possible to his own writing [40]. An open question is, knowing that a handwriting specimen is a forgery, how to detect who has forged the handwriting. Some attempts have been made [41] to track this problem but with poor results. Regarding disguising, this problem has also attracted much attention in the forensic area. This problem arises when the author changes his own handwriting. The purpose could be for the later denial of the own handwriting, in which case it is also termed as "auto-simulation." Note that both genuine and disguised texts are written by the author of the specimen but with different intentions. A writer produces a genuine text that allows author identification. Whereas a disguised handwriting is written to make it look like a forgery for a possible later denial. These cases have been mainly studied in handwriting signatures [42, 43]. The difficulty of forensic-based challenges can

be faced by online systems. Since they have the advantage of having the timing information, it is expected better results in a near future.

Health Applications

Although most of the many existing studies related to handwriting and handwritten signatures have been based on on-surface movements (see, e.g., [1, 18]), some studies have pointed out the importance of in-air movements as well. In [44] the authors performed an entropy analysis of handwriting samples acquired from a group of 100 people (for more information, refer to BiosecurID database [45]) and observed that both types of movements contain approximately the same amount of information. Moreover, based on the values of mutual information, these movements appear to be notably non-redundant. This property has been advantageously used in several fields of science. For instance, the authors in [21, 46] proved that in-air movement increases the accuracy of Parkinsonic dysgraphia identification. Specifically, when classifying the Parkinsonic dysgraphia by support vector machines (SVM) in combination with the in-air features, they reached 84% accuracy which is 6% better in comparison with classification based on on-surface features only. When combining both feature sets, they observed 86% classification accuracy. Similar accuracy rates were obtained in a different study by [47], which analyzed various handwriting tasks to discriminate between Parkinson's disease (PD) vs. elder healthy controls. Better accuracy rates around 96% were also obtained in [47] when comparing PD vs. young healthy controls.

The in-air movement also supports the diagnosis of Alzheimer's disease (AD) [48]. These researchers observed that patients with AD spend 7 times longer in-air when compared with a control group. In the case of on-surface movement, it is only 3 times longer. Similarly, [49] found out that the in-air duration can be a good measure for performance analysis of children with a high-functioning autism spectrum disorder. The in-air movement has also been used for the identification and the quantitative analysis of developmental dysgraphia in child population [50–52]. In [50], it was proved that kinematic features derived from this kind of movement (especially jerk, which is the rate at which the acceleration of a pen changes with time) provide good discrimination power between children with dysgraphia and the control group.

On the other hand, there is a successful research line in handwriting analysis for health applications based on kinematic models. There exist many theories that have tried to model the speed profile of human movement in general and handwriting in particular [53]. Among the models which provide analytical representations, the kinematic theory of rapid human movements [54–56] and its delta- and sigma-lognormal models have been used to explain most of the basic phenomena reported in classical studies on human motor control [57] and to study several factors involved in the fine motricity [58].

As can be seen in Table 1, the sigma-lognormal model represents a breakthrough due to its feasibility and reliability to describe a wide range of human movements. One of the main advantages of this model is that it considers physical body features such as the neuromuscular system responsible for the production of human movements and thus reflects some personal characteristics difficult to impersonate. To work out the sigma-lognormal parameters, the robust Xzero algorithm implemented by the ScriptStudio application was proposed in 2007 [78] and iDeLog was proposed in 2020 [79]. Since its first version, it was quickly widespread, and several improvements have been published, for instance, [80]. From a fundamental perspective, the powerfulness of this methodology relies on the lognormality principle [81] which states that the lognormal velocity profiles observed in handwriting and signature reflect the behavior of individuals who are in perfect control of their movements [22]. As a corollary, motor control learning in young children can be interpreted as a migration towards lognormality while, as

Table 1 Some kinematic theory applications related to handwriting biometrics

Health-based applications	Security-based applications	Other handwriting-based applications
Temporal evolution of handwriting skills [59]	Signature verification systems [58, 60]	Western [61] and Indian [62] handwriting generation
Tools to help children learning handwriting [63]	Training improvements with duplicates data augmentation [64]	Gesture generation [65]
Tools for neuromuscular health care [66]	Forgery detection improvements [67]	Captcha generation [68],
Motor control disorders and brain strokes-based systems [69]	On-line learning improvements with handwriting generation [70]	Graffities design [71]
Parkinson disease-based systems [72]		Mouse movement analysis [73],
Turn cranio-caudal signature characterization [74].		Uni and bi manual drawing movements [75]
Children with ADHD [76]		Human machine Interface [77]

aging and health issues intensify, a progressive departure from lognormality is occurring. For the greater part of their lives, healthy human adults take advantage of their lognormality to control their movements efficiently [82].

For a recent review of handwriting analysis to support neurodegenerative diseases diagnosis, see [3, 17, 46, 83].

Metadata Applications

Behavioral biometrics, in addition to security and health applications, can provide additional information, known as metadata. Sometimes also referred to as soft biometrics [84], they can be based on system hardware specifics (technical metadata) or on personal attributes (non-technical metadata) [85, 86]. System-related metadata represent the physical characteristics of biometric sensors and are essential for ensuring the minimum acceptable quality of the raw biometric signals. Previous work in personal related metadata has shown that it is possible to estimate some metadata like script language, dialects, origin, gender, and age by statistically analyzing human handwriting.

As examples of gender recognition based on handwriting, we can mention the following works. In [10] using only four repetitions of a single uppercase word, the average rate of well-classified writers is 68%; with sixteen words, the rate rises to an average of 72.6%. Statistical analysis reveals that the rates mentioned above are highly significant. In order to explore the classification potential of the in-air strokes, these were also considered. In that case, results were not conclusive, with an average of 74% well-classified writers when information from in-air strokes was combined with information from on-surface ones. This rate is slightly better than the one achieved by calligraphic experts. However, we should keep in mind that this is a two-class problem and even by pure chance we would get 50% accuracy.

A system that classifies handwriting into demographic categories using measurements such as pen pressure, writing movement, stroke formation, and word proportion has been proposed in [17]. The authors reported classification accuracies of 77.5%, 86.6%, and 74.4% for gender, age, and handedness classification, respectively. In this study, all the writers produced the same letter. Authors in [87] also addressed the classification of gender and handedness in the online mode. The authors used a set of 29 features extracted from both online information and its offline representation and applied SVM and Gaussian mixture models (GMM) to perform the classification. The authors reported accuracy of 67.06% for gender classification and 84.66% for handedness classification. In [88], the researchers separately reported the performance of the offline mode, the online mode, and their combination. The accuracy for the offline mode was 55.39%.

Emotional states, such as anxiety, depression, and stress, can be assessed by the Depression Anxiety Stress Scales (DASS) questionnaire. A new database that relates emotional states to handwriting and drawing tasks acquired with a digitizing tablet has been presented in [89]. Experimental results show that the recognition of anxiety and stress was better than depression recognition. This database includes samples of 129 participants whose emotional states were assessed by the DASS questionnaire and is freely distributed for those interested in research in this line.

Applications Combining Security and Health: Issues and Challenges

Security and health applications have been discussed in the previous sections as fields isolated from each other. They are indeed studied separately for most of the scientific community. However, in some cases, both should be fully considered jointly as they cannot be completely isolated one from the other (see Fig. 4). This is particularly true in the context of the Personal Digital Bodyguard vision [5] which aims at supplementing people's sensitive data protection with signature and writer verification.

Most biometric security applications only try to determine the identity of a subject or to verify if he/she is the person who claims to be. However, in the context of the acquisition of biometric signals with different devices and data quality [54, 90], it may be beneficial to gather some additional information for the system to be context-aware [12], as envisioned by the cognitive computation initiative. In the following, we summarize three of such possible scenarios:

a) Is the subject stressed? It is not the same problem to confirm the identity and open a door if, for example, the subject's heart is beating at 70 beats per minute (bpm) or if it is beating at 120 bpm. If the heart is much more accelerated than normal, some suspicious activity can be happening (e.g., the user is being coerced). To solve this, some biometric systems have a mechanism to notify security guards or the police about the coerced situation without letting the threatening person notice it. To do that, the user may have enrolled at least two different biometric templates. Both will open the door, but one of them will activate a silent alarm. This concept is known as duress detection [91]. This knowledge can also be obtained just considering how the subject interacted with the sensor in previous days. Similarly, the user can enroll in a couple of different signatures, one for duress recognition and the other one, for a normal operation. Again, it would be possible for a third party to be familiar with the genuine signature that does not activate any silent alarm and to force the user to use that signature.

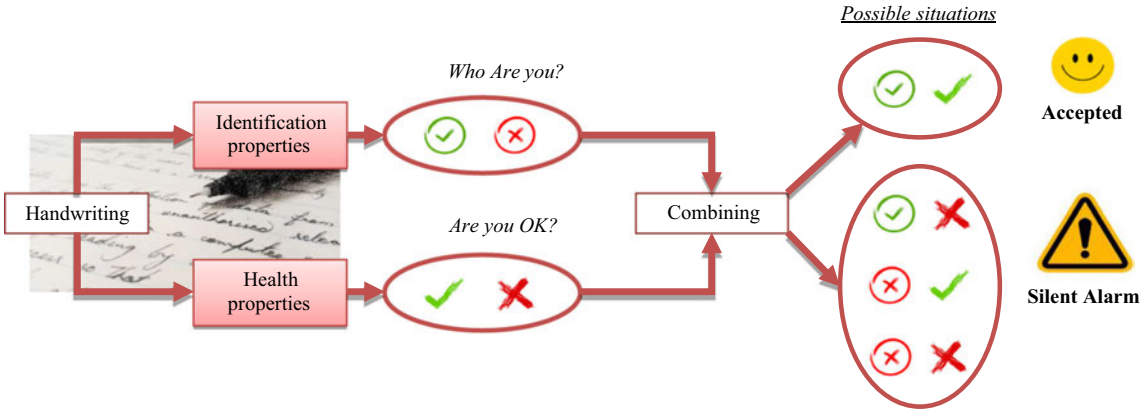

Fig. 4 Towards a combination of identification and health properties of biometric handwriting information

A robust biometric security system should be able to detect the stress situation based on characteristics that cannot be easily controlled by the user. Detection of user stress from signature or handwriting is a challenging research topic that can indeed improve security systems.

b) Is the subject suffering from any disease that makes him unable to understand the real implications of his acts? In [11], we presented the case of a woman affected by Alzheimer's disease. In that case, several women made an elderly woman sign her name on blank sheets of paper, alleging that they needed her signature to get some of her medicines. When the elder woman died, the women took advantage of the signed sheets in order to write a rental agreement. The declared date of this agreement was 1985, but several documents signed in 1986 showed better control of calligraphic movements. In fact, the hesitantly written signature document signed in 1985 was closer in appearance to the blank sheets signed when the elderly woman had dementia than to the 1986 document. Thus, it was demonstrated that in fact, the rental document was not signed in 1985 but later. While this is an offline example from the 1980s of the past century, we can forecast in a near future situations like this one for the online case.

Another possibility is to be affected by depression. Drawings for analyzing depressive disorders in older people were used in [92].

These two examples indicate that even if in the context of biometric signature verification one can conclude that the signature is genuine, this may not be enough. One may in addition take into account aspects such as the health state of the subject. Considering both aspects (identity and health), it can be concluded that, from a legal point of view, a signature is not valid because the subject may not have been in a sound state of mind. In such situations, the biometric authentication of the individual does not solve the problem and some additional considerations should be taken into account. This is not just related to health. Another similar situation where a genuine biometric sample is used fraudulently is a replay attack. In a replay attack, the biometric signal is usually genuine, but it was acquired/recorded in the past and presented again and should be considered as a fake attempt [93].

c) Is the individual temporarily affected by drug substances? Changes in handwriting due to alcohol were reported in [94, 95]. The effects of caffeine on handwriting were detected in [96]. Similar experiments regarding the effects of marijuana and alcohol were performed in [97].

One of the main concerns of biometrics applied to security is privacy [8]. Technological advances allow to store, gather, and compare a wide range of information on people. Using identifiers such as name, address, passport, or social security number, institutions can search databases for individuals' information. This information can be related to salary, employment, sexual preferences, religion, consumption habits, medical history, etc. This information can be collected with the consent of the user, but in some cases, it could also be extracted from biometric samples without the knowledge of the user. Thus, the user could be completely unaware that some additional and private information can be extracted from his biometric samples [98]. Therefore, there is a potential risk.

Let us think, for instance, in sharing medical information. Obviously, in the case of an emergency, this sharing among hospitals would be beneficial. On the contrary, if this information is transferred to a personal insurance company or a prospective employer, the insurance or the job application can be denied. The situation is especially dramatic when biometric data collection is intended for security applications to grant access to a facility or classified information, but a third party tries to infer the health condition of the subject. For instance, in the case of eye biometrics [92], an expert can determine that a patient has diabetes, arteriosclerosis, hypertension, etc.

For any biometric identifier, there is a portion of the population for which it is possible to extract relevant information

about their health, with similar implications to the ones described in the previous paragraph. This is not a specific problem of handwriting signals. Some other biometric signals exhibit the same potential problems, for example, speech disorders and hair or skin color problems. An important question is what is exactly disclosed when biometric scanning is used. In some cases, additional information not related to identification might be obtained. One possible scenario could be a company where an attendance system requires workers to sign each day. The main purpose of this task could be to check if the worker is at his workplace during the working days. However, once the handwriting is provided, the company could decide to analyze the signature to detect some pathologies or drug abuse and to dismiss those workers who do not show good health. And last but not least, once we provide our biometric samples, they can stay in a database for dozens of years and due to technological advances, they can be used in a simple way in the future to extract additional information that was not intended during acquisition. For this reason, we should think about technical solutions to preserve privacy and legal regulations to avoid such foreseeable issues.

Sometimes the situation is just the opposite. With the growth of interest in the fields of e-health and telemedicine, scientists started to develop automatic handwriting analysis systems that can be used for disease diagnosis [99], rating, or monitoring [82]. Basically, a database of healthy control samples from healthy individuals and pathological samples is acquired, disseminated and used for research purposes. Its registers are usually anonymized removing (destroying) any link to donor names and/or passports or national identity codes. However, this anonymization process could be useless if the acquired samples permit a biometric identification based on handwriting or drawings. This might not be feasible at present, but it might be possible in the near future with the improvement of the processing algorithms.

A related topic is de-identification for privacy protection in multimedia content. De-identification in multimedia content can be defined as the process of concealing the identities of individuals captured in a given set of data (images, video, audio, text), to protect their privacy. This will provide an effective means for supporting directives and laws related to personal data protection, e.g., the EU's General Data Protection Regulation (GDPR).

Future Trends

Security and health applications of handwriting analysis cannot be considered as separate fields anymore. While significant scientific developments exist in the field of biometric recognition using the handwritten signature for security [4, 18], few efforts have been made in general handwriting [20] and drawing [38] for security. Few efforts have also been deployed in health applications [3, 17, 47, 83, 99] as well as in possibilities of combining security and health.

As a summary of the research discussed in the present paper, on the one hand, the state of the art in applications based on online handwritten tasks can be considered:

a) Mature in security applications based on signature [4, 18]
b) Incipient in security applications based on the handwritten text [20, 36]
c) Incipient in security applications based on drawing tasks [37, 38]
d) Incipient in health applications based on handwriting text and drawing tasks [3, 47, 100–102]
e) Incipient in health applications based on signature [3, 18, 47, 99]

On the other hand, it is difficult to find published research in joint applications where security is studied in combination with one of the following health-related aspects:

f) Is the user to authenticate under stress?
g) Is he suffering any disease that makes him unable to understand the real implication on his acts?
h) Is he temporarily affected by drug or substance abuse?

Similarly, there is a lack of research in applications where health is the main goal and the following issue is addressed at the same time:

i) In order to keep the user's privacy [7], the handwritten signal is transformed [98] in order to remove his identity while preserving the diagnosis potential of the sample.

For the future, we see four main areas of research in online handwriting analysis for security and health, as shown in Table 2:

- Processing, analysis, and recognition of handwriting signals; with special emphasis in motor models based on neuroscience [103] and methods based on deep learning [101, 104] able to make the most of large-scale datasets [105].
- Support for early diagnosis [99] of pathologies using handwriting, especially neurodegenerative diseases [3, 17, 47, 83].
- Continuously monitoring the evolution of neurodegenerative diseases, rehabilitation, and healthy aging [56, 82]; using handwriting and other touch interaction signals [106].
- Removing undesired information from handwriting representations [98]: removal of health information for security applications and removing of identifying information in tasks acquired for health analysis purposes [7].

Table 2 Future developments in the area of handwriting analysis: research areas and specific problems

Research areas	Specific problems/Technologies
1. Fundamental research in: • Neuroscience-based models • Deep learning • Large-scale datasets	Writer identification in text-dependent and text-independent modes Recognition systems combining signatures + text Drawing, patterns, and touchscreen interaction for user identification
2. Supporting early diagnosis of pathologies	Novel health-based applications using text, drawings, and touchscreen interaction Signatures for diagnosis diseases
3. Continuous monitoring the evolution of diseases	Detection of stress Detection of drug substance intakes
4. Removing either health state or identity information	Anonymization of identity by keeping diagnostic properties Removing/obscuring undesired health information by keeping identification properties

Necessity of handwriting data for working on future areas

These four areas of future research can be further broken down as follows:

1. Development and scientific progress in biometric security applications based on handwritten text (capital letters, cursive letters, etc.) [20, 36], where the goal is not the classical optical character recognition (OCR). The goal is to identify the author of the text in two different modes: text dependent and text independent. Additional functionality is checking if the author of the text is forced to write a specific text or if he is free to write whatever he wants.
2. While signature-based recognition systems are quite mature, the complementary information of the combination between signature and text provided by the same author as well as the possibility of crossed recognition has not been deeply analyzed yet.
3. Development of new algorithms able to identify the author of a drawing in a similar way to what is done with signatures or handwriting. In the same way that a specific simple pattern can be used to unlock the smartphone [39], a specific drawing (invented or copied) could hold the same functionality [38]. Pattern unlocks consist of a grid of dots on a device's lock screen which users connect uniquely to gain access to the phone. However, the possibilities are much reduced when compared with handwritten drawings.
4. Development and scientific progress in biometric health applications based on handwritten text and drawings [47]. This is a promising research line to detect healthy aging, evaluate the effect of prescribed drugs on a specific disease (such as apomorphine on Parkinson's disease [107]), etc.
5. Analysis of the potential use of handwritten signatures for diagnosing diseases [47, 99]. Although the signature tends to be a mechanical movement with almost no cognitive effort to perform it, it has potential use in health applications.
6. Stress detection given handwritten tasks has potential implications on security applications, e.g., coercion detection [40].
7. Drug substance abuse can have legal implications for professional activities. It would be cheap and non-invasive to conduct preliminary tests based on handwriting tasks.
8. Development of algorithms to anonymize handwritten samples in order to hide the identity of the user while preserving the diagnostic capability of the samples [98].
9. Development of algorithms to anonymize handwritten samples in order to hide the health information of the user while preserving the identification capability of the samples [7].

In order to advance these research lines, adequate and realistic handwritten data is needed for experimentation. That data should necessarily involve several acquisition sessions, approved by an ethical committee, in order to cope with the temporal variability of the users as well as different tasks:

- Signature
- Cursive letters (free text and predefined text)
- Capital letters and digits (free text and predefined text)
- Drawings (simple strokes, Archimedes spiral, clock drawing tests, pentagon tests, house copying tests, etc.)

Fortunately, some databases are already available for research in several scenarios:

- Biometric security using signature [18, 48, 104, 105] and text [45] [36]
- Parkinson's disease and essential tremor [3, 47, 100, 107]
- Alzheimer's disease and mild cognitive impairment [57]
- Dysgraphia [108]

Conclusion

In this paper, we have pointed out future trends and challenges in biometric research on signature and handwriting. Special emphasis is given to the fact that, contrary to other biometric traits, handwriting signals are of interest in both e-security and e-health. Some challenges are identified that should attract the interest of the research community towards a more secure society.

We consider that this paper could help future researchers working in handwriting analysis to identify the main research topics to be addressed in the next years, as well as to attract new researchers from other fields.

Funding Information This study was funded by Spanish grants MINECO/FEDER TEC2016-77791-C4 and RTI2018-101248-B-I00, IDEA-FAST (H2020-JTI-IMI2-2018-15-two-stage-853981), Bio-Guard (Ayudas Fundacion BBVA 2017), and Cecabank. Réjean Plamondon has been supported by NSERC Grant RGPIN-2015-06409. Ruben Tolosana enjoys a postdoc position funded by Comunidad de Madrid (PEJD-2019-POST/TIC-16031).

Compliance with Ethical Standards

Conflict of Interest The authors declare that they have no conflict of interest.

Ethical Standards All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards. For this type of study formal consent is not required.

Research Involving Human and Animal Rights This chapter does not contain any studies with animals performed by any of the authors.

Informed Consent Informed consent was obtained from all individual participants included in the study.

References

1. Plamondon R, Shirari S. On-line and off-line handwriting recognition: a comprehensive survey. IEEE Trans Pattern Anal Mach Intell. 2000;22(1):63–84.
2. Li SZ and Jain AK (Eds.). Encyclopedia of Biometrics, 2nd Ed., Springer, 2015.
3. De Stefano C, Fontanella F, Impedovo D, Pirlo G, Scotto di Freca A. Handwriting analysis to support neurodegenerative diseases diagnosis: a review. Pattern Recogn Lett. 2019;121:37–45.
4. Martinez-Diaz M, Fierrez J and Hangai S. "Signature Matching", S.Z. Li and A.K. Jain (Eds.), Encyclopedia of Biometrics, 2nd Ed., Springer, 2015, pp. 1382–1387.
5. Plamondon R, Pirlo G, Anquetil É, Rémi C, Teulings HL, Nakagawa M. Personal digital bodyguards for e-security, e-learning and e-health: a prospective survey. Pattern Recogn. 2018;81:633–59.
6. Tolosana R, Vera-Rodriguez R, Fierrez J, Morales A, Ortega-Garcia J. Benchmarking desktop and mobile handwriting across COTS devices: the e-BioSign biometric database. *PLoS One*. 2017;12(5):e0176792.
7. Gomez-Barrero M, Galbally J, Morales A, Fierrez J. Privacy-preserving comparison of variable-length data with application to biometric template protection. IEEE Access. 2017;5:8606–19.
8. Faundez-Zanuy M. Privacy issues on biometric systems. IEEE Aerosp Electron Syst Mag. 2005;20(2):13–5.
9. Morales A, Morocho D, Fierrez J and Vera-Rodriguez R. "Signature authentication based on human intervention: performance and complementarity with automatic systems", IET Biometrics, 2017, pp. 1–9.
10. Marcos Faundez-Zanuy, Enric Sesa-Nogueras "preliminary experiments on automatic gender recognition base don online capital letters". in Recent Advances of Neural Networks Models and Applications. Proceedings of the 23rd Workshop of the Italian Neural Networks Society (SIREN), May 23-25, Vietri sul Mare, Salerno, Italy Bassis, Simone; Esposito, Anna; Morabito, Francesco Carlo (Eds.) 2014, XII, 443 Springer ISBN 978-3-319-04128-5
11. Book chapter "Privacy of Online Handwriting Biometrics Related to Biomedical Analysis" Marcos Faundez Zanuy, Jiri Mekyska. IET in User-Centric Privacy and Security in Biometrics. edited by Claus Vielhauer. November 2017 Book DOI: 10.1049/PBSE004E Chapter DOI: 10.1049/PBSE004E_ch2 e-ISBN: 9781785612084
12. Nappi M, Ricciardi S, Tistarelli M. Context awareness in biometric systems and methods: state of the art and future scenarios. Image Vis Comput. 2018;76:27–37.
13. Cognitive Computing Consortium: Cognitive Computing Defined. https://cutt.ly/qr8pyiu. Accessed 26 Feb 2020.
14. Reynolds H and Feldman S. "Cognitive computing: beyond the hype", KM World, 2014.
15. Marcelli A, Parziale A and Senatore R. "Some observations on handwriting from a motor learning perspective", in Proc. 2nd Workshop on Automated Forensic Handwriting Analysis, 2013, pp. 6–10.
16. Angelillo M T, Impedovo D, Pirlo G, L. Sarcinella L, Vessio G, ."Handwriting dynamics as an indicator of cognitive reserve: an exploratory study." 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC). IEEE, 2019.
17. Vessio G. Dynamic handwriting analysis for neurodegenerative disease assessment: a literary review. Appl Sci. 2019;9(21):46–66.
18. Diaz M, Ferrer MA, Impedovo D, Malik MI, Pirlo G, Plamondon R. A perspective analysis of handwritten signature technology. ACM Comput Surv. 2019;51(6):1–39.
19. Angelillo M T, Balducci F, Impedovo D, Pirlo G, Vessio G. Attentional pattern classification for automatic dementia detection. IEEE Access. 2019;7:57706–16.
20. Tolosana R, Vera-Rodriguez R and Fierrez J, "BioTouchPass: handwritten passwords for touchscreen biometrics", IEEE Transactions on Mobile Computing, 2020.
21. Drotár P, Mekyska J, Rektorová I, Masarová L, Smékal Z, Faundez-Zanuy M."A new modality for quantitative evaluation

of Parkinson's disease: in-air movement", in Proc. 13th International Conference on Bioinformatics and Bioengineering, 2013, pp. 1–4.
22. Impedovo D. Velocity-based signal features for the assessment of Parkinsonian handwriting. IEEE Signal Process Lett. 2019;26(4): 632–6.
23. Martinez-Diaz M, Fierrez J and Hangai S. "Signature Features", S.Z. Li and A.K. Jain (Eds.), Encyclopedia of Biometrics, 2nd Ed., Springer, 2015, pp. 1375–1382.
24. Plamondon R, Privitera CM. The segmentation of cursive handwriting: an approach based on off-line recovery of the motor-temporal information. IEEE Trans Image Process. 1999;8(1):80–91.
25. Crispo G, Diaz M, Marcelli A, Ferrer MA, "Tracking the ballistic trajectory in complex and long handwritten signatures", in Proc. 16th International Conference on Frontiers in Handwriting Recognition, 2018, pp. 351–356.
26. Lorette G, Plamondon R. Automatic signature verification and writer identification: the state of the art. Pattern Recogn. 1989;22(2):107–31.
27. Houmani N, Mayoue A, Garcia-Salicetti S, Dorizzi B, Khalil MI, Moustafa MN, Abbas H, Muramatsu D, Yanikoglu D, Kholmatov A, Martinez-Diaz M, .Fierrez J, Ortega-Garcia J, Roure Alcobé J, Fabregas J, Faundez-Zanuy M, Pascual-Gaspar J M, Cardeñoso-Payo V, Vivaracho-Pascual C. BioSecure signature evaluation campaign (BSEC'2009): evaluating online signature algorithms depending on the quality of signatures. Pattern Recogn. 2012;45: 993–1003.
28. Yeung DY, Chang H, Xiong Y, George S, Kashi R, Matsumoto T, Rigoll G. "SVC2004: First International Signature Verification Competition", in Proc. International Conference on Biometric Authentication, 2004, pp. 16–22.
29. Malik MI et al. "ICDAR2015 competition on signature verification and writer identification for on- and off-line skilled forgeries (SigWIcomp2015)", in Proc. IEEE International Conference on Document Analysis and Recognition, 2015.
30. Zhang B and Srihari S. "Analysis of handwriting individuality using word features", in Proc. 7th International Conference on Document Analysis and Recognition, 2003, pp.1142–1146.
31. Hook C, Kempf J and Scharfenberg G. "A novel digitizing pen for the analysis of pen pressure and inclination in handwriting biometrics", in Proc. Biometric Authentication Workshop, 2004, Lecture Notes in Computer Science, vol. 3087, pp. 283–294.
32. Srihari S, Sung-Hyuk C, Sangjik L. "Establishing handwriting individuality using pattern recognition techniques", in Proc. 6th International Conference on Document Analysis and Recognition, 2001, pp. 1195–1204.
33. Chapran J. Biometric writer identification: feature analysis and classification. Int J Pattern Recognit Artif Intell. 2006;20:483–503.
34. Sesa-Nogueras E, Faundez-Zanuy M. Biometric recognition using online uppercase handwritten text. Pattern Recogn. 2012;45:128–44.
35. Parizeau M and Plamondon R. "What types of scripts can be used for personal identity verification?", Plamondon R, Suen CY, Simner M. Computer Recognition and Human Production of Handwriting, 1989, pp. 77–90.
36. Tolosana R, Vera-Rodriguez R, Fierrez J, Ortega-Garcia J. BioTouchPass2: touchscreen password biometrics using time-aligned recurrent neural networks. IEEE Transact Inform Forensics Sec. 2020;15:2616–28.
37. Martinez-Diaz M, Fierrez J, Galbally J. The DooDB graphical password database: data analysis and benchmark results. IEEE Access. 2013;1:596–605.
38. Martinez-Diaz M, Fierrez J, Galbally J. Graphical password-based user authentication with free-form doodles. IEEE Transac Human-Mach Syst. 2016;46(4):607–14.
39. De Luca A, Hang A, Brudy F, Lindner C, Hussmann H, "Touch me once and I know it's you!: implicit authentication based on touch screen pattern", in Proc. of the SIGCHI Conference on Human Factors in Computing Systems, 2012. pp. 987–996.
40. Tolosana R, Vera-Rodriguez R, Fierrez J, Ortega-Garcia J "Presentation attacks in signature biometrics: types and introduction to attack detection", Marcel S, et al. (Eds.), Handbook of Biometric Anti-Spoofing (2nd Edition), Springer, 2019.
41. Ferrer MA , Morales A, Vargas J F, Lemos I Quintero M. "Is it possible to automatically identify who has forged my signature? Approaching to the identification of a static signature forger", in Proc, 10th IAPR International Workshop on Document Analysis Systems, 2012, pp. 175–179.
42. Mohammed L, Found B, Caligiuri M Rogers D. "The dynamic character of disguise behavior for text-based, mixed, and stylized signatures", J Forensic Sci, 2010, pp. 136–141.
43. Liwicki M, Heuvel C E v d, Found B, Malik M I. "Forensic signature verification competition 4NSigComp2010 - detection of simulated and disguised signatures", in Proc. 12th International Conference on Frontiers in Handwriting Recognition, 2010, pp. 715–720.
44. Sesa-Nogueras E, Faundez-Zanuy M, Mekyska J. An information analysis of in-air and on-surface trajectories in online handwriting. Cogn Comput. 2012;4(2):195–205.
45. Fierrez-Aguilar J, Galbally J, Ortega-Garcia J, Freire M R, Alonso-Fernandez F, Ramos D, Toledano D T, Gonzalez-Rodriguez J, Siguenza J A, Garrido-Salas J, Anguiano E, Gonzalez-de-Rivera G, Ribalda R, Faundez-Zanuy M, Ortega J A, Cardeñoso-Payo V, Viloria A, Vivaracho C E, Moro Q I, Igarza J J, Sanchez J, Hernaez I, Orrite-Uruñuela C, Martinez-Contreras F, Gracia-Roche J J. BiosecurID: a multimodal biometric database. Pattern Anal Applic. 2010;13(2):235–46.
46. Drotar P, Mekyska J, Rektorová I, Masarová L, Smékal Z, Faundez-Zanuy M. Analysis of in-air movement in handwriting: a novel marker for Parkinson's disease. Comput Methods Prog Biomed. 2014;117(3):405–11.
47. Castrillon R, Acien A, Orozco-Arroyave J R, Morales A, Vargas F J, Vera-Rodrıguez R, Fierrez J, Ortega-Garcia J, Villegas A. "Characterization of the handwriting skills as a biomarker for Parkinson disease", in Proc. IEEE Intl. Conf. on Automatic Face and Gesture Recognition, 2019.
48. Ortega-Garcia J, Fierrez-Aguilar J, Simon D, Gonzalez J, Faundez-Zanuy M, Espinosa V, et al. "MCYT baseline corpus: a bimodal biometric database", in *Proc.* IEEE Conf Vision Image Signal Proc. 2003;150(6):395–401.
49. Rosenblum S, Simhon HAB, Gal E. Unique handwriting performance characteristics of children with high-functioning autism Spectrum disorder. Res Autism Spectr Disord. 2016;23:235–44.
50. Mekyska J, Faundez-Zanuy M, Mzourek Z, Galaz Z, Smekal Z, Rosenblum S. Identification and rating of developmental dysgraphia by handwriting analysis. IEEE Transact Human-Mach Syst. 2017;47(2):235–48.
51. Rosenblum S, Dvorkin AY, Weiss PL. Automatic segmentation as a tool for examining the handwriting process of children with dysgraphic and proficient handwriting. Hum Mov Sci. 2006;25(45):608–21.
52. Rosenblum S, Parush S, Weiss PL. Computerized temporal handwriting characteristics of proficient and non-proficient Handwriters. Am J Occup Ther. 2003;57(2):129–38.
53. Plamondon R, O'Reilly C, Galbally J, Almaksour A, Anquetil É. Recent developments in the study of rapid human movements with the kinematic theory: applications to handwriting and signature synthesis. Pattern Recogn Lett. 2014;35(1):225–35.

54. Plamondon R. A kinematic theory of rapid human movements. Part II: movement time and control. Biol Cybern. 1995;72(2): 309–20.
55. Plamondon R. A kinematic theory of rapid human movements. Part III: kinetic outcomes. Biol Cybern. 1998;78(2):133–45.
56. Plamondon R. A kinematic theory of rapid human movements. Part IV: a formal mathematical proof and new insights. Biol Cybern. 2003;89(2):126–38.
57. Plamondon R, Alimi A. Speed/accuracy tradeoffs in target-directed movements. Behav Brain Sci. 1997;20:279–349.
58. Woch A, Plamondon R, O'Reilly C. Kinematic characteristics of bidirectional delta-lognormal primitives in young and older subjects. Hum Mov Sci. 2011;30(1):1–17.
59. Carmona-Duarte C, Ferrer MA, Parziale A, Marcelli A. Temporal evolution in synthetic handwriting. Pattern Recogn. 2017;68:233–44.
60. Fischer A, Plamondon R. Signature verification based on the kinematic theory of rapid human movements. IEEE Transac Human-Mach Syst. 2017;47(2):169–80.
61. Ferrer MA, Diaz M, Carmona-Duarte C, Morales A. A behavioral handwriting model for static and dynamic signature synthesis. IEEE Trans Pattern Anal Mach Intell. 2017;39(6):1041–53.
62. Bhattacharya U, Plamondon R, Dutta Chowdhury S, Goyal P, Parui SK. A sigma-lognormal model-based approach to generating large synthetic online handwriting sample databases. Int J Doc Anal Recognit. 2017;20(3):155–71.
63. Djeziri S, Guerfali W, Plamondon R, Robert JM. Learning handwriting with pen-based systems: computational issues. Pattern Recogn. 2002;35(5):1049–57.
64. Diaz M, Fischer A, Plamondon R, Ferrer M A. "Towards an automatic on-line signature verifier using only one reference per signer", in Proc. 13th International Conference on Document Analysis and Recognition, 2015, pp. 631–635.
65. Almaksour A, Anquetil E, Plamondon R, O'Reilly C. "Synthetic handwritten gesture generation using sigma-lognormal model for evolving handwriting classifier", in Proc. 15th International Graphonomics Society Conference, 2011, pp. 98–101.
66. Impedovo D, Pirlo G, Mangini F M, Barbuzzi D, Rollo A, Balestrucci A, Impedovo S, Sarcinella L, O'Reilly C, Plamondon R "Writing generation model for health care neuromuscular system investigation", in Proc. 10th International Meeting on Computational Intelligence Methods for Bioinformatics and Biostatistics, 2013, pp. 1–16.
67. Gomez-Barrero M, Galbally J, Fierrez J, Ortega-Garcia J, Plamondon R, "Enhanced on-line signature verification based on skilled forgery detection using sigma-lognormal features", in Proc. International Conference on Biometrics, 2015, pp. 501–506.
68. Ramaih C, Plamondon R and Govindaraju V. "Handwritten CAPTCHA generation based on the sigma-lognormal model," in Proc. 16th International Graphonomics Society Conference, 2013, pp. 105–108.
69. O'Reilly C and Plamondon R. "Design of a neuromuscular disorders diagnostic system using human movement analysis", in Proc. 11th International Conference on Information Science, Signal Processing and their Applications, 2012, pp. 787–792.
70. Reznakova M, Tencer L, Plamondon R, Cheriet M. "The generation of synthetic handwritten data for improving on-line learning", in Proc. 17th International Graphonomics Society Conference, 2015, pp. 55–58.
71. Berio D, Leymarie FF and Plamondon R. "Computer aided design of handwriting trajectories with the kinematic theory of rapid human movements", in Proc. 18th international Graphonomics society conference, 2017.
72. Van Gemmert A, Plamondon R and O'Reilly C. "Using the sigma-lognormal model to investigate handwriting of individuals with Parkinson's disease", in Proc. 16th International Graphonomics Society Conference, 2013, pp. 119–122.
73. Martín-Albo D, Leiva LA, Huang J, Plamondon R. Strokes of insight: user intent detection and kinematic compression of mouse cursor trails. Inf Process Manag. 2016;52(6):989–1003.
74. Lebel K, Nguyen H, Duval C, Plamondonand R, Boissy P. Capturing the cranio-caudal signature of a turn with inertial measurement systems: methods, parameters robustness and reliability. Front Bioengin Biotechnol. 2017.
75. Pan Z, Talwar S, Plamondon R, van Gemmert AWA. Characteristics of bi-directional Unimanual and bimanual drawing movements: the application of the delta-lognormal models and sigma- lognormal model. Pattern Recogn Lett. 2019;121: 97–103.
76. Laniel P, Faci N, Plamondon R, Beauchamp MH, Gauthier B. "Kinematic analysis of fast pen strokes in children with ADHD", Applied Neuropsychology: Child, 2019, pp. 1-16.
77. Leiva LA, Martin-Albo D, Plamondon R. The kinematic theory produces human-like stroke gestures. Interact Comput. 2017;29(4):1552–65.
78. O'Reilly C, Plamondon R. Development of a sigma-lognormal representation for on-line signatures. Pattern Recogn. 2009;42(12):3324–37.
79. Ferrer MA, Diaz M, Carmona-Duarte C, Plamondon R. iDeLog: iterative dual spatial and kinematic extraction of sigma-lognormal parameters. IEEE Trans Pattern Anal Mach Intell. 2018;42(1): 114–25.
80. Martín-Albo D, Plamondon R and Vidal E. "Improving sigma-lognormal parameter extraction", in Proc. 13th international conference on document analysis and recognition, 2015.
81. Plamondon R, O'Reilly C,Rémi C, Duval T. "The lognormal handwriter: learning, performing and declining", Frontiers in Psychology: Cognitive Science. Special Issue in Cognitive Science, Writing Words: From Brain to Hand, 2013, p. 1–14.
82. Plamondon R, Marcelli A, Ferrer MA. (Eds), The Lognormality Principle and its Applications in e-security, e-learning and e-health. World Scinetific, 2020.
83. Impedovo D, Pirlo G. Online handwriting analysis for the assessment of Alzheimer's disease and Parkinson's disease: overview and experimental investigation. Front Pattern Recogn Artif Intell. 2019;5:113.
84. Tome P, Fierrez J, Vera-Rodriguez R, Nixon MS. Soft biometrics and their application in person recognition at a distance. IEEE Transac Inform Forensics Sec. 2014;9(3):464–75.
85. Vielhauer C, . Basu K, Dittmann J, Dutta P K. "Finding meta data in speech and handwriting biometrics", in Proc. of SPIE, 2005, vol. 5681, p. 504–515.
86. Scheidat T, Wolf F, Vielhauer C. "Analyzing handwriting biometrics in metadata context", in Proc. of the SPIE, 2006.
87. Liwicki M, Schlapbach A, Loretan P, Bunke H. "Automatic detection of gender and handedness from on-line handwriting", in Proc. 13th International Graphonomics Society Conference, 2007, pp. 179–183.
88. Liwicki M, Schlapbach A, Bunke H. Automatic gender detection using on-line and off-line information. Pattern Anal Applic. 2011;14:87–92.
89. Likforman-Sulem L, Esposito A, Faundez-Zanuy M, Clemencon S, Cordasco G. EMOTHAW: a novel database for emotional state recognition from handwriting and drawing. IEEE Transac Human-Mach Syst. 2017;47(2):273–84.
90. Alonso-Fernandez F, Fierrez J, Ortega-Garcia J. Quality measures in biometric systems. IEEE Secur Priv. 2012;10(9):52–62.
91. Martin C, Oh E, Addy K, Eskildsen K. Biometric verification and duress detection system and method. Patent US. 2007;20070198850:A1.

92. Alonso-Fernandez F et al. “Cross-sensor and cross-spectral periocular biometrics: a comparative benchmark including smartphone authentication”, arXiv preprint arXiv:1902.08123, 2020.
93. Marcel S, Nixon MS, Li S Z. “Handbook of biometric anti-spoofing”, 2nd Ed., Springer, 2019.
94. Faruk A, Turan N. Handwritten changes under the effect of alcohol. Forensic Sci Int. 2003;132(3):201–10.
95. Phillips JG, Ogeil RP, Muller F. Alcohol consumption and handwriting: a kinematic analysis. Hum Mov Sci. 2009;28:619–32.
96. Tucha O, Walitza S, Mecklinger L, Stasik D, Sontag TA, Lange KW. The effect of caffeine on handwriting movements in skilled writers. Hum Mov Sci. 2006;25:523–35.
97. Foley RG, Miller L. The effects of marijuana and alcohol usage on handwriting. Forensic Sci Int. 1979;14(3):159–64.
98. Morales A, Fierrez J and Vera-Rodriguez R. “SensitiveNets: learning agnostic representations with application to face recognition”, arXiv preprint arXiv:1902.00334, 2019.
99. Pirlo G, Diaz M, Ferrer MA, Impedovo D, Occhionero F, Zurlo U. “Early diagnosis of neurodegenerative diseases by handwritten signature analysis”, in Lecture Notes in Computer Science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), 2015.
100. Pereira CR, Weber S A T, Hook C, Rosa GH, Papa J P. “Deep learning-aided Parkinson’s disease diagnosis from handwritten dynamics”, in Proc. 29th Conference on Graphics, Patterns and Images, 2016. p. 340–346.
101. Moetesum M, Siddiqi I, Ehsan, S. et al. “Deformation modeling and classification using deep convolutional neural networks for computerized analysis of neuropsychological drawings.” Neural Comput & Applic, 2020; 1–25.
102. Moetesum M, Siddiqi I, and Vincent N. "Deformation classification of drawings for assessment of visual-motor perceptual maturity." Int. Conf. on Document Analysis and Recognition *(ICDAR)*. IEEE, 2019.
103. Merel J, Botvinick M, Wayne G. Hierarchical motor control in mammals and machines. Nat Commun. 2019;10:54–89.
104. Tolosana R, Vera-Rodriguez R, Fierrez J, Ortega-Garcia J. Exploring recurrent neural networks for on-line handwritten signature biometric. IEEE Access. 2018;6:5128–38.
105. Tolosana R, Vera-Rodriguez R, Fierrez J, Ortega-Garcia J. “DeepSign: Deep On-Line Signature Verification”, arXiv preprint arXiv:2002.10119, 2020.
106. Fierrez J, Pozo A, Martinez-Diaz M, Galbally J, Morales A. Benchmarking touchscreen biometrics for mobile authentication. IEEE Transac Inform Forensics Secur. 2018;13(11):2720–33.
107. Angelillo MT, Impedovo D, Pirlo G, Vessio G. “Performance-driven handwriting task selection for Parkinson’s disease classification.” Int. Conf. of the Italian Association for Artificial Intelligence, 2019, Springer, Cham.
108. Garré-Olmo J, Faundez-Zanuy M, Lopez-de-Ipiña K. Kinematic and pressure features of handwriting and drawing: preliminary results between patients with mild cognitive impairment, Alzheimer disease and healthy controls. Curr Alzheimer Res. 2017;14(9):960–8.
109. Jain AK, Nandakumar K, Ross A. 50 years of biometric research: accomplishments, challenges, and opportunities. Pattern Recogn Lett. 2016;79:80–105.