IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 24, 2016, accepted November 11, 2016, date of publication December 29, 2016, date of current version March 2, 2017.

Digital Object Identifier 10.1109/ACCESS.2016.2646398

Study of Imposter Attacks on Novel Fingerprint Dynamics Based Verification System

ISHAN BHARDWAJ[1], (Member, IEEE), NARENDRA D. LONDHE[1], (Senior Member, IEEE), AND SUNIL K. KOPPARAPU[2], (Senior Member, IEEE)

[1]National Institute of Technology Raipur, Raipur 492010, India
[2]Department of Speech and natural language processing, Tata Consultancy Services Ltd., Mumbai 400601, India

Corresponding author: N. D. Londhe (nlondhe.ele@nitrr.ac.in)

ABSTRACT The rapid momentum in the realization of security solutions, availability of affordable hardware components, and computing devices has led to a tremendous rise in biometric research. However, the threat of spoofing has raised palpable security concerns. In this paper, we examined a recently introduced novel behavioral biometrics technique, namely, fingerprint dynamics. The technique exploits individual's behavioral characteristics observed from multi-instance finger scan events. The objective of this investigation was to study the spoof resistance capabilities of the fingerprint dynamics-based standalone identity verification system. We used a custom-built hardware unit to collect biometric samples from a total of 50 participants, in an environment that closely mimics the operational scenario. Data collection was done in several sessions per user, spread over a period of seven weeks. We performed an exhaustive analysis of several time-derived features, and selected a combination of best-performing features using genetic algorithm. We also conducted a systematic evaluation using support vector machine and k-nearest neighbor classifiers. We performed a series of verification experiments under three different and practically relevant attack scenarios, namely: 1) combined zero-effort and active imposter; 2) only zero-effort imposter; and 3) only active imposter. We find that the proposed technique exhibits promising results under all the three attack scenarios.

INDEX TERMS Authentication, biometrics, fingerprint dynamics, fingerprint recognition, security.

I. INTRODUCTION

Increasing penetration of computers and online systems, in all walks of our lives, demands a very high degree of security and privacy measures. The applications that use computers and online systems are diverse, ranging from information retrieval, banking, access control, law enforcement, and forensics to name a few. A prominent tool to securitize the majority of these areas is user verification or authentication. Until recently password and token-based techniques were among the few successful practically used means of user authentication. However, their inability to meet the desired user level of security and user expediency aspects led to the development and use of alternative means of authentication [1]. An eminent choice to password-based authentication system is biometrics [2]. Biometric based systems verify and distinguish people based on their physiological or behavioral characteristics, or both [3].

A. BIOMETRICS

Biometric modalities can be primarily categorized into two groups, namely, physiological and behavioral biometrics. Physiological biometrics have gained a reputation and are seen in a large number of implemented user verification systems [3]. However, there are also several studies (example [4], [5]) emphasizing the role of behavioral biometrics that can aid in verifying a user identity conveniently. Behavioral biometrics can be implemented in situations where physiological biometric data cannot be acquired (for example recognizing a person from a distance using gait, or while using a computer system using keystroke dynamics). Behavioral biometrics operates on the fact that individuals develop very distinctive characteristics as they go about doing their day to day work. The distinctive characteristics are generally associated with human actions, skills, knowledge gained, and habits that can be utilized to uniquely identify or verify an individual [6]. Moreover, some of the behavioral characteristics can be easily employed for continuous person authentication [7] while the user is performing certain action or task [8], [9], additionally this is non-obtrusive. For this reason, the behavioral biometrics can also aid in preventing intrusion attempts persuasively.

Various factors like health, mood, and environment can affect the intra-class variation in behavioral biometrics [8]. In many studies, discussed in [2], it has been claimed that

interclass variations in behavioral biometric characteristics can be comparatively lower than state-of-the-art physiological biometric traits. Hence, solely relying on behavioral biometrics is apparently unsuitable for large-scale identification. However, the techniques based on behavioral biometrics are well suited for identity verification task, and are usually capable of achieving acceptable accuracies [5]. Furthermore, systems based on behavioral traits can be designed to learn and adapt over a period of time [10], for example by updating the user models for each successful verification attempt. This may turn out to be a great merit to overcome the challenges like age, varying human behavior etc., and can result in a continuously updating system with high user acceptability [11]. Multi-biometrics can also be seen as a solution to such problems, and can handle the causatum pretty well [12]. In these systems, information pertaining to a behavioral trait can be used in conjunction with the physiological trait, to improve the performance as well as security aspects of the overall user verification system. The non-obtrusive property of behavioral biometrics is an added advantage, which doesn't impose any extra burden on the user, making it a preferred choice for multi-biometric systems. As most of the behavioral biometrics systems do not need specialized hardware, most of the desired characteristics can be captured using existing components [13]. The additional equipment, if required to acquire additional data, are usually cost effective, making techniques based on behavioral biometrics a reasonable choice [5], [14], [15].

Moreover, like conventional authentication system most of the biometric based systems, whether physical, behavioral or the multibiometric, are susceptible to attacks [12]. These attacks broadly falls in two categories: direct (or presentation) attacks, and indirect attacks [6]. Researchers [14], [16] suggest that despite various counter measures these issue are still prevalent and new techniques are required to deal with the associated threats. Thus an authentication system that is capable to provide high performance and spoof resistance, along with non-obtrusiveness and cost effectiveness, is highly desirable.

B. CONTRIBUTION OF THE WORK

In this paper, we present an experimental study to assess the discriminability of the fingerprint dynamics under various realistic spoof attack scenarios; and along the way identify and articulate some associated challenges. We explore the possibility of developing a spoof resistant authentication system based on this novel behavioral characteristic. We believe this study have substantial potential to serve as a strong base for further exploration by the research community. The study commences with a preface to behavioral characteristics associated with fingerprint scanning action, followed by the feature extraction and analysis, experiments with different classification paradigm, and validation of the postulate. To the best of our knowledge, there is no such study previously reported in the literature.

In order to evaluate the postulate, the prime requirement is the need to have a suitable dataset. As there is no publicly available database, we devised a hardware unit to acquire user samples and constructed an appropriate database. This dataset is yet another principal contribution of our work. Collecting user behavior data is challenging from practical and legal perspective [17], in spite of this, we acquired samples from 50 subjects.

The rest of this paper is organized as follows: Section II gives an overview of the related literature and the proposed technique. Section III describes the experimental scenarios including the data collection and feature extraction procedure. Section IV reports the empirical results and discussion. Section V presents our concluding remarks on the study.

II. BACKGROUND

The proposed technique is closely related to two well-established biometric techniques, namely, (a) fingerprint and (b) keystroke dynamics. Liveness detection is another field that shares some attributes with the proposed technique in this paper. Being relatively new, our proposed technique can be confused with many other existing techniques in the literature. To avoid this comparison and confusion, we outline such techniques to bring out the freshness of the fingerprint dynamics. A brief review of fingerprint dynamics and the work closely related to it, is given in the following subsections.

A. FINGERPRINT

User recognition systems based on fingerprints are one of the most deployed biometric systems till date [1], [2]. Suitability, both for verification as well as identification task, high recognition accuracy, permanence, and wide acceptability are a few merits among several others that contribute to its popularity. A practical problem, which can substantially affect the performance of a fingerprint-based authentication system, is the acquisition of low-quality fingerprints [18]. The poor quality of fingerprints can be due to the partial or insignificant area acquisition, undesirable finger roll, noise or smudge on the sensor, non-ideal skin conditions etc. [3]. Spoofing is another threat that raises palpable security concerns [1], [19], [20]. Similar to other biometric systems the fingerprint-based system can be circumvented by a skillful imposter [21], [6]. Moreover, when the fingerprint of a user is compromised, the immutability property of fingerprint biometrics may give birth to another noteworthy threat, namely, permanent loss of one's fingerprint biometric data [3], [6], [19]. The multi-biometric systems are seen as a prominent solution to alleviate most of these limitations and to improve the system performance. However, as discussed in Section I, such systems demand separate hardware and data acquisition from the user, making it an expensive and intrusive alternative to the unimodal systems. Thus in this paper, we have limited our study to assess the fingerprint dynamics as a standalone system; however, the proposed technique can be integrated with multi-instance fingerprint recognition systems to

formulate a robust multi-biometric system [21]. Then the technique can work non-obtrusively while minimizing most of the deficits associated with typical biometric and multi-biometric systems. The proposed technique, in such scenario, can be seen as an assistive biometric technique to improve the spoof resistance and performance of the fingerprint-based authentication system rather than an alternative to it.

B. LIVENESS DETECTION

Recently in the field of biometrics, besides other anti-spoofing approaches such as the use of multibiometric or challenge-response methods, liveness detection has gained a reputation. It has emerged as a prominent solution to counter the spoof attacks on various biometric systems [6], including the fingerprints based systems as well [22]. In the domain of the fingerprint based authentication, it can be defined as a process that aids in determining whether the fingerprint sample presented to the sensor, is a live person's sample or a spoof artifact [20]–[23].

The liveness detection techniques can be broadly categorized into two classes, namely hardware based and software based. The solutions falling into the domain of software, implement various pre-processing techniques to improve the discrimination capability of the existing algorithm or employ advanced classification techniques [24]. The software-based techniques are in general less expensive (as no extra device is needed), and less intrusive (as their implementation is transparent to the user) [25]. The liveness detection techniques based on the hardware typically utilize some fortified hardware or sensor units in order to detect certain characteristics of a living trait. These techniques are generally expensive to deploy and may impose certain constraints on the biometric acquisition.

Many techniques that can effectively detect the liveness cannot be considered for practical application in the field biometrics, if they do not fulfil certain challenging requirements [16], [26]: (i) non-invasiveness, the technique should comply with the norms of human safety and in no case be harmful to the individual; (ii) user friendly, easy to use; (iii) fast processing, it should not take unacceptably long duration of time to provide the outcome; (iv) low cost, the cost of implementation should not be extraordinarily high or should not surpass the cost of loss when the technique is not implemented; (v) high performance, the system should be able to accurately predict the spoof attempts and live samples. The inclusion of such technique also required to not result in degraded recognition performance of the biometric system. In literature, some of the liveness detection methods are observed to have a few other limitations as well [1], [21]. Such as the ability to detect only certain material based spoof samples, limited performance in presence of high-quality spoof samples, etc. [22]. Despite being not so expensive by itself, some of the liveness detection techniques may require upgrading or completely removing the already deployed hardware, that contribute to increased cost of the authentication systems. Furthermore, in literature, the liveness detection is generally used for detecting spoof finger impressions only [1] and not for improving the recognition accuracies. Thus we can say that a more cost effective, user-friendly and performance centric solution is required that can overcome the majority of limitations of the existing liveness detection methods.

C. KEYSTROKE DYNAMICS

The fingerprint dynamics technique [27] is inspired by the keystroke dynamics system [28], a popular behavioral characteristic based on the fact that different humans tend to strike the keys differently (in terms of key presses, the time differences between two keypresses etc.) on the computer keyboard during their interaction with the computers. Several studies, such as by National Institute of Standard and Technology (NIST) and National Science Foundation (NSF), assert the competence of keystroke patterns with respect to many prominent physiological biometric traits [29]. Ample work done in the field of keystroke dynamics corroborates this statement [30]. The performance of the keystroke dynamics based systems can be substantially influenced by three factors, namely, string length, clock resolution, and training data. The significance of typing string length has been advocated by many researchers (example see [31], [32]) who report a radical increase in misclassification rates when the length of the keystroke string drops below 10 characters. Clock resolution can also affect the system performance significantly. Higher resolutions are able to capture details of the time difference between two consecutive keystrokes more accurately, making the overall system performance better. Greater amount of training data generally leads to better performance of a classification system; however, required size of the training dataset is also closely coupled with the population size and classification methodology [30] used. It is but natural to keep these aspects in mind when dealing with similar behavioral biometric technologies.

D. FINGERPRINT DYNAMICS

There are numerous characteristics associated with human behavior, which are utilized by different biometric techniques based on measures of pressure, time dynamics etc. [7]. Time dimension or more precisely the intra-time duration between two events when performing a task has proven to be quite successful in defining human characteristics [5], [27].

Acquiring fingerprint dynamics can be described as a process of time recording events, while the user goes about the task of scanning multiple fingers in a certain sequence against the fingerprint sensor. The dynamics refer to the various timing parameters that can be observed in the time dimension. Generally, in the multi-instance biometric scan, the dynamics display unique behavioral patterns of the users. Multiple instances facilitate significant improvement in the overall performance, by minimizing factors like intra-class variations etc. that usually affect the performance of conventional methodologies. It was perceived from our previous works [14], [21] that an individual's fingerprint dynamics

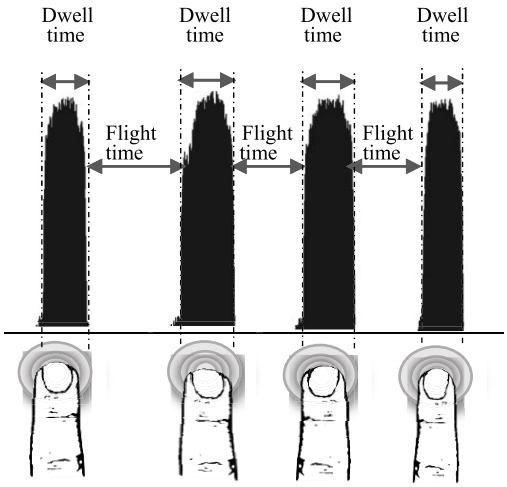

FIGURE 1. Time stamps acquisition from multi-instance finger scan events.

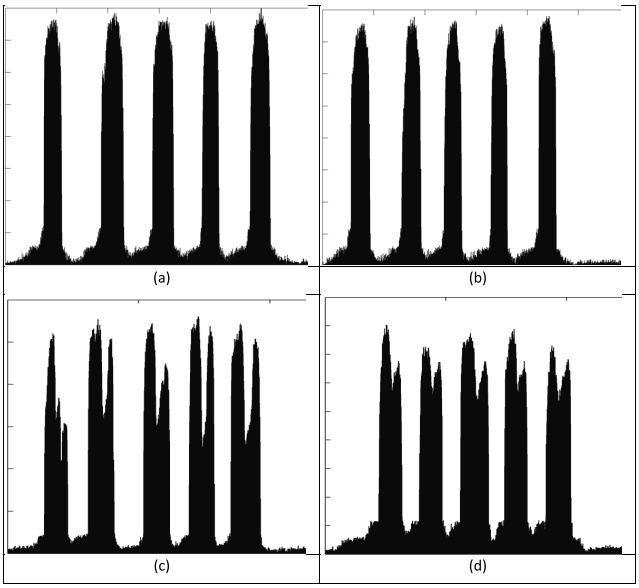

FIGURE 2. Sample recorded time events of user one 2(a) and 2(b), second user 2(c) and third user 2(d).

does evolve over time yet they tend to be consistent enough to distinguish an individual. Fig. 1 depicts an exemplary multi-instance finger swipe act against the sensor. The time user takes for swiping a finger is termed as the dwell time and the time between two consecutive swipe actions is referred to as the flight time. A detailed description of several time-derived parameters is given in Section III.

For acquisition of fingerprint dynamics, a user performs the scanning task in a certain fashion, including some or all of the fingers of his choice. This involves another important principle, termed as fingerprint sequencing [33], which levies a condition that the sequence of fingers of a user, should be the same for the enrolment and verification [34]. Hence, for the purpose of verification the user not only have to use the same fingers, as the choice made during enrolment, but also scan the fingers in the same sequence. Thus a different sequence of fingers represents a unique biometric pattern for the same person. It enables a user to choose a different sequence of fingers for different applications and also provide revocability. If the permissible length of the sequence is n then each user is left with n^{10} choices of finger sequence (assuming that the individual has ten fingers). Fingerprint sequencing thus contributes to a stronger system in the sense that an intruder is required to guess the correct sequence (1 of n^{10} possibilities) of fingers used. Furthermore, a choice can be given to the user to choose a length of the sequence of his choice, thus giving the user an extra degree of freedom. Fig. 2(a) and 2(b) depicts two swiping patterns of length five from the same user while Fig. 2(c) and 2(d) depicts two swiping sequences of the same length from two other individuals. Here the similitude between the patterns of the same user, and the difference among the patterns of all the three users can be visually observed. These figures indicate the possibility that exists for application of finger dynamics as an instrument to verify the identity of a human being in security sensitive authentication systems.

E. RELATED WORK

Recently the dynamics based systems have been paid attention by the researchers. For example in [35], the authors presented an approach for authentication that utilizes multi-touch gestures. They report a set of five-finger touch gestures, based on movement features of the center of the palm and fingertips. The study is based on multiple gestures and requires multi-touch surface. In addition to imposing conditions like the need for a large sized multi-touch surface, to accommodate gestures of all the five fingers simultaneously, the achieved results are marred by several limitations, such as, only five samples each for training and testing of a gesture from a person, all the user samples acquired in an unspecified, short period of time (perhaps at the same time), and more importantly, active imposter attacks were not considered. In [36], a similar study with computationally efficient method based on statistical touch dynamic images is proposed. More recently an extended study [37] that combines the keystroke and gestures based authentication for smartphones, has been introduced in the biometric literature. The scheme is solely based on thumb strokes (one finger), and facilitate post authentication user verification, in addition to the entry-point authentication. A number of similar studies have been presented in the literature based on analogous techniques. However, fingerprint dynamics proposed in this paper, differ from these analogues behavioral techniques in many aspects making it advantageous to use fingerprint dynamics. For example unlike touch screen gesture based systems the fingerprint dynamics based system does not require any special hardware, it just requires the multi-instance acquisition of distinct fingers with the existing fingerprint hardware. Moreover, the same swipe action is performed rather than having to deal with varied multiple gestures. Fingerprint

dynamic systems are not limited to use on devices with touch screen capabilities only (mainly mobile device) unlike gesture based techniques, additionally, the fingerprint dynamics based authentication can be implemented on any device with inbuilt or external fingerprint sensor. Furthermore, as discussed in section II (A) the fingerprint dynamics data can be acquired along with the fingerprint of the user. This is generally not possible with the gesture based system that relies only on the behavioral characteristics of the user or demand separate acquisition for other biometric characteristics [37], if used as a part of the multimodal biometric system.

Unlike keystroke dynamics based systems [32], where an input device consists of multiple keys and the actual location of the keys on the keyboard plays a significant role in determining the user identity, the fingerprint dynamics is acquired by a single sensor unit turning the location factor dysfunctional. This aspect also contributes in eliminating two deficits of keystroke based systems, namely (a) ubiquitous keyboards of different layout and size which can greatly affect the system performance [32] and (b) the problem of possible negative time, due to the pressing of next key before release of the previous one [29], [38].

Furthermore, most of the conventional authentication systems do not comply with the fundamental requirements, namely, the ease to remember but hard to guess [35], [39], flexibility to change, and distinctiveness of input pattern for different accounts of the same user etc. [40]. Most of these aspects are generally not possible with either password or biometrics-based authentication system alone. One of the objective behind introducing the fingerprint dynamics technique was to facilitate these important practical aspects, combining the merits of password and biometrics into a single authentication system, while alleviating most of the limitations associated with either of them. The rapidly increasing application of online transactions and the ubiquitous portable devices, i.e. smartphones and laptops, with inbuilt biometric sensors and high computation power becoming pervasive, makes it feasible to implement the proposed technique for the masses. A detailed comparative evaluation of the fingerprint dynamics with other analogues techniques can also be found in our previous work [14]. Our aim, in what we thus believe to be a novel technique, is to demonstrate its capability as a standalone system to verify the identity of individuals in presence of imposter attempts (zero-effort, active imposters and both) [6].

III. METHODOLOGY

In this section, a brief overview of user authentication system based on fingerprint dynamics is given followed by the description of data collection, and feature extraction processes.

A. SYSTEM OVERVIEW

Like typical authentication systems, the proposed system works in two prime phases, namely, enrolment and verification (Fig. 3). Enrolment stage includes the user registration,

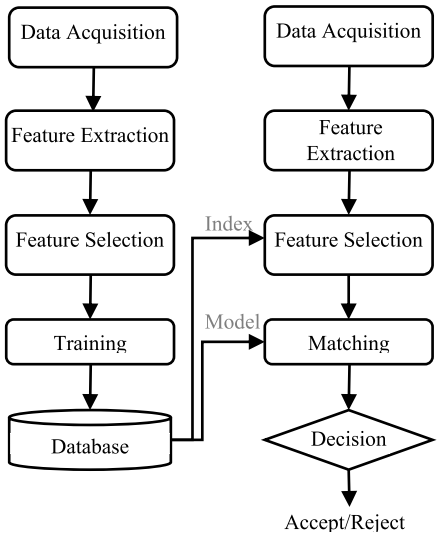

FIGURE 3. Generic Layout of the system indicating the enrolment and verification process.

where users provide credentials and other supplementary information along with the biometric data, in the form of multi-instance finger swipe action. The system records the various associated time stamps and may ask the user to provide the data several times. It is important to note that the system utilizes the same sensor and the same feature extraction module, but works on the fused information from multiple instances within the same biometric modality. A feature extraction unit is applied to extract useful information, representing user characteristics in a more appropriate from for classification. A feature selection module is used to automatically select a subset of the most discriminating features. Following this, the training is performed in order to obtain user template/model, which are subsequently stored in the database. For authentication, a similar process is repeated with exactly same parameters extracted as in the training phase. The user provides some preliminary information, in addition to the biometric data, to verify his identity. The user's stored template/model is retrieved and matched against the recently entered multi-instance biometric data. If the matching score falls above the threshold (τ) then the system will acknowledge the user as verified. A detailed description of these steps is given in the following subsections.

B. DATA COLLECTION

For the acquisition of user data (fingerprint dynamics), we devised an experimental setup by placing a capacitive sensor over the dummy fingerprint sensor unit. This is achieved by burning the program logic and adding the components to a microcontroller board (based on ATmega328P), which is further connected to a computer system via the serial bus interface. We used Matlab®2015 to design the acquisition module and user interface to acquire the signals transmitted through the microcontroller board [41]. The layout of data acquisition system is depicted in Fig. 4. A preliminary set of experiments, [14] demonstrates that once users are familiar, most of them take less than nine thousand milliseconds to

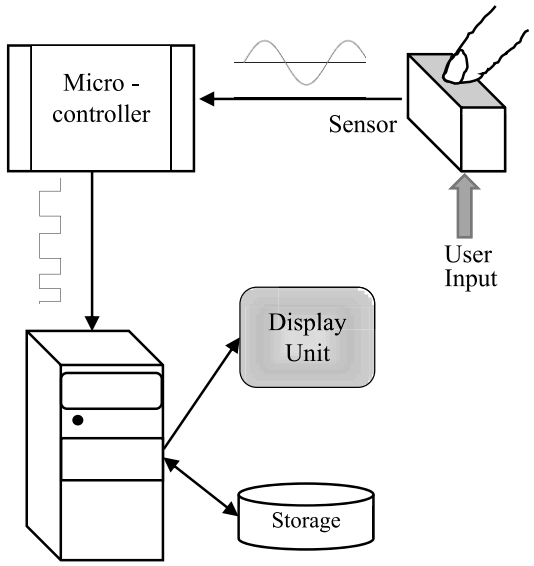

FIGURE 4. The layout of data acquisition system used for collecting user samples.

scan their fingers in a sequence of five swipes. Hence, the acquisition from a capacitive sensor is enabled for about ten thousand milliseconds to let the users swipe their fingers. As the user swipe their fingers, the associated timing data is transferred back to the system via the serial bus interface at a baud rate of 9600 (bps). The data is represented by an array of sensed values sampled at 5 milliseconds.

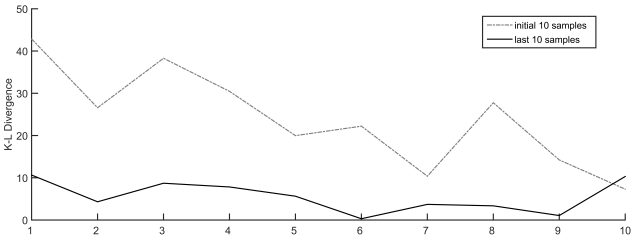

FIGURE 5. User's sample stability analysis using K-L divergence.

A pool of 50 volunteers, from different educational backgrounds and in the age group of 20-41 years, both males and females, have participated in the study. In order to cover the variability of the behavioral characteristics, the data acquisition is done over a period of seven weeks. Each volunteer had a maximum of three sessions per day. A statistical analysis was conducted on initial input patterns from some randomly selected individuals to observe the underlying intra-class variability. Kullback-Leibler (K-L) divergence, which is also known as the relative entropy, is used as a measure for this assessment [42]. In Fig. 5, the initial samples from a user show higher variability in comparison to the samples collected at a later time for the same user. We attribute this to users requiring a few sessions of practice to stabilize. To overcome this, the data from first few sessions of each user is discarded in our experimental analysis.

Each user is asked to choose a finger sequence of their own choice during the enrolment process, involving fingers from any of their two hands. However, two constraints are applied, in order to properly explore the discriminating power of the system. Firstly, the length of sequence from every user is fixed, making a fair evaluation of system performance. Secondly, the length of the swiping sequence is limited to exactly 5 swipes per acquisition attempt. This is in contrast to reports of researchers, working in the field of keystroke dynamics, [31], [32] claiming that system performance deteriorates dramatically when the sequence length falls below ten. While this constraint imposes a great challenge on the system performance, it also provides the user convenience in form of single hand operation as well as ease to memorize, resulting into increased user acceptability. A rigorous assessment is carried out by applying these constraints to evaluate the performance on the moderate sized dataset. These constraints can be removed for large scale applications making the system more robust to attacks. The constructed data set is made publicly available for research and academia [43].

C. FEATURE PROCESSING

The fingerprint dynamics rely on various parameters derived from timing information associated with finger swipes against the sensor. The system is designed to record comprehensive timing information, comprising of the events of finger press and release. The features are derived in three basic stages: pre-processing, feature extraction, and feature subset selection. In the literature, feature extraction is considered to have a substantial impact on the system performance [44]. For fast, efficient, and robust feature extraction, pre-processing is usually done to derive the data in a suitable form for further processing. Feature selection is a process of selecting the most suitable features out of the derived feature set.

1) PREPROCESSING AND FEATURE EXTRACTION

The acquired data may contain noise caused by phantom spikes or discontinuities, due to external factors or mishandling by the user. To deal with such deficiencies, preprocessing operations like basic threshold-based filtering are performed to detect and remove the spikes, as well as fill the gaps caused by discontinuities in the acquired signal. The processed data is then utilized by feature extraction module to extract primary parameters that are vital to derive the behavioral characteristics. Two such primary parameters that can be derived from n fingerprint scan events are F1 or Dwell time (1), i.e. time duration between the finger press and release of the same finger, and F2 or Flight Time (2), i.e. the duration between a finger release and the successive finger press, expressed as follows.

$$D_{pr}(i) = f_{pr}(i) - f_{pp}(i), \quad where\ i = 1 \ldots n \tag{1}$$

$$F_{rp}(i) = f_{pp}(i+1) - f_{pr}(i), \quad where\ i = 1 \ldots n-1 \tag{2}$$

where for ith finger swipe $f_{pp}(i)$ and $f_{pr}(i)$ are the two values representing touchdown (press) and lift-up (release)

events. Similarly, features F3 and F4 can be derived from the timing information between a finger press and the consecutive finger press (3) and a finger release and the subsequent finger release (4) events respectively.

$$FD_{pp}(i) = f_{pp}(i+1) - f_{pp}(i), \quad where\ i = 1 \ldots n-1 \tag{3}$$

$$FD_{rr}(i) = f_{pr}(i+1) - f_{pr}(i), \quad where\ i = 1 \ldots n-1 \tag{4}$$

Several other secondary features can be derived from these primary features as shown in Table I and Table II.

TABLE 1. Features derived from dwell time.

Feature	Expression	
F5	$D_{mean} = \frac{1}{n}\sum_{i=1}^{n} D_{pr}(i)$	(5)
F6	$D_{psum}(k) = \sum_{i=k}^{k+1} D_{pr}(i), \quad where\ k = 1 \ldots n-1$	(6)
F7	$D_{tsum}(k) = \sum_{i=k}^{k+2} D_{pr}(i), \quad where\ k = 1 \ldots n-2$	(7)
F8	$D_{sqrt}(i) = \sqrt{D_{pr}(i)}, \quad where\ i = 1 \ldots n$	(8)
F9	$D_{max} = \max(D_{pr})$	(9)
F10	$D_{min} = \min(D_{pr})$	(10)
F11	$D_{nroot} = \sqrt[n]{\prod_{i=1}^{n} D_{pr}(i)}$	(11)
F12	$D_{log}(i) = \log(D_{pr}(i)), \quad where\ i = 1 \ldots n$	(12)
F13	$D_{std} = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(D_{pr}(i) - D_{mean})^2}$	(13)
F14	$D_{norm}(k) = \frac{D_{pr}(k)}{\left(\sum_{i=1}^{n} D_{pr}(i)\right)} where\ k = 1 \ldots n$	(14)
F15	$D_{tnorm}(k) = \frac{D_{pr}(k)}{\left(\sum_{i=1}^{n} D_{pr}(i) + \sum_{i=1}^{n-1} F_{rp}(i),\right)}$ where $k = 1 \ldots n$	(15)

2) FEATURE SELECTION

Literature indicates the importance of feature selection task in machine learning applications [46]. It has emerged as a prominent maneuver, in the field of machine learning and pattern recognition, to improve the overall performance of a system [14]. Eliminating irrelevant features and selecting the group of most discriminating features, can also alleviate the curse of dimensionality, resulting in reduced system complexity, processing time, and associated cost [45]. Studies like [47], report its influence even on state-of-the-art

TABLE 2. Features derived from flight time.

Feature	Expression	
F16	$F_{mean} = \frac{1}{n-1}\sum_{i=1}^{n-1} F_{rp}(i)$	(16)
F17	$F_{psum}(k) = \sum_{i=k}^{k+1} F_{rp}(i), \quad where\ k = 1 \ldots n-2$	(17)
F18	$F_{tsum}(k) = \sum_{i=k}^{k+2} F_{rp}(i), \quad where\ k = 1 \ldots n-3$	(18)
F19	$F_{sqrt}(i) = \sqrt{F_{rp}(i)}, \quad where\ i = 1 \ldots n-1$	(19)
F20	$F_{max} = \max(F_{rp})$	(20)
F21	$F_{min} = \min(F_{rp})$	(21)
F22	$F_{nroot} = \sqrt[n-1]{\prod_{i=1}^{n-1} F_{rp}(i)}$	(22)
F23	$F_{log}(i) = \log(F_{rp}(i)), \quad where\ i = 1 \ldots n-1$	(23)
F24	$F_{std} = \sqrt{\frac{1}{n-2}\sum_{i=1}^{n-1}(F_{rp}(i) - F_{mean})^2}$	(24)
F25	$F_{norm}(k) = \frac{F_{rp}(k)}{\left(\sum_{i=1}^{n-1} F_{rp}(i)\right)} where\ k = 1 \ldots n-1$	(25)
F26	$D_{tnorm}(k) = \frac{F_{rp}(k)}{\left(\sum_{i=1}^{n} D_{pr}(i) + \sum_{i=1}^{n-1} F_{rp}(i)\right)}$ where $k = 1 \ldots n$-1	(26)

classifiers, which can scale to handle an increased number of features. Typical classifiers do not provide the information about how well the features are able to represent the class. Thus a sophisticated method is desired, to identify the combination of important features, for effective classification.

In this paper, we use a randomized genetic algorithm (GA) based wrapper feature selection approach [44]. Lately, GA-based methods have been deployed in various fields of machine learning for optimal subset selection [46]. Although GA-based methods usually require higher computation time, they are the preferred choice for problems with not so vast dataset. Moreover, the wrapper based methods have an edge over the basic filter-based feature selection methods that it is not limited to find the most discriminatory features only but also the combination of such features. Hence, using GA-based feature selection scheme, we try to discover a combination of the most discriminating feature subsets that result in low classification error. This is achieved by employing a classifier at the base of GA for evaluation of the selected subsets at each iteration [48] (Fig 6).

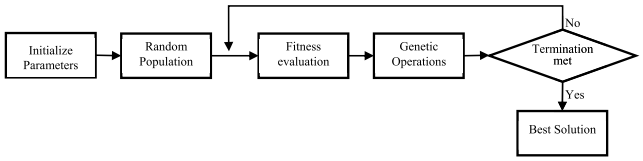

FIGURE 6. GA-based feature subset selection scheme.

Two simple wrapper-based approaches with feature subset evaluation using k-Nearest Neighbour (k-NN) and Support Vector Machine (SVM) were employed [46], [49]. GA is designed to optimize two objectives, one is to select the subset of the most important features that results in high classification accuracy, and second is the length of feature vectors, for reduced computation cost of classification. A snapshot of GA-based feature selection algorithm is depicted in Fig. 6. We have used the well-known tournament selection method and rank-based fitness scaling function. The output feature subset is fed to respective classification approach.

IV. RESULTS AND DISCUSSION

In this section, we present the analysis of selected features as mentioned in the previous section, then we describe in detail the experiments conducted in three different scenarios. Further, we discuss the results and the findings of this study.

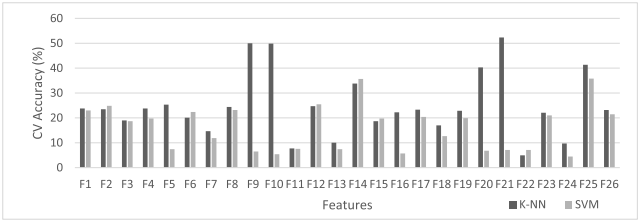

FIGURE 7. Feature discriminability analysis for k-NN and SVM classifiers.

A. FEATURE ANALYSIS

The features used in this study are listed in the Fig. 7 along with their individual discriminability power in terms of leave one out cross-validation accuracy. A total of 16 runs (8 for each classifier) are performed to study the underlying randomness of the GA-based feature selection approach, and the correlation among the features, if any. For a fair evaluation, the same number of features are selected for both the classifiers. We find that a combination of 14 features met the trade-off between performance and length of the feature vector, a comparative representation of which is given in Fig. 8. From the statistical analysis of the data depicted in Fig. 7 and 8 we draw many interesting deductions, namely,

1) The initial analysis of the Fig. 7 indicates that some features performed harmoniously for both the classifiers, whereas some exhibited a significant difference in performance. For example F9 and F10 works well with k-NN but are not at par with SVM which justifies the use of wrapper feature selection method.

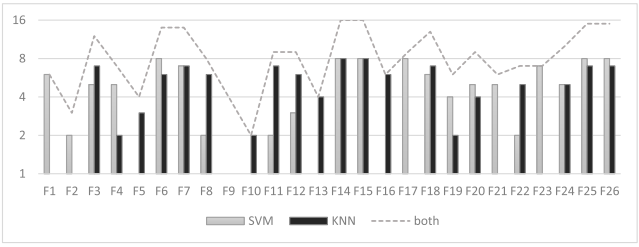

FIGURE 8. Prevalence of features selected using different runs of GA-based feature selection algorithm.

2) Some features are repeatedly selected for one classifier for most of the runs while for the other those features have not been selected even once, see Fig. 8. For example, F1 and F23 were repeatedly selected for SVM, but never for k-NN. This ascertains that features which are vital for one classifier, may not be important for the other.
3) The statistical analysis of the features selected by multiple runs of GA-based feature selection algorithm designates the dominance of certain features, for example, F6, F7, F15, F18 and F26 among others. While some features like F9, which is the maximum dwell time for any attempt, is never selected for any of the classifiers.
4) The collective analysis of Fig. 7 and Fig. 8 indicates that an individually good performing feature does not guarantee to work well when combined with others. For example F9 in Fig. 7 for k-NN achieves 2nd highest cross-validation (CV) accuracy individually but is never selected by multiple runs of GA, whereas the F15 having half the CV accuracy of the F9 is selected for k-NN as well as SVM both.

B. PERFORMANCE EVALUATION

For any authentication system, the performance analysis is a two-fold task, which includes how well the system recognizes a genuine user attempt as well as how well the system detects the false attempts by imposters. The problem domain thus can be divided into two subtasks. Out of 50 subjects first, a group of 19 individuals was randomly selected as genuine users. Another group of imposters was created with 31 participants in order to assess the discrimination power of the postulate. Out of these (31), 18 participants were asked to provide forged samples to bypass the system with only the knowledge of the genuine user's secret sequence's length (zero-effort imposters). Whereas to the rest 13 (31 - 18) participants, the secret sequences of each genuine user was disclosed completely (active imposters). A total of 3240 fingerprint swipe samples, resulting from 648 fingerprint swipe sequence of length five each, were collected from genuine users. For experimentation, 389 finger sequences of the total sequences (60% of 648) are used for training purpose and rest (40% of 648) for testing. Again 3185 samples, from 637 sessions (fingerprint swipe sequences), are collected for imposter attacks, out of which 245 are zero-effort and 392 are

from active imposters. Thus a total of 896 test observations are collected, summing to 1285 finger swipe sequences over all, which involved 6425 finger swipes. Unlike the active imposter dataset where we had dedicated attackers per user, zero-effort imposter attempts are simply the random sequence of identical length, hence they are used against every user, resulting into 4655 (i.e. 245*19) zero-effort imposter attempts of length five each.

Following this arrangement of data, classification is performed by using two popular methods: k-NN and SVM classifiers. We used Matlab®2015 libraries for both the classifiers. Various associated parameters of the classifiers are selected using 'leave one out' cross-validation. For all the experiments conducted in this study, identical training and testing sets are used for the two different classifiers under different attack scenarios. The classifier parameters also remained invariant for different experiments conducted. A description of the classifiers may be briefly summarized as follows:

k-NN is considered as one of the most preferred choices for time dynamics based authentication systems [30], [49]–[51]. A simple k-NN classifier with Mahalanobis distance, computed using a positive definite covariance matrix C, is implemented. For classification distance between test sample q_s from test data Q and the training sample x_m of training data X is calculated using (27). Squared inverse distance weights are used for calculating the score by measuring the distance from the new test sample to the nearest feature samples in the training data. The number of neighbors was selected as 4 after testing the range from 1 to 10.

$$D_{Mah} = \sqrt{(x_m - q_s)\, C_x\, (x_m - q_s)^T} \tag{27}$$

where m = 1,2…no. of training observation X, and s = 1,2,….no. of test observations Q.

SVM, also known as maximum margin classifier, draws a decision boundary or hyperplane with a maximum distance between two classes by solving a quadratic optimization problem. SVM is quite a popular learning algorithm due to good generalization capability [49], and is widely used in the closely related, keystroke dynamics based studies as well, [30], [44]. In this paper, a polynomial kernel of second order is implemented with 'one versus all' (OvA) method. Hence, for N enrolled users, N models are trained using binary SVM classifiers by assigning a positive class label to samples of a user, and negative to rest of them. This is repeated for each of the N users.

For verification task, the classification turns into a binary problem of accepting or rejecting the input pattern. Hence, for a given test sample ω^t, the job is to determine whether it is from the claimed identity or by an imposter. For this purpose, the test sample is matched against the user template (ω^o) of the claimed identity and a decision is made on the basis of (28), using the similarity score obtained from the learning algorithm (for the test sample) and the threshold (τ).

$$I \in \begin{cases} accept, & if\ f\left(\omega^o, \omega^t\right) > \tau \\ reject, & otherwise \end{cases} \tag{28}$$

where $f(\omega^o, \omega^t)$ is the matching function that produces a similarity score.

The Equal Error Rate (EER) is used as the evaluation criteria for the identity verification experiments [38]. EER is a prominent measure of the system performance as it aggregates measures, False Positive Rate (FPR) and False Negative Rates (FNR), and act as an operational point between the two errors [51]. FPR (29) and FNR (30) denotes the fraction of imposter attempts accepted as genuine and the genuine user attempts rejected respectively, by the system.

$$FPR = \frac{Number\ of\ imposters\ accepted}{Total\ number\ imposter\ attempts} * 100 \tag{29}$$

$$FNR = \frac{Number\ of\ genuine\ input\ rejected}{Total\ number\ genuine\ attempts} * 100 \tag{30}$$

For experimentation, we first assess the system performance by taking into account the complete set of 26 features in three attack scenarios using the above-mentioned classification paradigms. Then we repeat the same set of experiments but only with the selected feature subsets from section III-C.

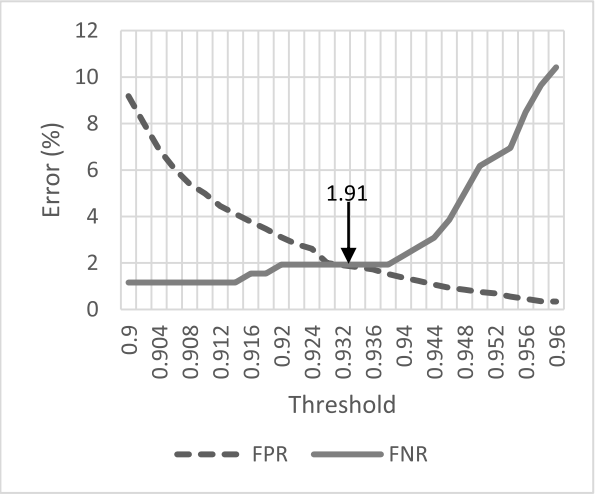

FIGURE 9. FPR and FNR plot and the corresponding EER for the verification system including all the features using SVM classifier.

1) SCENARIO1: ALL IMPOSTER ATTACK

Under the all imposter attack scenario, the evaluation of verification accuracy is done by involving both the zero effort and active imposter attempts along with genuine users'. Thus resulting in a total of 896 test samples. For k-NN based system FPR and FNR of 1.33% and 1.54% is achieved respectively. For the SVM-based system, slightly lower performance is achieved with FPR and FNR of 1.90% and 1.93% respectively. Fig. 9 illustrates the plot of FPR and FNR against the varying range of threshold value and EER for the SVM-based system.

2) SCENARIO 2: ACTIVE IMPOSTER ATTACK

In order to explore the ability of the system to resist spoof attacks, it is crucial to conduct various individual and specific attacks separately and observe their impact on the system performance. Systems that perform well for user identity verification in presence of genuine attempts may fail when presented with dedicated imposter attempts. Hence, we conducted an active imposter attack where the secret sequence of every legitimate user was disclosed to each of the imposters. As discussed in section IV (b), each imposter tried to bypass the system by using the knowledge of the secret sequence of the targeted genuine user. Similar to the experiment performed for scenario 1, two systems, based on the two classifiers, are tested in the presence of active imposter attempts. An FPR and FNR equal to 3.32% and 4.25% is achieved for k-NN based system, whereas for SVM-based system FPR and FNR equal to 7.14% and 6.95% are achieved respectively.

3) SCENARIO3: ZERO-EFFORT IMPOSTER ATTACK

Typically attackers hardly have any information about the genuine user's real input patterns and thus they try to outwit the system by trying several random inputs. To mimic this we conducted a zero-effort imposter attack, where the only information an imposter had was the length of the secret sequence of fingers. A total of 4655 imposter attempts were conducted along with genuine users' data. The systems based on both the classifiers are tested, and FPR and FNR equal to 1.2%, 1.16% are achieved for k-NN and 1.31%, 1.16% for SVM respectively.

TABLE 3. Performance of verification system using all the features.

Classifier Paradigm	Attack Scenario	EER (%)
SVM	All Imposter Attack	1.91
	Active Imposter	7.05
	Zero Effort Imposter	1.23
KNN	All Imposter Attack	1.43
	Active Imposter	3.78
	Zero Effort Imposter	1.18

The misclassification rates for all the six experiments, conducted in the three different scenarios, are reported in terms of EER values in Table III. It is evident from the results that while SVM and k-NN perform equivalently well for zero-effort attacks, their performance degrades significantly for active imposter attacks. The obtained results also indicate that SVM is more affected by active imposter attacks as compared to k-NN. Moving beyond this initial analysis, we further investigate the above three scenarios for the selected 14 feature subset under analogues conditions.

For scenario 1, considering all the samples from both the imposters and genuine users, FPR and FNR equal to 0.76%, 0.77% for k-NN and 2.17%, 1.93% for SVM are achieved respectively, comprising samples from both the imposters. Whereas for scenario 2, i.e. active imposter attack, FPR and FNR equal to 3.32%, 3.47% for k-NN and 7.4%, 7.34% for SVM are achieved. Again with scenario 3, involving only zero-effort imposters, FPR and FNR equal to 0.40%, 0.40% for k-NN and 1.14%, 1.16% for SVM are achieved.

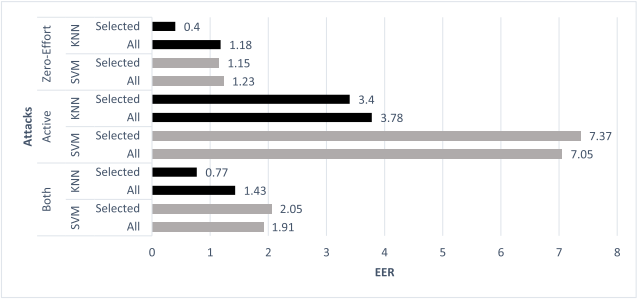

FIGURE 10. A comparative analysis of EER values for different attack scenarios with all features and selected feature subset for k-NN and SVM classifiers.

Fig. 10 depicts collective EER values for all the above verification experiments conducted. The analysis showed that the fingerprint dynamics based system achieved comparable performance with a short length input pattern (5 swipes per user) for all features selected as well as a subset of features in all the three scenarios. From the comparative evaluation of the performance of the two classification algorithm involved, the slightly inferior performance of the SVM as compared to k-NN can be attributed due to the fact that the features used in the study are more suitable for the k-NN classifier than the SVM. The results obtained, follow the assumption of feature subset selection task to improve the performance of the system. It can be seen in Fig. 10 that there is slight deterioration in the performance of SVM, except scenario 3, with about half the features selected. This is attributed to the fact that in this paper, the wrapper approach investigated the features only on the basis of genuine users' data samples. Thus the features selected for SVM classifier resulted in subpar performance for the scenario where active imposter data is involved. On the other hand, there is a significant improvement in the performance of k-NN based system. This corroborates to the deductions made in the literature [46], about the sensitiveness of k-NN classifiers to the selection of features.

However, the objective of this manuscript was not to find the best learning algorithm, but to investigate how well the system performs in the different attack scenarios. Although the exemplary results achieved are quite promising, the performance is still not high enough to establish the fingerprint dynamics based authentication system as a prominent choice over the other established biometric modalities. The findings from this work thus suggest a trajectory for future work alleviating the deficit in the work presented. A few of

the approaches to improve the performance accuracy might be to use more training data, extracting more discriminant features, and employing advanced learning algorithms, like the ensemble classifiers. Other possible solution might be to deploy more sophisticated hardware, capable of providing stable values with the low noise level in the acquired signal, to reduce the intra-user variability. Improving the resolution of the clock deployed, as discussed in section II, can also contribute to minimizing the interclass similarity of user profiles.

V. CONCLUSION

This paper presented a study on spoof resistance capabilities of the recently introduced behavioral biometric technique, namely, fingerprint dynamics. Two biometric systems using k-NN and SVM classifiers are implemented that utilize associated time measurements from multi-instance fingerprint acquisition events. Total 12 experiments are conducted on samples from 1,285 sessions, collected from 50 subjects which involved 6,425 finger swipes. From the selection of best-suited feature subsets using GA based approach and the exhaustive feature analysis, it is found that features may have dissimilar prominence for distinct classifiers. The paper investigated the verification capability of the technique to distinguish legitimate user successfully under different attack scenarios, including the active imposters. Overall best EER of 0.4% is achieved for zero effort imposter attack and highest of 7.37% under active imposter attacks. Thus the active imposter attacks are most successful. The conducted experiments successfully demonstrate the discriminative information in the fingerprint dynamics of individuals. Based on the investigation and findings, we perceived some interesting lessons, which may suggest a trajectory for future work.

Our study has provided an insight into the expediency of the proposed technique as a tool to verify human identity and established an approach that can effectively employ in a vast application domain. The foreseen applications of fingerprint dynamics are in assisting the fingerprint recognition system for improved performance. The primary domain would include strengthening spoof resistance and the system accuracy even in the event of a dedicated direct attack on the system. Additionally, it can be deployed with already existing fingerprint sensors if the time logging capability is enabled. The only challenge is the deployment of multi-instance fingerprint acquisition but it also provides enhanced performance and security benefits. Furthermore, being unobtrusive the fingerprint dynamics would alleviate the deficit of multi-biometric systems, generally faced with traits that demand separate data acquisition

REFERENCES

[1] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognit. Lett.*, vol. 79, pp. 80–105, Aug. 2016.

[2] J. A. Unar, W. C. Seng, and A. Abbasi, "A review of biometric technology along with trends and prospects," *Pattern Recognit.*, vol. 47, no. 8, pp. 2673–2688, Aug. 2014.

[3] A. Jain, P. Flynn, and A. A. Ross, Eds., *Handbook of Biometrics*. NY, USA: Springer, 2007.

[4] P. Turaga, R. Chellappa, V. S. Subrahmanian, and O. Udrea, "Machine recognition of human activities: A survey," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 11, pp. 1473–1488, Nov. 2008.

[5] L. Wang, Ed., *Behavioral Biometrics for Human Identification: Intelligent Applications*. Hershey, PA, USA: IGI Global, 2009.

[6] A. K. Jain and K. Nandakumar, "Biometric authentication: System security and user privacy," *IEEE Comput.*, vol. 45, no. 11, pp. 87–92, Nov. 2012.

[7] J. Roth, X. X. Liu, and D. Metaxas, "On continuous user authentication via typing behavior," *IEEE Trans. Image Process.*, vol. 23, no. 10, pp. 4611–4624, Oct. 2014.

[8] A. A. E. Ahmed and I. Traore, "A new biometric technology based on mouse dynamics," *IEEE Trans. Depend. Sec. Comput.*, vol. 4, no. 3, p. 165, Jul./Sep. 2007.

[9] C. E. Rogers, A. W. Witt, A. D. Solomon, and K. K. Venkatasubramanian, "An approach for user identification for head-mounted displays," in *Proc. ACM Int. Symp. Wearable Comput.*, Sep. 2015, pp. 143–146.

[10] I. Deutschmann and J. Lindholm, "Behavioral biometrics for DARPA's active authentication program," in *Proc. IEEE Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2013, pp. 1–8.

[11] H. Gamboa and A. Fred, "A behavioral biometric system based on human-computer interaction," *Proc. SPIE*, vol. 5404, pp. 381–392, Aug. 2004.

[12] P. Wild, P. Radu, L. Chen, and J. Ferryman, "Robust multimodal face and fingerprint fusion in the presence of spoofing attacks," *Pattern Recognit.*, vol. 50, pp. 17–25, Feb. 2016.

[13] A. Jain and V. Kanhangad, "Exploring orientation and accelerometer sensor data for personal authentication in smartphones using touchscreen gestures," *Pattern Recognit. Lett.*, vol. 68, pp. 351–360, Dec. 2015.

[14] I. Bhardwaj, N. D. Londhe, and S. K. Kopparapu, "A novel behavioural biometric technique for robust user authentication," *IETE Tech. Rev.*, pp. 1–13, Aug. 2016. [Online]. Available: http://dx.doi.org/10.1080/02564602.2016.1203271

[15] J. R. Bhatnagar, B. Lall, and R. K. Patney, "Performance issues in biometric authentication based on information theoretic concepts: A review," *IETE Tech. Rev.*, vol. 27, no. 4, pp. 273–285, Jul. 2010.

[16] Z. Akhtar, C. Micheloni, and G. L. Foresti, "Biometric liveness detection: Challenges and research opportunities," *IEEE Security Privacy*, vol. 13, no. 5, pp. 63–72, Sep./Oct. 2015.

[17] N. Neverova *et al.*, "Learning human identity from motion patterns," *IEEE Access*, vol. 4, pp. 1810–1820, Apr. 2016.

[18] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed. London, U.K.: Springer, 2009.

[19] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[20] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Comput. Surv.*, vol. 47, no. 2, Jan. 2014, Art. no. 28.

[21] I. Bhardwaj, N. D. Londhe, and S. K. Kopparapu, "A spoof resistant multibiometric system based on the physiological and behavioral characteristics of fingerprint," *Pattern Recognit.*, vol. 62, pp. 214–224, Feb. 2017.

[22] A. Rattani, W. J. Scheirer, and A. Ross, "Open set fingerprint spoof detection across novel fabrication materials," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2447–2460, Nov. 2015.

[23] C. Champod and M. Espinoza, "Forgeries of fingerprints in forensic science," in *Handbook of Biometric Anti-Spoofing*, S. Marcel, M. S. Nixon, and S. Z. Li, Eds. London, U.K.: Springer, 2014, ch. 2, pp. 13–34.

[24] C. Wang, K. Li, Z. Wu, and Q. Zhao, "A DCNN based fingerprint liveness detection algorithm with voting strategy," in *Proc. Chin. Conf. Biometric Recognit.*, Nov. 2015, pp. 241–249.

[25] J. Feng and A. K. Jain, "Fingerprint reconstruction: From minutiae to phase," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 2, pp. 209–223, Feb. 2011.

[26] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, Eds., *Handbook of Fingerprint Recognition*. London, U.K.: Springer, 2009.

[27] I. Bhardwaj, N. D. Londhe, and S. K. Kopparapu, *Method and System for Multifactor Biometric Authentication*, document 3895/MUM/2014, Dec. 2014.
[28] J. A. Robinson, V. W. Liang, J. A. M. Chambers, and C. L. MacKenzie, "Computer user verification using login string keystroke dynamics," *IEEE Trans. Syst., Man A, Syst. Humans*, vol. 28, no. 2, pp. 236–241, Mar. 1998.
[29] M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," *Appl. Soft Comput.*, vol. 11, no. 2, pp. 1565–1573, Mar. 2011.
[30] K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," in *Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, Jun./Jul. 2009, pp. 125–134.
[31] K. Kotani and K. Horii, "Evaluation on a keystroke authentication system by keying force incorporated with temporal characteristics of keystroke dynamics," *Behaviour Inf. Technol.*, vol. 24, no. 4, pp. 289–302, Jul. 2005.
[32] J. Montalvão, E. O. Freire, M. A. Bezerra, Jr., and R. Garcia, "Contributions to empirical analysis of keystroke dynamics in passwords," *Pattern Recognit. Lett.*, vol. 52, pp. 80–86, Jan. 2015.
[33] M. H. Lin, S. Gao, K. S. Huang, and J.-M. Wang, "Sequence-encoded multiple biometric template security system," U.S. Patent 6 393 139 B1, May 21, 2002.
[34] J. A. Moore, "Fingerprint scan order sequence to configure a print system device," U.S. Patent 8 179 543, May 15, 2012.
[35] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: A novel approach to authentication on multi-touch devices," in *Proc. ACM SIGCHI Conf. Human Factors Comput. Syst.*, May 2012, pp. 977–986.
[36] X. Zhao, T. Feng, W. Shi, and I. A. Kakadiaris, "Mobile user authentication using statistical touch dynamics images," *IEEE Trans Inf. Forensics Security*, vol. 9, no. 11, pp. 1780–1789, Nov. 2014.
[37] L. Zhou, Y. Kang, D. Zhang, and J. Lai, "Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones," *Decision Support Syst.*, vol. 92, pp. 14–24, Sep. 2016.
[38] L. C. F. Araujo, L. H. R. Sucupira, M. G. Lizarraga, L. L. Ling, and J. B. T. Yabu-Uti, "User authentication through typing biometrics features," *IEEE Trans. Signal Process.*, vol. 53, no. 2, pp. 851–855, Feb. 2005.
[39] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. Van Oorschot, "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism," *IEEE Trans. Depend. Sec. Comput.*, vol. 9, no. 2, pp. 222–235, Mar. 2012.
[40] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *Int. J. Human-Comput. Stud.*, vol. 63, no. 1, pp. 102–127, Jul. 2005.
[41] I. Bhardwaj, N. D. Londhe, and S. K. Kopparapu, "Fingerprint dynamics: A novel biometrics for personal authentication," presented at the IEEE Int. Conf. Signal Inf. Process. (IConSIP), Nanded, India, Oct. 2016, pp. 6–8.
[42] A. Morales, J. Fierrez, and J. Ortega-Garcia, "Towards predicting good users for biometric recognition based on keystroke dynamics," in *Proc. Eur. Conf Comput. Vis.*, 2014, pp. 711–724.
[43] I. Bhardwaj. *2015 Fingerprint Dynamics Database 2015 Part I*, accessed on Jan. 7, 2016. [Online]. Available: https://goo.gl/YcQlYy
[44] E. Yu and S. Cho, "GA-SVM wrapper approach for feature subset selection in keystroke dynamics identity verification," in *Proc. IEEE Int. Joint Conf. Neural Netw.*, Jul. 2003, pp. 2253–2257.
[45] I. Bhardwaj, N. D. Londhe, and S. K. Kopparapu, "Feature selection for novel fingerprint dynamics biometric technique based on PCA," presented at the 5th IEEE Int Conf Adv. Comput., Commun. Informat., Jaipur, India, Sep. 2016, pp. 1730–1734.
[46] M. Pal, "Hybrid genetic algorithm for feature selection with hyperspectral data," *Remote Sens. Lett.*, vol. 4, no. 7, pp. 619–628, Jul. 2013.
[47] A. Ç. Pehlivanlı, "A novel feature selection scheme for high-dimensional data sets: Four-staged feature selection," *J. Appl. Statist.*, vol. 43, no. 6, pp. 1140–1154, Apr. 2016.
[48] M. L. Raymer, W. F. Punch, E. D. Goodman, L. A. Kuhn, and A. K. Jain, "Dimensionality reduction using genetic algorithms," *IEEE Trans. Evol. Comput.*, vol. 4, no. 2, pp. 164–171, Jul. 2000.
[49] C.-J. Huang, D.-X. Yang, and Y.-T. Chuang, "Application of wrapper approach and composite classifier to the stock trend prediction," *Expert Syst. Appl.*, vol. 34, no. 4, pp. 2870–2878, May 2008.
[50] P. H. Pisani and A. C. Lorena, "A systematic review on keystroke dynamics," *J. Brazilian Comput. Soc.*, vol. 19, no. 4, pp. 573–587, Nov. 2013.
[51] G. Kambourakis, D. Damopoulos, D. Papamartzivanos, and E. Pavlidakis, "Introducing touchstroke: Keystroke-based authentication system for smartphones," *Secur. Commun. Netw.*, vol. 9, no. 6, pp. 542–554, Jun. 2014.

ISHAN BHARDWAJ (S'12) received the B.Tech. degree in computer science and engineering from Uttar Pradesh Technical University, Lucknow, India, in 2010, and the M.Tech. degree in computer technology from the National Institute of Technology at Raipur, Raipur, India, in 2012, where he is currently pursuing the Ph.D. degree.

Since 2012, he has been a recipient of the MHRD Fellowship from the Government of India. His research interest includes the information security, biometrics, and pattern recognition techniques. Apart from articles in conferences and journals, he holds two patents (pending) in the field of biometrics.

NARENDRA D. LONDHE (M'10–SM'13) received the B.E. degree from Amravati University in 2000, and the M.Tech. and Ph.D. degrees from IIT Roorkee, Roorkee, India, in 2004 and 2011, respectively. He is currently an Assistant Professor with the Department of Electrical Engineering, National Institute of Technology at Raipur, Raipur. He has authored articles in many reviewed journals and conferences.

SUNIL K. KOPPARPU (M'05–SM'14) received the Ph.D. degree in electrical engineering from IIT Bombay, Mumbai, India, in 1997.

From 1997 to 2000, he was with the Commonwealth Scientific and Industrial Research Organization, Brisbane, Australia. He was with the Research and Development Group, Aquila Technologies Pvt., Ltd., India, as an Expert for developing virtual self-line of e-commerce products. He was with the Cognitive Systems Research Laboratory, Tata Infotech Ltd., as a Senior Research Member, in 2001. He is currently a Principal Scientist with TCS Innovations Laboratories, Mumbai, he is actively involved in the areas of speech, image, and natural language processing. Apart from several patents and journal and conference publications, he co-authored books and more recently a Springer brief on non-linguistic analysis of call center conversation.