ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

PULSE COUNTING BIOMETRIC

N.V.S.Vamsi Krishna[1], Ms.S.Pavithra[2]
Student, Department of ECE, Saveetha University[1]
Assistant professor, Department of ECE, Saveetha University[2]
Saveetha School of Engineering, Chennai.

Received on: 15.08.2016 *Accepted on: 20.09.2016*

Abstract:

This paper propose a new biometric system that converts the human body's response to an electrical square pulse signal. However this biometric will be accustomed enhance security within the context of example applications: (1) as a further authentication mechanism in PIN entry systems, and (2) as an eternal authentication mechanism on a secure terminal. The pulse-response biometric is effective as a result of every organic structure exhibits a singular response to an indication pulse applied at the palm of 1 hand, and measured at the palm of the opposite. Employing a paradigm setup, we tend to show that users will be properly identified, with high chance, in an exceedingly matter of seconds. This identification mechanism integrates with alternative well established strategies and offers a reliable further layer of further security. This paper tend to build a proof-of-concept paradigm and perform experiments to validate the feasibility of mistreatment pulse-response as a biometric. These results in unit terribly encouraging: we tend to bring home the bacon accuracies of 100 percent over a static knowledge set and half a mile over a knowledge set with samples appropriated many weeks.

1. Introduction:

Many modern access control systems augment the traditional two-factor authentication procedure (something you recognize and one thing you have) with a 3rd factor: "something you are", i.e. some form of biometric authentication .This additional layer of security comes in several flavors: from fingerprint readers on laptops accustomed facilitate straightforward login with one finger swipe, to iris scanners used as auxiliary authentication for accessing secure facilities. within the latter case, the licensed user usually presents a sensible card, then sorts in an exceedingly PIN, And finally performs an iris (or fingerprint) scan. During this paper, we tend to propose a brand new biometric supported

the human body's response to a sq. pulse signal. we tend to contemplate 2 motivating sample scenarios: The first is that the ancient access management setting represented on top of wherever the biometric is employed as a further layer of security once a user enters a PIN, e.g., into a bank ATM. The pulse-response biometric facilitates unification of the steps of PIN entry and biometric capture. We tend to use PIN entry as a running example for this state of affairs throughout the paper. This is {often this can be} as a result of PIN pads area unit often fabricated from metal, that makes capturing The continuous authentication drawback is especially difficult to unravel mistreatment ancient statistics. as an example, if fingerprints area unit used rather than pulse-response, the user would need to interrupt work to sporadically swipe a finger on a scanner, which might be terribly unquiet. There are some tries to unravel this drawback employing a digital camera and face recognition .However, such systems will be fooled by a photograph of the legitimate user and that they additionally need the user to stay the top in an exceedingly more-or-less constant position, unless a lot of advanced head following system is employed. To assess efficacy and practicableness of the pulse-response biometric, we tend to design a platform that allows North American nation to assemble pulse response knowledge. Its main purpose is to verify that we will determine users from a population of take a look at subjects. We tend to additionally used it to check the distinctive ability and stability of this biometric over time. we tend to additionally explored 2 systems that apply the pulse response biometric to the 2 sample eventualities mentioned above: one to unobtrusively capture the biometric as a further layer of security once getting into a PIN, and also the alternative – to implement continuous authentication.

The rest of the paper is union as follows: Section II provides some background on statistics and presents our style goals. Section III describes the pulse-response biometric intimately. Sections IV and V gift the PIN entry and continuous authentication systems, severally. Section VI describes the biometric knowledge capture setup and Section VII presents experimental results. Connected work is overviewed in Section VIII and also the paper concludes with Section IX.

2. Background:

This section provides some statistics background and summarizes the word used throughout the paper. Then, style goals

area unit conferred statistics. The means of the term biometric varies looking on context. The North American nation National Science & amp; Technology Council's (NSTC) committee on statistics describes its 2 valid meanings: (1) a measurable biological (anatomical and physiological) and activity characteristic which will be used for automatic recognition of people,(2) an automatic technique of recognizing a personal supported measurable biological (anatomical and physiological) and activity characteristics [6]. Throughout the remainder of this paper we tend to use biometric within the former sense, i.e., as a characteristic of a specific individual. The North American nation National Institute of Standards and Technology (NIST) divide biometric measurements into two categories, physiological and behavioral. The previous depends on the physiology of an individual and includes: fingerprints, hand pure mathematics, face recognition, speech analysis, and iris/retina scans.

Activity statistics relies on user behavior and includes: keystroke timings, pronunciation analysis, gait recognition, and analysis of stylus pressure, acceleration and form in hand-writing. Physiological statistics will facilitate determine a personal from an oversized pool of candidates. However, there are a unit some caveats. In general, physiological statistics area unit thought of moderately difficult to bypass. as an example, though hand pure mathematics is extremely stable over the course of one's adult life, it doesn't offer enough distinctive power to be used because the solely suggests that for identification [6]. Also, some face recognition systems will be fooled by AN appropriately-sized exposure of a legitimate user. this is often actually a weakness if face recognition is employed to unlock a Smartphone. B. Identification vs Identification authentication refers to spot confirmation or verification. Once a user claims a precise identity (e.g., by inserting a card into AN ATM or getting into a ushered into a terminal, and so writing in an exceedingly PIN or a password) authentication entails deciding whether or not the claim is correct. The goal of the biometric classifier is to match this sample to the proverbial template for that user. The classifier returns the probability a match. we tend to visit this sort of comparison as 1:1. Authentication differs from identification, wherever this sample comes from AN unknown user, and also the job of the biometric classifier is to match it to a proverbial sample. We tend to decision this a 1:n comparison. Identification is more divided into 2 types: open-set and closed-set.1 we are saying that AN identification is closed-set, if it's proverbial a priori that the user is within the classifier's information, i.e., the classifier should select the most effective match from a pool of candidates. Otherwise, we tend to visit it as open-set identification.

3. Pulse-Response Biometric:

The pulse-response biometric works by applying a coffee voltage pulse signal to the palm of 1 hand and activity the body's response within the palm of the opposite hand. The signal travels up through the user's arm, across the body part, and down the opposite arm. The biometric is captured by activity the response within the user's hand. This response is then reworked to the frequency domain via quick Fourier rework (FFT). This transformation yields the individual frequency parts (bins) of the response signal, that kind data that's then fed to the classifier. Operating within the frequency domain eliminates a need for positioning the pulses after them area unit measured. Details of our mensuration setup and experiments will be found in Section VII. the most reason for this biometrics' ability to tell apart between users is because of delicate variations in body conduction, at completely different frequencies, among completely different individuals. Once an indication pulse is applied to at least one palm and measured within the alternative, this has got to travel through the body tissue – blood vessels, muscle, fat tissue, animal tissue and bones – to achieve the opposite hand. Variations in bone structure, muscle density, fat content and layout of blood vessels, lead to slight variations within the attenuation of the signal at completely different frequencies. These variations show up as variations within the magnitude of the frequency bins when the FFT. This is often what permits North American nation to tell apart between people. Pulse-response is physiological biometrics incest measures a person's physiological characteristics, instead of however that person behaves. However, it's a lovely property unremarkably related to activity biometrics: it will be captured in an exceedingly fully passive means. Mechanism, Basically it offers the most effective properties of each physiological and activity statistics. At constant time, pulse-response needs special-purpose hardware. Constant is true the other physiological biometric. as an example, fingerprints want a fingerprint reader, face recognition needs a exactness camera and hand pure mathematics – a scanner. Since pulse-response is captured mistreatment electrical signals, there area unit few restrictions on the precise construction of the statistics capture hardware. to live the user, there's a further signature that is really a part of the pulse-response reader.

4. Combining Pinentry with Biometric Capture:

This section describes a way to use pulse-response to reinforce security of PIN entry systems while not inconveniencing the user. A. System And human Models of PIN Entry theme we tend to use a running example of a metal PIN key-pad with an adjacent metal pad for the user's alternative hand. The PIN key-pad has the same old digit (0-9) buttons further

as AN "enter" button. It additionally has AN embedded detector that captures the pulse-signal transmitted by the adjacent metal pad. We will create by mental act this setup within the setting of a bank ATM permitting licensed users to withdraw money. The goal of the human is to impersonate a certified user and withdraw money. We tend to assume that the human can't fool the pulse-response classifier with chance over that found in our experiments represented in Section VII. We tend to assume that the ATM is provided with a modified authentication module that, besides corroborative the PIN, captures the pulse-response biometric and determines the probability of the measured response akin to the user identified by the antecedently inserted ATM card and also the entered PIN. This module works as delineate in Figure one. We tend to assume that the ATM has access to a information of valid users, either domestically or over a network. or else, the user's ATM card will contain knowledge required to perform pulse-response verification. If hold on on the cardboard, this knowledge should be encrypted and attested employing a key proverbial to the ATM; otherwise, the human (who will be assumed to be in possession of the card) may replace it with knowledge matching its own pulse-response.

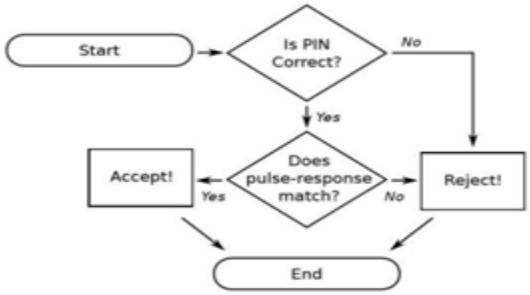


Fig. 1: ATM call flowchart.

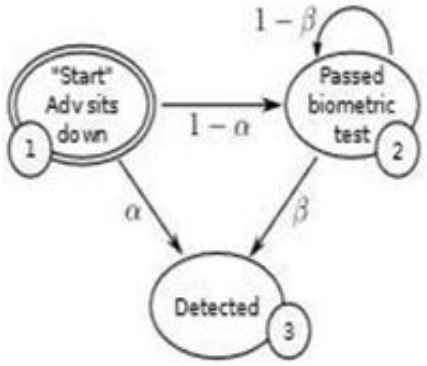
PIN Entry theme The ATM has got to confirm whether or not knowledge sampled from the user whereas getting into the PIN, is in step with that hold on within the information. this needs the utilization of a classifier that yields the probability of a sample returning from a proverbial distribution. The likely hood is employed to see whether or not the fresh measured samples area unit shut enough to the samples within the information to provide a match. mistreatment our paradigm, we will build such choices with high confidence. Before we glance at the safety of the pulse-response PIN entry system, we want to create positive that it meets our style goals. Universal an individual mistreatment this PIN entry system should use each hands, one placed on the metal pad and one to enter the pin. This needs the user 2 even have 2 hands. Whereas, a traditional PIN entry system will be operated with one hand; therefore, catholicity of our system is

somewhat lower. This is often a limitation of the biometric, though a remedy might be to store a flag on the user's ATM card indicating that a incapacity, therefore exempting this person from the pulse-response check. this may permits our approach to graciously degrade to a generic PIN entry system. Distinctive and Permanent. In Section VII-D we tend to show that our paradigm will confirm, with high chance, whether or not an issue matches a specific pulse-response. Thus, it's very unlikely for 2 individuals to exhibit precisely the same pulse response. We tend to additionally show that AN individual's pulse-response remains fairly consistent over time. Unassertive. The projected theme is extremely unassertive. Pulse response measurements, the task looks terribly difficult, if not possible.

5. Continuous

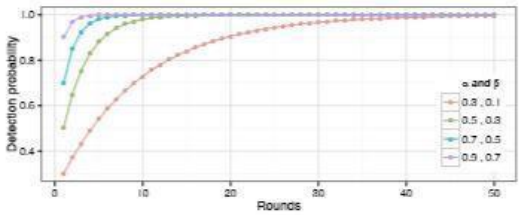
Authentication: We tend to currently gift an eternal authentication theme. Its goal is to verify that constant user World Health Organization at the start (and securely) logged into a secure terminal, continues to be physically gift at the keyboard. Here, the heartbeat response biometric is not any longer used as a further layer of security at login time. Rather, the user's pulse-response biometric is captured at login time and succeeding measurements area unit accustomed manifest the user mistreatment the initial reference. system consists of a package method that manages initial login and frequency of reacquisition for the pulse-response biometric. This method is additionally answerable for displaying warnings to the user and notifying directors just in case of a violation. we tend to visit it because the continuous authentication method (CAP) and assume that neither the legitimate user nor the human will disable it. Biometric kind of like the first user, it should evade the classifier on an eternal basis. we tend to explore this more within the security analysis section below. Security Analysis of Continuous Authentication theme The human will subvert the continual authentication system by managing to use the secure terminal when another user has logged in and (possibly) left. within the analysis below, we tend to assume that the initial user and also the human area unit collaborating. This eliminates any uncertainty that results from the first user discovering that the adversary is using its terminal, which is extremely exhausting to model accurately. The results of our analysis are so a worst-case state of affairs and also the detection chance could be a edge on security provided by the continual authentication system. One parameter in our security analysis is that the range of times biometric acquisition is performed since the time once the human at the start appeared at the keyboard. The longer the amount between every acquisition, the longer it takes for the system to live the human a fixed range of times, and thus (potentially) longer to discover adversary's presence. Policy plays a vital role within the

sensible security of the system. as an example, suppose that the policy is to only show a warning whenever a twin in pulse-response is detected. Such a system can supply very little, if any, security against a determined human. Therefore, for the aim of security analysis, we tend to contemplate the attack foiled as presently because the continuous authentication method detects a retardant.



Markov model of the continuous authentication detection chance.

We model the continual authentication state of affairs mistreatment 2 chances. The first is that the chance that the human is detected in real time, i.e., the first time its pulse-response biometric is captured. This corresponds to sensitivity, i.e., true positive rate rumored in Section VII. we tend to use ninety nine (rather than the 100 percent found in our experiments) so as to model the possibility of creating a clasification mistake at this time. On average, per our experiments, the biometric of the human differs enough from the first user to be detected simply. we tend to visit this chance as ↵. If the adversary's biometric is extremely near that of the first user, it would not be detected anytime biometric capture is performed. If the human manages to fool the classifier once, it should be as a result of its biometric is extremely near that of the first user. Spherical (or one transition) will be portrayed by the real number



Detection chance of our continuous authentication theme as a operate of the quantity of biometric acquisitions performed (rounds), for designated values of ↵ and .Handling False Negatives False negatives visit incorrectly detective work the presence of A human, i.e., once the first user continues to be at the terminal. in an exceedingly state of affairs wherever

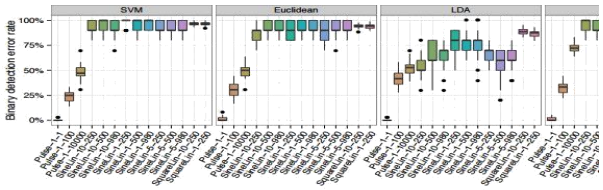
biometric identification is employed as a further layer of security throughout the authentication procedure, this drawback will be managed just by restarting the login procedure, if the first try fails. In an exceedingly continuous authentication system wherever one detection event may cause the system to lock up, false negatives need to be treated in an exceedingly a lot of organized manner. a method of handling false negatives in an exceedingly continuous authentication system, is to specify a policy that permits a precise range of human detection events each n-th spherical, while not taking any action. as an example, permitting one human detection event each one hundred rounds corresponds to a false negative rate of a hundred and twenty fifth.

An alternative choice is to mix the continual authentication mechanism with a less easy biometric to upset ambiguous detection events. as an example, when some human detection events, the user is asked to confirm its identity by swiping a thumb on AN adjacent fingerprint scanner. While not pulse-response the user would have to do that every ten seconds close to, which might render the system quite unusable. However, combined with our continuous authentication system, such confirmation may ought to occur a lot of less oftentimes. Finally it's doable to bit by bit work up the severity of actions taken by the continual authentication method, anytime AN human detection event happens. For the first time, displaying a warning can be the foremost applicable action. If detection re-occurs, a lot of and a lot of severe actions will be taken. it's most unlikely, with a fairly low false negative rate, to possess multiple consecutive human detection events if the first user continues to be at the terminal.

6. Biometric acquisition system:

Style during this section, we tend to describe choices and parameters that went into the look of our final classifier. We tend to conducted many experiments throughout to check completely different signal sorts, voltage levels, and frequencies. we tend to still experiment with completely different signal sorts and it seems that, contrary to our initial assumption, single pulse signals have significantly higher distinctive power. distribution denoted by the box plots themselves area unit the results of the classifiers achieved by five times 5-fold cross-validation. we tend to show the box plots instead of simply the mean to obviously show the variance in performance for every classifier. we tend to see that the slender pulse signal outperforms each alternative signal sort by a noteworthy margin. we tend to get consistent error rates near zero for a pulse signal of one V and a dimension of one hundred nanoseconds. Wider pulse signals additionally provide good results however the standard of the result looks to decrease with the dimension of the heartbeat. For the

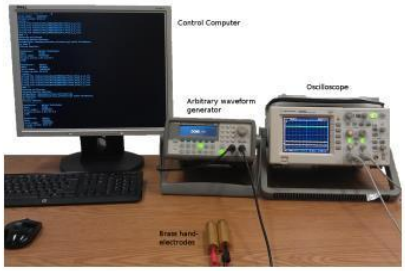
circular function and sq. wave sweeps the results vary significantly with the selection of classifier. Using LDA, some circular function sweeps look attention-grabbing however obscurity close to pretty much as good because the slender pulse signal. Signal Voltage There area unit many factors besides the distinctive power of the ensuing biometric, to contemplate once selecting voltage levels. it's vital that the users of our system don't expertise any discomfort once their biometric data is captured. that needs the voltages to be fairly low. we tend to take a look at 3 completely different voltage levels for all signal types: one, five and ten volts peek-to-peek (Vpp geometrician distance to the centre of mass of every class. Binary detection error rate. Box plots of the binary detection error rate for four completely different classifiers. The distribution shown by every box plot is that the results of applying stratified 5-fold cross-validation to the info set five times in an exceedingly row. we tend to take a look at many completely different signal sorts, voltage levels and frequencies for every classifier. we tend to see that slender pulse signals area unit systematically activity well.



Classifier is conceptually terribly straightforward however still offers fairly sensible results. Mahalanobis Distance (MH) instead of presumptuous uniform and orthogonal dispersion among the frequency parts (as within the geometrician categorizer) the variance matrix for every class is taken under consideration within the distance calculation. this permits for a distance metric that's proportional to the form of the category (in n dimensional feature space). The performance of this classifier didn't take issue significantly from the geometrician, suggesting that the form of every category isn't significantly skew. Support Vector Machine (SVM) for every combine of teams we tend to train one binary classifier(one-against-one).The final prediction is found by voting. The inverse kernel width for the Radial Basis kernel is decided by the zero.1 and 0.9 quantile of the pairwise geometrician distance between the samples. This classifier offers systematically sensible results and is our final alternative of classifier. Linear Discriminant Analysis (LDA) LDA seeks to scale back the dimensionality of the input data while preserving as much of the category distinctive power as doable. Our LDA classifier performs the linear analysis on all the categories in our information, then compares the position of recent samples within the ensuing lower dimension feature area. The performance of this classifier degrades a lot of graciously than several of the opposite strategies however ultimately it didn't prove as powerful because the SVM

technique. K Nearest Neighbor (Knn) we tend to tested the k nearest neighbors classifier for k =1and k =3, mistreatment geometrician distance. it's a straightforward classifier that usually works o.k. in apply. In our case although the performance of Knn was still not pretty much as good as SVMs.

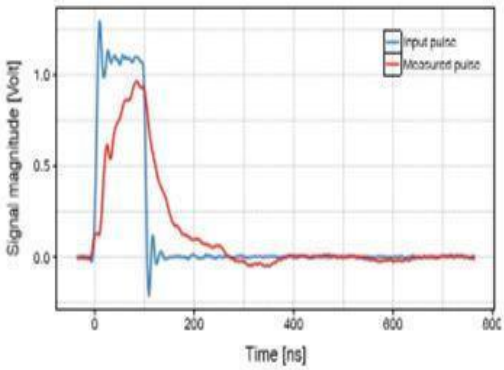
7. Experiments: During this section we'll describe our experimental setup and gift the results of our experiments with our final classifier



Our proof-of-concept mensuration setup. The take a look at subject is holding the 2 brass hand electrodes and also the pulse signal is generated by AN Agilent 33220A (20 MHz) capricious wave generator. The receiver is AN Agilent DSO3062A (60 MHz), one GSa/s digital storage electronic equipment.

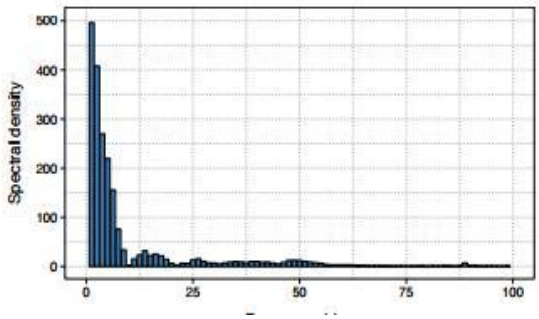
The design choices and motivations behind ourfinal classifier area unit represented intimately in Section VI. Any names from take a look at persons showing during this section's figures are anonymized through pseudonyms in such the simplest way that we might find yourself with sampling conditions as various as doable, for every user. The interval between measurements sessions with constant user varied between some hours up to many weeks. This was wiped out order to do to eliminate any impact that Signal magnitude [Volt]

Input pulse Measured pulse



The input and output wave. One mensuration consists of 4000 samples with a sample rate of five hundred MSa/s. it's clear that the measured pulse has been modified by passing through the user. Twenty five fifty seventy five one hundred Frequency bins

Spectral density



The raw FFT knowledge of the measured pulse, extracted from our mensuration setup. The info consists of the first one hundred frequency bins of the measured wave. Sampling at a specific time of day may need on our results, i.e., that our biometric would stay a lot of or less permanent over time, and across completely different periods of the day. Feature Extraction the info we tend to extract from our mensuration setup is within the style of a 4000 sample time-series describing the voltage variation as seen by the electronic equipment. Figure seven shows the input pulse sent by the wave generator and also the pulse measured by the electronic equipment. The time series measurements are converted to the frequency domain mistreatment FFT and also the first one hundred frequency bins of the FFT knowledge is employed for classification. 90 ninety two ninety four ninety six ninety eight one hundred ninety ninety two ninety four ninety six ninety eight one hundred Threshold [%] Sensitivity (TPR) The results for our authentication classifier supported the one knowledge set.

We tend to obtained actuality positive rate by activity five times 5-fold cross-validation for every take a look at subject. The xaxis describes the discrimination threshold for assignment the classifier's prediction output to a positiveor a negative. Results we tend to gift 2 com pletely different classifiers, one for authentication and one for identification. The authentication classifier relies an unknown person and also the requested person's hold on biometric template. The identification classifier, additionally supported SVM, verifies a 1:n match between a sample from a proverbial person against all the samples in an exceedingly information. Our identification classifier could be a closed set classifier on support vector machines (SVM) and solves the matter of corroborative a 1:1 match between a sample kind mythical creature curves for our authentication classifier supported unseen take a look at knowledge. We tend to show results for 3 completely different classification strategies. The dotted lines area unit for the results on the one knowledge set, the solid lines area unit over time.

8. Conclusion: We've projected a brand new biometric supported the human body's response to an electrical sq. pulse

signal. we tend to used our new pulse-response biometric as a further authentication mechanism in an exceedingly PIN entry system, enhancing the safety of the PIN entry mechanism while not adding further inconvenience for the user. we tend to additionally applied our new pulse-response biometric to the problem of continuous authentication. We design edam continuous authentication mechanism on a secure terminal, guaranteeing that the user that started the session continued to be the person physically at the keyboard. We tend to showed through experiments on our proof-of-concept paradigm system, that every organic structure exhibits a singular response to an indication pulse applied at the palm of 1 hand, and measured at the palm of the opposite. mistreatment our paradigm setup we tend to wherever able to determine users with high chance in an exceedingly matter of seconds. This identification mechanism integrates o.k. with alternative well established strategies, e.g., PIN entry, to provide a extremely reliable further layer of security, either on an eternal basis or at login time.

References:

1. V. Biometric. (2009, Feb.) How to make the fake fingerprints (by VIRDI). Last accessed 03.08.2013 A. Boehm, D. Chen, M. Frank, D. Huang, C. Kuo, T. Lolic, I. Martinovic, and D. Song, "Safe: Secure authentication with face and eyes," in In Proceedings of International Conference on Security and Privacy in Mobile Information and Communication Systems, Jun. 2013.
2. N. Clarke and S. Furnell, "Advanced userauthentication for mobile Devices," Computers & Security, vol. 26, no. 2, pp. 109 – 119, 2007.
3. C. Cornelius, J. Sorbet, R. Peterson, J. Skinner, R. Halter, and D. Katz, "Who wears me? bio impedance as a passive biometric," in Proceedings of the USENIX Workshop on Health Security and Privacy, August 2012.
4. N. S. . T. Council, "Biometrics frequently asked questions," 2006.
5. M. Frank, R. Bidet, E. Ma, I. Martinovic, and D. Song,"Touchalytics: On the applicability of touchscreen input as a behavioral biometric for Continuous authentication," Information Forensics and Security, IEEE Transactions on, vol. 8, no. 1, pp. 136 –148, 1 2013.
6. J. Globally, A. Ross, M. Gomez-Barrera, J. Fierrez, and J. Ortega-Garcia, "From the iris code to the iris: A new vulnerability of iris recognition systems," in White paper for Black Hat USA 2012, Feb. 2012, last accessed 03.08.2013.