Computer and Information Science; Vol. 8, No. 3; 2015
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Authentication Systems: Principles and Threats

Sarah N. Abdulkader [1], Ayman Atia [1] & Mostafa-Sami M. Mostafa [1]

[1] HCI-LAB, Department of Computer Science, Faculty of Computers and Information, Helwan University, Cairo, Egypt

Correspondence: Sarah N. Abdulkader, HCI-LAB, Department of Computer Science, Faculty of Computers and Information, Helwan University, Cairo, Egypt. E-mail: nabil.sarah@gmail.com

Received: April 23, 2015 Accepted: May 25, 2015 Online Published: July 25, 2015

doi:10.5539/cis.v8n3p155 URL: http://dx.doi.org/10.5539/cis.v8n3p155

Abstract

Identity manipulation is considered a serious security issue that has been enlarged with the spread of automated systems that could be accessed either locally or remotely. Availability, integrity, and confidentiality represent the basic requirements that should be granted for successful authentication systems. Personality verification has taken multiple forms depending on different possession types. They are divided into knowledge based, token based, and biometric based authentication. The permanent ownership to the human being has increased the chances of deploying biometrics based authentication in highly secure systems. It includes capturing the biological traits, which are physiological or behavioral, extracting the important features and comparing them to the previously stored features that belong to the claimed user. Various kinds of attacks aim to take down the basic requirements at multiple points. This paper describes different types of authentication along with their vulnerable points and threatening attacks. Then it provides more details about the biometric system structure as well as examples of distinguishing biological characteristics, organized by their locations. It shows the performance results of various biometric systems along with the deployed algorithms for different components.

Keywords: authentication features, authentication systems, biometric authentication structure, biometrics validity, security threats

1. Introduction

Nowadays, Security of computer systems is facing a lot of threats and difficulties mainly with the technological aspects and remote access. It has been found that ensuring confidential access to only authorized users and protecting the privacy of their personal and transactional information might limit the influence of the confronted attacks.

Authentication systems are supposed to meet three basic requirements, called availability, integrity, and confidentiality, against various attacks (Hausawi, Allen, & Bahr, 2014). The first requirement is concerned with the availability of system resources to legitimate users. Compromising this requirement is the main target for denial of service attacks. They aim at preventing genuine users from accessing their resources. On the other hand, system's integrity, which represents the second requirement, ensures linking the authorized users to their actions. So it implies defeating the intrusion of an imposter and denying his request to deal with system resources as well as overcoming the threat formed by insider users like insider repudiation attacks. This kind of attacks allows corrupted users to claim the irresponsibility of a malicious action. The final requirement is to guarantee the confidentiality and user's privacy. Function creep threats are targeting this requirement, allowing the stealing of user authenticating features to acquire control of another system or resource (Matyas & Riha, 2010).

The main contribution of this paper is to describe different types of authentication systems along with their vulnerable points and threatening attacks. It gives more details about the biometric system structure, provides examples of distinguishing biological characteristics, and evaluates them according to the common biometrics validity factors and the market's point of view. It also summarizes the performance results of various biometric systems along with the deployed algorithms for different components.

Various types of authentication systems have been developed to protect user identity and system resources against different types of attacks. The deployed authentication is determined by the needs, resources, priorities, and environmental surroundings. There are three main approaches that outline the authentication systems nature. They rely on the possession of knowledge, object, or biometrics as described in the following sections.

1.1 Knowledge Based Authentication

It is an authentication approach where the user is verified after proving the ownership of certain information. The supplied knowledge can take the form of confidentially exchanged passwords or pieces of information, called factoids. Factoids can be described as personal or non-personal, static or dynamic (He, Luo, & Choi, 2007). This approach has gone under different types of attacks that depend on password guessing, user observation or impersonation as informed by (Jesudoss & Subramaniam, 2014; Raza, Iqbal, Sharif, & Haider, 2012). Guessing the password has been part of brute force, and dictionary attacks (Mathew & Thomas, 2013). In a brute force attack, the intruder tries all combinations of characters that constitute the used language. Despite its certain results, it is considered time consuming to search all the possibilities. Thus increasing the length of the utilized password has been suggested as a solution to reduce the possibility of being attacked. This solution raises memorability issues and causing some users to lower their guard and write down their password instead of keeping it secretly in mind. Another way to conquer password via navigating different combinations has been produced in the dictionary attack. It only goes through the most common words rather than trying all possibilities.

Observing what the user writes or sends has been the base for several kinds of attacks like shoulder surfing (Chakraborty & Mondal, 2014), video recording (Shi & Gu, 2012), and keyloggers (Patel et al., 2012). Shoulder surfing and video recording aim at monitoring the user while he enters the password. The attack takes place either locally as in shoulder surfing or remotely as in video recording. Keyloggers, also called key sniffers, are often software programs responsible for sending user's activities and keystrokes to the attacker helping him to login as the corresponding victim.

Spying and intervention through an ongoing communication between two parties and impersonating one or both of them to the other has been performed in Eavesdropping, Man-in-the-Middle, Replay, and Phishing Attacks. Eavesdropping involves spying on the running conversation for later use. On the other hand, Man-in-the-Middle attacker impersonates both parties to each other and takes all roles in the active transaction. Replay attack is a form of eavesdropping that utilizes the overheard identity proof of the user in later transactions. Another way for identity stealing happens in phishing attack where the attacker masquerade as a website that requests user's authentication information. (Sahu, Dalai, & Jena, 2014)

1.2 Token Based Authentication

It is another approach of authentication that verifies the identity based on the ownership of certain objects like a bank credit card. It faces several issues regarding the need for special readers and the stealing of the verifying tokens (Ma & Feng, 2011). As demonstrated in (Panjwani, Naldurg, & Bhaskar, 2010), mobile devices have been registered as a valid token in banking transactions.

Securing or checking the identity in the world of "Internet Of Things" (IOT) (Friese, Heuer, & Kong, 2014; Pokric, Krco, & Pokric, 2014) have acquired the deployment of Radio Frequency Identification (RFID) tags as verifying tokens (Bertoncini, Rudd, Nousain, & Hinders, 2012). They are devices attached to access cards, badges, contactless credit cards, and e-passports. They are threatened by eavesdropping, unauthorized reading, owner tracking, and cloning (Saxena, Uddin, Voris, & Asokan, 2011). RFID tags are combined with One Time Password (OTP) in (C.-H. Huang & Huang, 2013) to overcome some security vulnerabilities like dictionary, replay, eavesdropping and tags forgery attacks. Challenge-response technique is also used for authenticating RFID tags, but it's considered a time consuming process especially in a high-volume supply chain system. A simple tag group authentication method has been proposed in (Leng, Hancke, Mayes, & Markantonakis, 2012) verifying the completeness and pureness of existing tags. Small amount of personal RFID tags is authenticated through the integration with the user owned mobile device as presented in (Saxena et al., 2011).

Another recent approach for token based authentication has invested the widespread and permanent use of mobile phones. In (Nseir, Hirzallah, & Aqel, 2013), they are used for authenticating ongoing bank transactions and provide mobile payment services (De, Dey, Mankar, & Mukherjea, 2013). Quick Response (QR) Code described in (Mayrhofer, Fuß, & Ion, 2013), as 2D barcode information captured by the camera installed in a mobile phone, combines both knowledge and object possession. It is used as electronic ticket as suggested in (Finzgar & Trebar, 2011). It describes the role played by mobile based ticket in releasing the transport companies from the need to smart cards and the related infrastructure. This security advance gives a great defense against various types of attacks as brute force, man-in-the-middle, and keyboard hacking attacks (Y. G. Kim & Jun, 2011). The location services offered by mobile phones have also contributed in the authentication process (S.-H. Kim, Choi, Jin, & Lee, 2013; Zhang, Kondoro, & Muftic, 2012). It could provide the continuous identification and authentication and forces the remote threats to be connected to physical locations as claimed in (Choi &

Zage, 2012).

1.3 Biometrics Based Authentication

The need for verifying attributes that cannot be overtaken by information sharing or token stealing has lead to the use of human physical traits or behavioral characteristics to prove the claimed identity (Kataria, Adhyaru, Sharma, & Zaveri, 2013). Physical traits are the descriptors of the body shape. They are found in hand geometry, palm print, face, fingerprint, iris, or retina. Behavioral characteristics, on the other hand, determine the person's behavioral attributes like typing rhythm, hand gestures, written signatures and voice (Ratha, Connell, & Bolle, 2001). Another advance in behavioral biometrics is the inclusion of voltage changes in biological system associated with some ongoing activities. It is called Electrophysiology. It is the study of the electrical properties of biological cells and tissues. There are several particular electrophysiological readings that show great opportunity to be used as biometrics. They have specific names, referring to the origin of the bioelectrical signals like Electrocardiography (ECG) for the heart, Electroencephalography (EEG) for the brain, Electrocorticography (ECoG) for the cerebral cortex, Electromyography (EMG) for the muscles, and Electrooculography (EOG) for the eyes.

2. Biometric System Structure

The involvement of human physiological or behavioral traits in the authentication process requires various phases to be deployed after training the users to work with the system as shown in figure 1(Veldhuis, 2008). Enrollment or calibration phase is responsible for storing the distinguishing information or template from each person in a database. It records and collects the biometric data from specific biometric-related sensors in the acquisition component. As these signals are subject to noise and attenuation, a preprocessing component is required to increase the signal to noise ratio. The resultant signal usually contains a vast amount of details. The system should decrease the details to be stored or checked, for efficient identity storage and matching decision. Thus, it uses the feature extraction component to take out the most discriminating features of the supplied signals. The features are then stored in the reference database which contains the data or the template to be used in the verification phase.

After enrollment, legitimate users get access to their resources or roles after successfully passing the verification phase. This phase takes as an input the claimed identity and the biometric sensor data of the subject to be authenticated. The claimed identity is then used as an index to the previously constructed database. The biometric data gathered, from the user requesting access, goes through the preprocessing and feature extraction components as in the enrollment phase. Then, classification component matches the information of the claimed identity and the features of the current subject in order to accept or deny this claim.

3. Biometric System Vulnerability Points

Ratha et al. (Ratha et al., 2001) have listed the vulnerability points attached to the biometric system according to the previously described structure in figure 1. At the location A the input of the acquisition component can be altered by the attacker who provides the sensors with formerly generated biometric data. The biometric raw data could be changed with previously stored or intercepted values at the link connecting acquisition and preprocessing components at the location B. Biometric features can be invaded by either fake extractor software that falsely took the place of the original one, at location C, or replacing the resultant features at location D. Locations E and F could witness template hacking either in their storing place or in their way for the checking process. Matcher or classifier component could be subject for software modification or final decision substitution at locations G and H respectively. These security breaches are categorized, according to (Jain, Ross, & Nandakumar, 2011), into attacks related to the user interface, attacks on modules, on the interconnection between modules and, on template database.

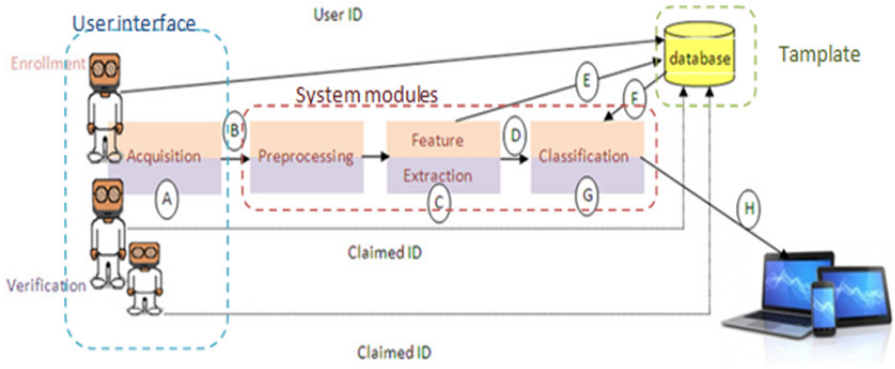

Figure 1. Biometric system overview

Vulnerability points A: at user interface, B: at the link connecting acquisition and preprocessing components, C: at feature extraction module, D: at the link connecting feature extraction and classification modules, E: at the storing database, F: at the template retrieving link, G: at the classification module, H:at the link delivering decision to its final destination.

3.1 Attacks at the User Interface

They are impersonation, obfuscation, or spoofing. The impersonation refers to intruding the system and claiming the identity of a legitimate user while obfuscation is a method for personality hiding and masquerading system's integrity. Spoofing, on the other hand, is to fool the system with artificial traits and gain undeserved access. Liveness detection could overcome the spoofing threat. It works by detecting other physiological or involuntary behavioral signs of life generated from an individual like checking perspiration and blood pressure (Sébastien Marcel, Nixon, & Li, 2014). Challenge-response technique, which depends on measuring either voluntary or involuntary response to the presented stimulation, as well as multimodal authentication contribute in exposing the user interface attacks as reported in (Galbally, Marcel, & Fierrez, 2014).

3.2 Attacks on the Template Database

Biometric data stored in template database could be exposed to modification or retrieval. Adversary attacks could make changes in the database to acquire access or have control over protected resources. They could also prevent authorized users from having their access rights. The illegitimate retrieval of biometric template is known as security leakage. Leakage can cause serious troubles as it does not only provide access to unauthorized people, but also violates the data confidentiality requirement of a biometric system. Once the biometric data is stolen or spoofed, it cannot be recovered or substituted as with other authentication systems.

Various techniques have been suggested to secure the biometric template like cancelable biometrics (Ratha et al., 2001) and fractional biometrics (Bayly, Castro, Arakala, Jeffers, & Horadam, 2010). Protection via cancelable biometrics involves performing an intentional, repeatable distortion of the received biometric signal based on a specific transform. On the other hand, fractional biometrics technique masks a fraction of biometric data before submission.

3.3 Attacks on System Modules and the Interconnections Between Modules

Attacks on system modules involve modification of the internal components. They can take place at the preprocessing, feature extraction, matching and decision modules. One of them is for the malicious software to pretend to be one of the modules and send the output that belongs to the adversary to consequent modules like Trojan horse attack.(Connell, Ratha, Gentile, & Bolle, 2013; Xi, Ahmad, Han, & Hu, 2011)

On the other hand, attacks on the interconnections between modules threat the privacy and data integrity of the communication channel like man-in-the-middle and replay attacks (Jain & Nandakumar, 2012). The hill-climbing attack presents a security breach that affects the paths from sensor to feature extractor and from feature extractor to matcher. It aims at reaching the score needed to get an affirmative identity check while subsequently modifying the existing biometric sample or feature set (Roberts, 2007). The transition from one fake generated output to another is controlled by raising the matching score that expresses the relation strength between the supplied and stored biometric data. In order to succeed, this threat should be able to provide the system with raw biometric sample data or features directly. It also should obtain the associated score. It is

considered the most dangerous threat. The main problem with hill-climbing attack is the huge amount of damage it can create. It does not only get passed through the system and affects is integrity, but it also compromises the user identity in any authentication system that examine the same biometric trait.

The trusted biometric system as highlighted in (Breebaart, Yang, Buhan-Dulman, & Busch, 2009) presents a solution for defeating those attacks. It holds the modules together in the same location or logically connected via mutual authentication, secure code execution practices or specialized tamper-resistant hardware.

4. Biometric Authentication Features

Various biometric authentication techniques are related to different parts of the human body like hand, head, and voice generating system as shown in figure 2. Human hand does not only contain unique geometrical features, but also other attributes like fingerprints, palm print, and palm vein network. Besides, Hand activities like gestures, keystrokes, mouse related movements, and written signatures are used to confirm the identity of human being through the analyzing the associated behaviors. Head contains features of face and brain parts. Face as well includes eyes with their unique iris and retina.

4.1 Hand Features

This authentication takes into consideration the shape and geometrical details of the whole hand (Amayeh, Bebis, Erol, & Nicolescu, 2006). Length and width of the fingers, the diameter of the palm and the perimeter are examples of these geometric features. The angle of the tip finger can be also a distinctive trait as demonstrated by (W. Y. Chen, Kuo, & Chung, 2013). Despite the advantage of simplicity, ease of use, and inexpensiveness, hand geometry measures are not identifying over a large population. The recording of features is also affected by some diseases like arthritis or objects that change the shape of the hand like jewelry. Some systems rely only on few fingers taking benefits of smaller acquisition devices. Identity confirmation can be done covertly via secret imaging for hand specifications.

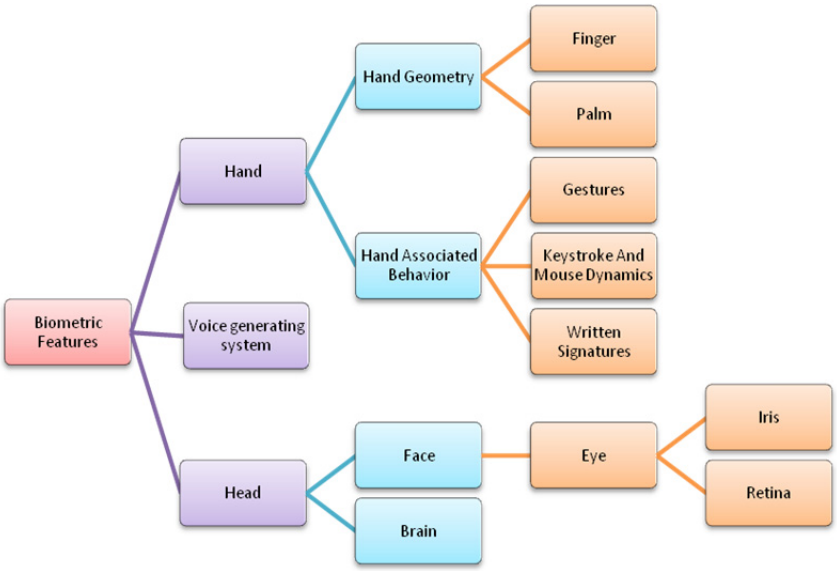

Figure 2. Biometric features

4.1.1 Fingerprint Features

It represents the most commonly used biometric in verifying user's identity. The distinction power provided by fingerprints does not only appear between different human beings, even identical twins, but also between fingers of the same person. The shape and details of ridges and valleys spread over fingertips constitute the acquired fingerprint where the ridge ending and bifurcation provide prominent features (Kataria et al., 2013). Fingerprints are collected as a 2D image that will be further processed by the authentication system. The fingerprint acquisition process does not always imply the user cooperation or awareness. People leave about 25 clear prints on average as claimed by (Matyas & Riha, 2010).

Fingerprint obfuscation and impersonation are examples of presentation threats that attack the fingerprint authentication system at the sensor level. Changing the structure of ridges can fool the verification process and increase its false rejection rate. It could take place with burning, cutting, abrading, or simply removing a portion of the skin from the fingertip. Artificial fingerprints are serving both obfuscation and impersonation. The

spoofing, as implied in (Marasco & Ross, 2014), can use different techniques like direct mold and Latent fingerprints.

The involvement of different feature types is explored for defeating the acquisition attacks. They include static and dynamic features. Static features involve the pore locations, individual pore spacing, and skin texture. Perspiration and ridge distortion can be detected in the dynamic behavior over a certain period of time. (Topcu, Kayaoglu, Yildirim, & Uludag, 2012) have used not only fingertips for authentication, but they also have incorporated non-distal phalanges in their verification system. They have found that the upper phalanx gives higher performance than the other phalanges. It achieves GAR of 98.9%, 91.4%, 75.0% at 0.1% FAR for distal phalanx, middle and bottom authentication respectively. In (H. Ravi & Sivanath, 2013), a touchless fingerprint authentication has been proposed with a webcam as an acquiring device. It eliminates the need for multiple touching of a common device limiting touching-transfer diseases and provide distant authentication. It attains an accuracy of 93.63%. While in (Alzahrani & Boult, 2014), Vaulted Fingerprint Verification protocol has been used to verify individuals remotely and conserve their privacy at the same time. It performs Equal Error Rate (EER) of about 7.5%. It attains comparable results to other discussed systems as shown in table 1.

Table 1. Fingerprint based verification systems

	Feature Extraction	Matching/Classification	Results		
(Alzahrani & Boult, 2014)	Minutiae triangles (NBIS's MINDTCT)	VFV	Equal Error Rate (EER) ~7.5%.		
(H. Ravi & Sivanath, 2013)	Minutiae extraction	Euclidean distance	Accuracy= 93.63%		
(Topcu et al., 2012) It uses NBIS commercial software	Minutiae extraction (NBIS's MINDTCT)	NBIS's BOZORTH3	Distal phalanx GAR=98.9%	Middle phalanx GAR=91.4%	Bottom phalanx GAR=75.0%

4.1.2 Palm Features

Palm contains three basic types of features for palm print authentication. They include principle lines, wrinkles, and ridges (Ray, 2013, X. Wu, Zhang, & Wang, 2006). The geometric features that describe palm shape can also cooperate as distinctive attributes for persons. The recording devices for palm print are more expensive than their finger counterparts, but the scanning process could also lead to a covert authentication.

Palm authentication starts with the 2-D image of the region of interest collected by the appropriate device. In (Kumar, Hanmandlu, Madasu, & Vasikarla, 2011), the authors have designed a low cost device for capturing the palm print images. The device accepts user's hand at any orientation unconstrained by any pegs or other such devices. It reaches an EER of 1.2%.

Another distinctive feature found in human palm is the physical structure of blood vessels network under the skin. The palm vein pattern contains a huge number of vessels. Their positions are the same during an individual's life. The verification process is not affected by the temperature, humidity or the surface wounds of the skin (Al-Juboori, Wu, & Zhao, 2013). Acquiring palm vein structure without the knowledge of an individual involves more challenging efforts (Zhou & Kumar, 2011). It preserves a low error rate with the false rejection rate (FRR) of 0.01%, and a false acceptance rate (FAR) of 0.00008% or lower (Watanabe, 2008), according to Fujitsu research as revealed in (Watanabe, Endoh, Shiohara, & Sasaki, 2005). It is acquired using infrared technology, thus the vessels containing the deoxidized hemoglobin are visible as a series of dark lines (Watanabe et al., 2005). An example of a palm vein authentication system has been proposed in (Al-Juboori et al., 2013). It employs Gaussian-Second-Derivative, Gabor Fisher Vein Feature (GFVF), and Cosine Distance method algorithms for preprocessing, feature extraction, and feature matching respectively, achieving EER of 0.0333%.

The robustness of palm vein features as intrinsic, biometric claimed by (Yuan & Tang, 2011) , has been defeated by the study in (Tome & Marcel, 2015). It has shown that the vulnerability of palm vein authentication to spoofing attacks via printed vein structure images of genuine users has increased FAR of the corresponding system to 65%.

In (Cai & Hu, 2010), the fusion of the images from multi-sensor imaging system has been investigated in order

to generate the distinguishing feature set from both palm print and palm vein. Jen-Chun Lee in (Lee, 2012) has examined the encoding of palm vein features into bit string representation, during the template construction needed for the identification task. The system has decreased the size required for palm vein features to 2520 bits. It has accomplished a recognition rate with EER that equals to 0.4%. As shown in table 2, most systems have achieved high recognition rate with EER <0.5%.

Table 2. Palm based verification systems

	Feature Extraction	Matching/Classification	Results	
(Lee, 2012)	Gabor filter	normalized hamming distance based similarity	EER=0.4%	
(Zhou & Kumar, 2011)	Neighborhood Matching Radon Transform(NMRT)	Hamming distance	POLYU DATABASE EER=0.03%	CASIA DATABASE EER=0.51%
For three training samples	Hessian-Phase-Based Feature Extraction		POLYU DATABASE EER=0.57%	CASIA DATABASE EER=1.44%
(Kumar et al., 2011)	Band Limited Phase Only Correlation (BLPOC)	Maxima of Band Limited Phase Only Correlation (MBLPOC)	EER=1.20%	
	Gabor filter	hamming distance	EER=3.1%	
(Cai & Hu, 2010)	dual-tree complex wavelet transform (DTCWT)	Mutual Information Between non-processed and processed images	Visible=1.5006	Infrared=0.7675
	discrete wavelet transform (DWT)		Visible=1.4727	Infrared=0.7403
	shift invariant discrete wavelet transform (SIDWT)		Visible=1.4958	Infrared=0.7482
(Al-Juboori et al., 2013)	Gabor Fisher Vein Feature (GFVF)	Cosine Distance method	EER = 0.0333%	
(X. Wu et al., 2006)	a set of directional line detectors	Defined similarity measure	EER =0.4%	
	Sobel filter		EER =5%	
	2D Gabor filter		EER =0.6%	

4.1.3 Hand Behavioral Features

The involvement of the hand associated behavioral features has created various types of authentication schemes like hand gestures, keystroke dynamics, mouse related events, and written signature. It's highly preferable in some environments where continuous authentication is required or wearing gloves is mandatory (Aslan, Uhl, Meschtscherjakov, & Tscheligi, 2014).

1) Hand gestures

Hand gestures work to deliver non-verbal messages and certain emotions or thoughts. They are either performed on purpose or involuntary. They are used in controlling activities for various applications and smart environments as part of human computer interfaces. They can also be used for commanding touch-sensitive devices. Hand gestures have been invoked in user authentication (Clark & Lindqvist, 2014; Jeon, Oh, & Toh, 2012; Koong, Yang, & Tseng, 2014). They have been preferred by the contributing subjects because of its ease, pleasure, and excitement over typical text-based passwords. Clark & Lindqvist in (Clark & Lindqvist, 2014) have reported that mimic user gestures or covertly recording his login activities are examples of attacks at user interface facing hand gesture authentication systems.

Gesture authentication is categorized into two main classes touch screen or motion based. A touch screen authentication system has been developed in (Sae-Bae, Ahmed, Isbister, & Memon, 2012). Sae-Bae et al. have

achieved an accuracy of about 90%, where gestures of five fingers have been used. The feature set includes movement characteristics of the center of the palm and fingertips. They examined the use of single gesture achieving an EER that equals to 10% but it decreases to 5% when combining two different gestures. Then they extended their work in (Sae-Bae, Memon, Isbister, & Ahmed, 2014) to trace the performance over gaps of several days. It has been found that the performance is degraded noticeably over multiple sessions. EER has changed on an average basis from 10.68%, in case of a single session, to 21.87%, in case of multiple sessions. They also have shown that user defined gestures present better results than the supplied ones. The same conclusion has been confirmed in (Sherman et al., 2014) through the use of free-form gesture in the authentication system. In (Koong et al., 2014), the authors investigate the effect of the number of contributing fingers on the verification process. It has achieved True Acceptance Rate (TAR) of 85% for three fingers, 90% for four fingers, and 88% for five fingers.

Motion based gesture verification has been described in (Aslan et al., 2014). It has been able to overcome the finger oil issues related to the recording of the touch based authentication. The system accomplishes an EER that equals to 11.71% using a leap motion 3D controller for the motion acquisition process. While (Fong, Zhuang, & Fister, 2013) have utilized sign language, captured by an ordinary video camera, as hand gestures for biometric authentication system. They found that the system is able to verify individuals with maximum accuracy of 93.75%, assessing the feasibility of using gestures for authentication as well as for message communication. (Jeon et al., 2012) have used Kinect sensor in the verification system where fusing features that describe position, velocity, and acceleration has been deployed. It reaches an EER that equals to 0.87% versus an average EER that equals to 2.33% for using a single type of features. Table 3 shows that Dynamic Time Wrapping (DTW) can be used in various systems with acceptable results.

Table 3. Hand gesture verification systems

	Feature Extraction	Matching/Classification	Results		
(Sae-Bae et al., 2014)	DTW(Manhattan)		Single session =10.68%	Multiple sessions=21.87%	
(Jeon et al., 2012)	DTW		EER=0.87%		
(Koong et al., 2014)	the relative position, distance of fingertips, and area of each three fingers	Euclidean distance and thresholding	For 3 fingers TAR=85%	For 4 fingers TAR=90%	For 5 fingers TAR=88%
(Fong et al., 2013)	Correlation based Feature Selection	SVM	87.5%		
		neural network (perceptron)	93.75%		
(Sae-Bae et al., 2012)	DTW		single gestures EER=10%	double gestures EER=5%	
(Aslan et al., 2014).	DTW		EER = 11.71%		

2) Keystroke and Mouse dynamics

The keystroke typing behavior of individuals has a unique rhythm. Studying time periods needed for key press and between successive presses has been useful for user authentication (Bhatt & Santhanam, 2013). The time duration required for pressing the key is called hold time while the interval between consecutive keys is called delay time.

Authentication of keystroke behavior depends on either fixed text or free text. Static authentication uses fixed or

predetermined text for human verification. Free text, on the other hand, is involved in continuous authentication that prevents the attacker from presenting an authorized user in an ongoing session (Syed, Banerjee, & Cukic, 2014; Zhong, Deng, & Jain, 2012). (Syed et al., 2014) have used the variations in typing sequence as distinctive features in their authentication system. A new distance metric has been suggested and used in (Zhong et al., 2012) for keystroke based authentication systems. It assists decoupling correlated data, normalizing feature variations, and suppressing outliers. The system has achieved an equal error rate of 8.4%.

Measuring keystroke behavior can be done without user awareness or cooperation. It also does not need any special or modified devices to capture the typing characteristics. Various advantages have been offered by the keystroke behavior for verification purposes. It facilitates a cost effective, user friendly and continuous verification with a potential for high accuracy (Karnan, Akila, & Krishnaraj, 2011). However, some of the challenges facing keystroke dynamics authentication have been revealed in (Banerjee & Woodard, 2012). As with the behavioral biometrics, the typing dynamics can be greatly changed with time, emotional variations, concentration levels and health conditions. The variability of used languages and keyboard layouts could affect the reported accuracy results. They can lead to the degradation of the system's performance when matching stored template generated from different language or keyboard layout. The mixed usage of physical keyboard and their virtual counterparts should be also tested, especially with the growing use of smart phones, tablets and other touch screen devices. The typing on these devices involves either hunt-and-peck or all fingers.

As attacking the computer systems could only be a few clicks away, mouse related events can be used to authenticate human behavior. Various challenges have been addressed for verifying mouse actions. As pointed out by (Jorgensen & Yu, 2011), the amount of mouse data and time required for user authentication could affect the practicality of mouse dynamics especially for continuous verification. (Shen, Cai, Guan, Du, & Maxion, 2013) have consumed 11.8 seconds for fixed mouse operation while achieving error rates of 8.74% and 7.69% for FAR and FRR respectively. In (X. Chen, Xu, Xu, Yiu, & Shi, 2014; X. Chen, Shi, et al., 2014), Practical Authentication with Identity Tracking System (PAITS) has been developed. It can check and track the claimed identity in only 5 seconds with 2.86% for FRR and 4% for FAR thus saving user's time while preserving high authentication results as shown in table 4.

Table 4. Keystroke and Mouse dynamics based verification systems

	Feature Extraction	Matching/Classification	Results
(X. Chen, Xu, et al., 2014)	movement range, movement direction and speed, Distribution of angles between two successive moves	Probabilistic neural network (PNN)	FRR=2.86% FAR= 4%
(Shen et al., 2013)	DTW + PCA	SVM	HTER=8.35%
		Back Propagation Neural Network(BPNN)	HTER=12.5%
		KNN	HTER=15.1%
(Zhong et al., 2012)	the timing information of the key down/hold/up events and time latency information	Nearest Neighbor(new distance metric)+noise removal	EER=8.4%
		Nearest Neighbor(new distance metric)	EER=.087%

3) Written signatures

Handwritten signatures have been widely accepted verification method in most financial transactions or official communications. However, the large number of documents has burdened the manual signature based system, increasing its time consumption rate. Therefore, automated verification systems that rely on written signatures have been extensively studied (Sanmorino & Yazid, 2012). Different non-English languages like Chinese, Japanese, Arabic, and Persian have been included in multiple authentication systems as stated in (Pal, Blumenstein, & Pal, 2011). The attacks revealed in According to (Ballard, Lopresti, & Monrose, 2006) handwritten signatures are exposed to attacks at sensor level either synthesized handwriting or human skilled forgeries.

There are two categories for handwritten signature authentication, offline and online. Offline or static authentication involves scanning and digitizing the regular signature that resides on a piece of paper. Pushpalatha et al. have proposed an authentication system that achieved a total success rate of 93.4% (Pushpalatha, Gautam, Kumar, & others, 2014). In (H. Ahmed, Shukla, & Rai, 2014), an offline system has been developed with paying attention to time and memory saving issues while maintaining high performance results. It has accomplished an EER of 7.60% requiring between 1.5 to 4.2 seconds for system training per person.

Online or dynamic authentication captures the behavior related to the signing activity and uses it for identity confirmation. In (Tian, Qu, Xu, & Wang, 2013), the activity of password writing in 3D space has been captured using Kinect giving a 100% precision and a 77% recall on average. Malaysian handwritten signatures have been involved in an online verification reaching FAR of 7.4% and FRR of 6.4% (Iranmanesh et al., 2014). Handwritten authentication has been integrated into different systems as suggested in (Renuka, Suganya, & Kumar, 2014) that has proposed character recognition with a behavioral identity check. It has achieved an accuracy rate of 98%.

Table 5 shows the results associated with various used methods for feature extraction and matching components in signature based verification.

Table 5. Signature based verification systems

	Feature Extraction	Matching/Classification	Results
(H. Ahmed, Shukla, & Rai, 2014)	Discrete Radon Transform (DRT)	Dynamic Time Warping algorithm (DTW)	EER =7.60%,
(Iranmanesh et al., 2014)	PCA	ANN	FAR= 7.4% FRR = 6.4% EER=6.9%
(Pushpalatha, Gautam, Kumar, & others, 2014)	Contourlet transform and Texture features	HMM	TSR =93.4% HTER=9.12%
(Tian, Qu, Xu, & Wang, 2013)	Positions & Distance ,Velocity , Acceleration , Slope angle , Path angle , Log radius of curvature	DTW	Precision = 100% Recall = 70%

4.2 Voice Features

Voice is one of the old behavioral characteristics that usually apply for person recognition in everyday life through normal interactions. It has been used to recognize people via direct communication or distant phone conversations. Voice distictivity, as other behavioral traits, comes from the uniqueness of physiological attributes like vocal cords, size and shape of the throat and mouth. They do not suffer from major changes over time. Learned behavioral patterns reflected from the speaking style also contribute in distinguishing or verifying the speaker (Kataria et al., 2013). They face variability according to various circumstances like age, medical condition, and emotional state.

Machine based voice authentication or speaker verification can be text-dependent, text-prompted or text-independent. In text-dependent voice verification, the system is customized to a specific phrase for both enrollment and verification (Alarifi, Alkurtass, & Al-Salman, 2011). While in text-prompted systems, the user is

prompted to pronounce random words offered instantly by the system. However, the free choice of spoken sentences is allowed in text-independent voice authentication systems (Bellegarda & Silverman, 2014; Z. Wu et al., 2015).

Chakrabarty et al. have performed EER of 15.66% with an online text-independent verification system (Chakrabarty, Prasanna, & Das, 2013). The undetermined words have been also involved in voice identification in (Jose Albin, Nandhitha, & Emalda Roslin, 2014) accomplishing an average sensitivity of 68%. The system in (Baloul, Cherrier, & Rosenberger, 2012) has attempted to reduce the value of EER to 0.83% and raise the performance accuracy while retaining the verification time of 2.53 seconds. Then Brunet et al. in (Brunet et al., 2013) have employed the Android platform in a speaker identification system achieving an EER of 4.52%.

Languages, other than English, have been tested for this authentication method. Marathi voice based system in (Bansod, Dadhade, Kawathekar, & Kale, 2014) has performed a recognition rate of 88% on database PHASE-II. A database with various language speakers like Arabic speakers, Mandarin speakers, Russian speakers, and Spanish speakers is used for cross-lingual authentication in (J. Wang & Johnson, 2013). The system accomplishes an accuracy of 72.3%. The used algorithms shown in table 6 reveal the extensive use of Mel Frequency Cepstral Coefficients (MFCC) as distinctive features across various system configurations.

The user interface attacks related to voice based verification vary according to the used system. In case of text dependent system, the attacker could record the required sentence in a previously prepared conversational scenario with the victim either covertly or overtly. In text-independent system, any pronounced phrase would compromise a threat. While in text-prompted systems, the attacker has to model the user's utterance characteristics learned from different phrases spoken by the user (Matyas & Riha, 2010).

Table 6. Voice based verification systems

	Feature Extraction	Matching/Classification	Results
(Chakrabarty et al., 2013)	Mel Frequency Cepstral Coefficients (MFCC)	Gaussian Mixture Model-Universal Background Model (GMM-UBM)	EER=15.66 %.
(Jose Albin et al., 2014)	Discrete Meyer (Dmey)	Back Propagation Network (BPN)	sensitivity =68%
(Brunet et al., 2013)	MFCC	VQ (vector quantization)	EER = 4.52%
(Bansod et al., 2014)	MFCC	DTW	PHASE-I database RR= 85% PHASE-II database RR=88%
	Linear Prediction Coding (LPC)		PHASE-I RR=60% PHASE-II RR= 72%
(J. Wang & Johnson, 2013)	Residual Phase Cepstrum Coefficients (RPCC)	GMM-UBM	Accuracy=67.7%
	Glottal Flow Cepstrum Coefficients (GLFCC)		Accuracy=72.3%
	MFCC		Accuracy =71.2%
(Baloul et al., 2012)	MFCC	V Q	EER = 0.83%

4.3 Head Based Features

There are plenty of distinctive features that are located on the head either internally as the brain behavior or externally like the apparent face characteristics and expressions. The next subsections give more details about those features that are either physiological or behavioral.

4.3.1 Face Based Features

Faces are always used as a means for others to recognize the noticed individual. The position, shape and the distances between face components as eyes, eyebrows, nose, lips and chin that are distinctive to each human

being. Face-based automated authentication system utilizes cameras rather than human eyes to check the person's identity. The imaging can take place either covertly or overtly. These systems capture the facial images in 2D or 3D spaces. Three-dimensional space allows the recognition system to include the attributes of the face surface modeled by (G. B. Huang, Lee, & Learned-Miller, 2012; Taigman, Yang, Ranzato, & Wolf, 2014). The system in (Borg, Said, Ben Amor, & Ben Amar, 2011), has reached an EER of 1.6%.

Facial expressions as well as aging represent huge issues in recognition systems. The aging effect on the verification has been tested in (T. Wu, Turaga, & Chellappa, 2012) where the system has an EER of 23.6%. The influence of expressions is suppressed by 3D information fusion as suggested by (Belahcene, Chouchane, & Ouamane, 2014). It has accomplished a Recognition Rate (RR) of 81.30% using CASIA color database. Another trend for dealing with facial expressions is by invoking them in facial behaviometrics. Talking face video verification is handled in (Li & Narayanan, 2011). It has achieved an EER of 8.4%. The effect of spontaneous smile activity has been used in authentication (Zafeiriou & Pantic, 2011). The value of the resultant EER is 2.5%, which seems to provide a promising approach as shown in table 7.

Table 7. Face based verification systems

	Feature Extraction	Matching/Classification	Results
(Belahcene et al., 2014)	Gabor filter + Principal Component Analysis (PCA) + Enhanced Fisher linear discriminant Model (EFM)	support vector machine (SVM)	RR = 81.30%.
(Zafeiriou & Pantic, 2011)	Free Form Deformations (FFD)	PCA	EER= 6.3%
		LDA	EER= 2.5%.
(T. Wu et al., 2012)	affine-invariant shape landmarks	Proposed method Ling's method LRPCA	EER=23.6% EER=24.1% EER=32.1%
(G. B. Huang et al., 2012)	pixels intensity	local convolutional restricted Boltzmann machine (LCRBM)	85.38%
	Local Binary Patterns (LBP)	CRBM	84.85%
(Borg et al., 2011)	Iterative closest point (ICP) + facial curves shape analysis+ beta wavelet approximation	sum fusion product fusion	EER=1.6% EER=1.6%
(Taigman et al., 2014)	Pixel intensities	deep neural net	97.35%
(Li & Narayanan, 2011)	discrete cosine transform(DCT)-mod2xy	Joint Factor Analysis (JFA) + GMM-Sparse	EER=9.45%

1) Eye based features

Eye organ of the face can be used separately to confirm human's identity. Visible features of the eye gathered from scanning the iris as well as Inner vessel network pattern behind the retina contribute in the authentication of the claimed personality.

- Iris based features

Iris is the colored region apparent in the eye between the pupil and the sclera on either side. It controls the amount of light entering inside the organ by resizing the pupil diameter. Iris recording, until recently, requires the collaboration of the individual. But now a good quality camera and zoom lens can provide a sufficient recording quality even from mediate distances, allowing the image capturing to be done covertly.

The system in (Pillai, Patel, Chellappa, & Ratha, 2013) performs iris based identity confirmation using a database that includes images with errors either in the acquisition or preprocessing. It achieves a verification rate of 98.13%. FAR of above 98% has been reached for video based iris verification. Enhancing the performance of iris based authentication has gained the attention of a lot of researchers as reported in (Bowyer, Hollingsworth, & Flynn, 2013). Singh has suggested a noise removal method from the acquired iris images as well as authenticating only specific parts of the iris (Singh, 2014). It leads to 1.67% and 2.50% for FAR and FRR respectively for masked iris parts versus 0.83% and 5% for non-masked parts. While a new feature extraction method that uses 1D features has been proposed in (Liu, Liu, & Chen, 2014). The system has attained an overall performance of 99.35%. Different fusion techniques at decision level have been evaluated for iris based authentication in (Granger, Khreich, Sabourin, & Gorodnichy, 2012) revealing that the results could be enhanced when Iterative Boolean Combination technique is employed for fusing the scores based on calculated Euclidean distances from the vertical and horizontal Linear Discriminant Analysis (LDA) boundaries.

In (Connell et al., 2013), a method for fake iris detection has been proposed. It uses a structured light projection method to discover the existence of artificial items hiding the real iris. It has taken advantage of the fact that the projected stripes appear straight for naked iris or curved for non-transparent contact lens on the cornea. Another solution for presentation attacks that could be integrated in the system is presented in (Tomeo-Reyes & Chandran, 2013). It has combined different parts from various supplied samples to defeat different obfuscation threats. The results of applying various types of obfuscation threats like wearing glasses, obstructing eyelid, or deviating gaze are detailed in table 8. The assistance of fingerprint in the multimodal authentication system has been investigated to enhance the performance of iris recognition and authentication. In (Bharadi, Pandya, & Nemade, 2014), the iris and fingerprint recognition decisions have been merged achieving total classification accuracy of 79.8%, while the results of FAR that equals to 0% and FRR that equals to 5.71% have been reported in (Conti, Vitabile, Agnello, & Sorbello, 2013). Continuous iris authentication using an eye tracker has been offered by (Mock, Hoanca, Weaver, & Milton, 2012) overcoming the issues facing static authentication. It achieves an accuracy of 92.9%.

Table 8. Iris based verification system

	Feature Extraction	Matching/Classification	Results	
(Conti et al., 2013)	Gabor filter+ Log-Gabor for iris Core and delta points for fingerprint	Hamming Distance (HD) for fused features	FAR=0% FRR = 8.33%	
(Mock et al., 2012)	Density values in the Red channel	k-nearest neighbors (KNN) For K=9	Left Eye Accuracy=67.9% Manhattan=92.9%	Right eye Accuracy =82.1%
(Bharadi et al., 2014)	Hybrid wavelets	KNN For K=9	Hybrid wavelets type I CCR =76.1%	Hybrid wavelets type II CCR =79.8%
(Pillai et al., 2013)	Gabor fused features	Normalized Hamming distance	98.13%	
(Liu et al., 2014)	Sobel operator and 1-D wavelet transform	matching reconstructed signal	FAR=.01% FRR=.69% Acc=99.35%	
(Singh, 2014)	2D Gabor Wavelets	Hamming Distance (HD)	With masking FRR=2.5% FAR=1.67%	Without masking FRR=5% FAR=0.83%
(Tomeo-Reyes &	2D Gabor filters	Hamming Distance (HD)	Degradation type	FAR/FRR (%) Proposed(multi part&multiclass

Chandran, 2013)			ifier) FAR/FRR (%)
	Glasses	.75/2.13	.24/0
	Eyelid obstruction	4.02/8.01	1.07/0.15
	Gaze deviation	7.82/9.4	6.03/6

- Retina based features

The human eye in its posterior portion has a thin tissue composed of neural cells called retina. The network of blood vessels feeding it has a unique pattern for each person. The imaging of the individual's retina requires a full cooperation and concentration from the user being identified or authenticated making a covert recording an impossible process. The overt scanning also raises problems with user satisfaction. But, to the best of our knowledge, retina based verification faces no attacks regarding user interface. Some diseases could affect the retinal pattern, but typically the basic structure of the retina remains unchanged throughout the entire life of a human being.

Retina-based personal identification in (Akram, Tariq, & Khan, 2011) has been tested for images with severe eye diseases included in STARE database. It has witnessed a slight degradation than the results experienced when using healthy retinal images contained in DRIVE database. The system accomplishes a recognition rate of 95.06% for STARE database and 100% for DRIVE database. While in (Qamber, Waheed, & Akram, 2012) an overall individual recognition rate of 98.87% has been reached using their retinae.

Vessel breakages, short vessels and spurs could cause the formation of false features. According to (Fatima, Syed, & Akram, 2013), those features are removed using a windowing technique on the skeleton vascular pattern. It has achieved a reduction factor of 94.74% for raw images and 90.96% for processed images. The effect of various similarity measures in retinal authentication has been also studied as published in (Jeffers, Davis, & Horadam, 2012).

The time required for making the verification decision has been observed and measured in multiple retina-based authentication systems while maintaining high performance results. In (M. I. Ahmed, Awal, & Amin, 2012), the average time for identity check is 10.25 seconds. This system has worked with images in two color spaces RGB and YCbCr. RGB color space has accomplished an accuracy of 84.2%, while a result of 89.2% has been reached for YcbCr color space. Another system in (Condurache, Kotzerke, & Mertins, 2012) has claimed that a result equals to 94.64% of correct decisions, has been revealed in six seconds only.

From table 9, it seems that wavelets are widely used for feature extraction in retina based verification leading to adequate accuracy results.

Table 9. Retina based verification systems

	Feature Extraction	Matching/Classification	Results	
(Vora, Bharadi, & Kekre, 2012)	Haar Wavelet Energy feature vector	KNN	EER=7%	
	Kekre Wavelet Energy feature vector		EER=4%	
(Qamber et al., 2012)	Gabor wavelet + crossing number method	Mahalanobis distance	RR=98.87%	
(M. I. Ahmed et al., 2012)	semi-circular blood vessel segment	2-D Correlation Coefficient	RGB color space Accuracy =84.2%	YCbCr color space Accuracy =89.2%
(Akram et al.,	Gabor wavelet +		STARE	DRIVE

2011)	crossing number method		database Accuracy =95.06%	database Accuracy =100%
(Jeffers et al., 2012)	retina graph	seven scoring functions	EERs in the range 0.3%−1.3%	
(Condurache et al., 2012)	scale-invariant feature transform (SIFT) -log-covariance based point-cloud features	Sparse classification	Accuracy =94.64%	

4.3.2 Brain Based Features

Electroencephalography (EEG) is used, as part of Brain Computer Interface (BCI), to study the differences in brain voltage expressing the occurrence of motor or mental activities. The brain responses to certain common actions are used to verify the claimed identity even for people with various disabilities or to convey secret messages through the verification process as implied in (Su, Zhou, Feng, & Ma, 2012).

Several researches have investigated the use of brain signals in personal identification and verification systems for different motivating actions. It does not face any spoofing attacks at the user interface level, as far as we know. Visual evoked potential and graphical stimulation have been widely used in a variety of forms like employing face stimulation via either self-face or non-self-face images, as anticipated by Yeom and his colleagues in (Yeom, Suk, & Lee, 2013a, 2013b). They first have chosen the highly distinctive channels and time components related to each user. Then they utilize the averaged Event Related Potential (ERP) signals over multiple trials in order to compute the corresponding features. They have reached a mean accuracy of 86.1%. While (K. Ravi & Palaniappan, 2005) and (Zúquete, Quintela, & Cunha, 2010) have presented black and white pictures from Snodgrass and Vanderwart picture set to 70 individuals. Ravi has achieved an identification accuracy of 95.25% using 40 Hz EEG oscillations. While Zúquete et al. have been concerned with reducing the consumption of electrodes. The performance of two classifiers, K-NN and SVDD, has been compared and their best attained results for eight electrodes are 95.1% and 98.5% respectively.

(Ashby, Bhatia, Tenore, & Vogelstein, 2011) have utilized mental based actions like baseline measurement, limb movement, counting, and rotation to authenticate five subjects. It operates low cost EEG headset from Emotiv Company to collect signals generated from 14 channels, thus increasing the price-based collectability of the system. They have reached an average accuracy 98.78% using one-versus-all SVM classifier while discriminating five types of features. On the other hand, Hema and his colleagues (C. R. Hema, Paulraj, & Kaur, 2008) pay special attention to the uniqueness of reading and multiplication mental responses. They have extracted PSD features from EEG Beta waves and applied them to feed forward neural classifier. The performance of identifying six subjects has reached an average accuracy of 94.4% to 97.5% for different activities. PSD features of mental spelling and reading activities have been classified using feed forward neural networks in (C. Hema & Osman, 2010). The identification system has gained performance accuracy of 78.6% based on single trial analysis compared to 90.4% for multiple trials averaging.

(Sebastien Marcel & Millán, 2007) have involved the mental generation of words in person authentication. The first letter, chosen randomly, is the same across all subjects. They have proposed a statistical framework based on Gaussian Mixture Models and Maximum a Posteriori model adaptation on word generation as well as motor imagery EEG signal. It has resulted in HTER ranging from 6.6% to 20.5% for motor imagery versus 12.1% to 26.1% for word generation for various number of gaussians in the mixture in a single day.

As shown in table 10, PSD features are extensively employed in brain verification giving acceptable results.

Table 10. Brain based verification systems

	Feature Extraction	Matching/Classification	Results
(Zúquete et al., 2010)	Energy of differential signals with the Parseval's spectral power ratio	K-Nearest Neighbor(KNN)	Accuracy=95.1%
		Support Vector Data Description (SVDD)	Accuracy=98.5%
(Ashby et al.,	Autoregression	SVM	Accuracy=98.78%

2011)	(AR) + power spectral density (PSD) + total power in five frequency bands + interhemispheric power differences + interhemispheric linear complexity			
(C. R. Hema et al., 2008)	PSD	feed forward neural network	Accuracy ranges from 94.4% to 97.5%	
(C. Hema & Osman, 2010)	PSD	feed forward neural network	Single trial Accuracy=78.6%	Multiple trials Accuracy=90.4%
(Sebastien Marcel & Millán, 2007)	PSD	GMM	HTER ranges from 6.6% to 26.1%	

5. Biometrics Validity Factors

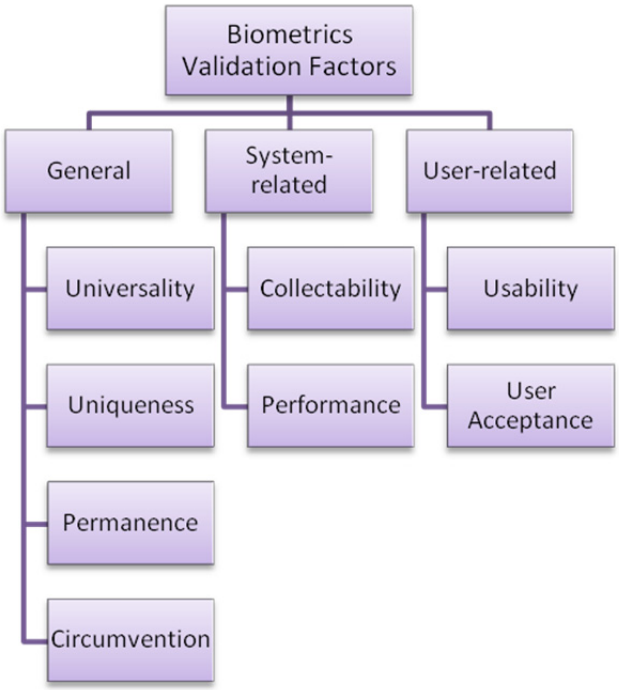

Figure 3. Biometrics Validation Factors

In order for human physical or behavioral traits to be authenticative, several factors should be checked to determine the effectiveness of a chosen verifying biometric (L. Wang, Geng, & Global, 2010). The validity factors, as shown in figure 3, can be categorized into general, system-related, and user-related factors. General factors include the essential characteristics of the authenticating trait like universality, uniqueness, and permanence. Universality verifies the existence of such trait in every human being, while uniqueness ensures its distinctiveness per individual. Permanence or constancy validates the time-invariance of the measured biological phenomena. Circumvention expresses the easiness of spoofing threat. The system-related factors guarantee the collectability and quantitative aspects along with the estimated system performance. Finally, user-related factors are concerned with the usability and user acceptance level.

Different features are validated against biometrics validity factors in (Kataria et al., 2013) with acceptance factor contains both user acceptance and ease of use as shown in table 11. Examples of some user interface threats are presented in table 12. Figure 4 represents the market share of authentication system for various features as

implied by International Biometric Group (IBG) in the interval 2007-2012 (Singla & Kumar, 2013). Although Fingerprint authentication is vulnerable to user interface attacks, it preserves a huge share in the biometric authentication market that exceeds the 50% limit for both offline and online fingerprint scanning. They also forecast that the market for healthcare will witness an extensive use of biometrics reaching $5 billion by 2020 for both overcoming the fraud issues facing the healthcare system in the US and continually keeping track of the state of the patient (King, 2015). Thus, it reflects a growing interest in authenticating vital signs like those provided by the heart or the brain.

Table 11. Biometrics validity factors for various features (Kataria et al., 2013) (H=High, M=Medium, L=Low)

Biometric trait	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptance	Circumvention
Finger print	M	H	H	M	H	M	M
Palm print	M	H	H	M	H	M	M
Hand Geometry	M	M	M	H	M	M	M
Palm vein	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
Retina	H	H	M	L	H	L	L
Face	H	L	M	H	L	H	H
Voice	M	L	L	M	L	H	H
Signature	L	L	L	H	L	H	H
Hand gestures	L	L	L	M	L	M	H
Mouse and keystrokes	L	L	L	M	L	M	M
EEG	H	H	M	M	L	L	L

Table 12. Examples of user interface threats

Biometric trait	Spoofing threats	Obfuscation threats
Finger print	Direct mold and Latent fingerprints. Covert recording	burning, cutting, abrading, removing a portion of the skin from the fingertip Artificial fingerprints
Palm print	Covert recording	burning, cutting, abrading, removing a portion of the skin
Hand Geometry	covert recording	some diseases like arthritis objects that change the shape of the hand like jewelry
Palm vein	Covert recording	
Iris	Covert recording	Glasses, eyelid obstruction, gaze deviation
Retina	No known threats	
Face	Covert recording	Changing face expressions, aging
Voice	Voice mimic, synthesis, covert recording	Aging, emotional state
Signature	Handwriting signature mimic, synthesis, covert recording	Writing behavior change
Hand gestures	Hand gestures mimic, synthesis, covert recording	Behavior change
Mouse and keystrokes	Modeling human behavior	Behavior change
EEG	No known threats	Behavior change

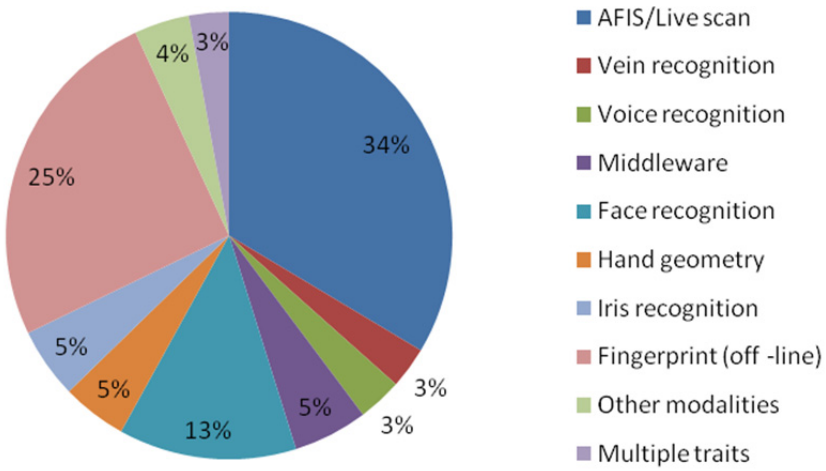

Figure 4. market share of different feature based biometric systems (Singla & Kumar, 2013)

6. Conclusion

Automated systems specially the remote ones suffer heavily from the problem of identity alteration. Multiple kinds of possessions have contributed in verifying the personality of an individual. Owning information, objects, and biological characteristics have been the discriminating factors in knowledge based, token based, and biometric based authentication respectively. Having knowledge or objects could be compromised or stolen. Biometric authentication has gained high success, especially with its permanent belonging to the human being. Some physiological traits are described to be unique and unchangeable while behavioral characteristics could be altered with time, emotional, and concentration level, but they mostly follow some common pattern. Biometric verification systems have a basic structure of four main components named acquisition, preprocessing, feature extraction, and template matching or classification. There are multiple attacks and vulnerability points threatening the authentication systems. They can be divided into attacks related to the user interface, attacks on modules and template database, and attacks on the interconnection between modules. The distinctive features are found in the hand, the voice and the head. The hand has a plenty of distinguishing attributes aside from its geometrical characteristics like fingerprints, palm print, and palm vein network. Behaviors generated from hand activities like gestures, keystrokes, mouse related movements, and written signatures are used to check the identity of the human being. The head contains features of the face and the brain parts. Face also includes eyes with their unique iris and retina. Finally, the decision of the used authentication system derived by the deployed authentication is determined by the needs, resources, priorities, environmental surroundings and the nature of the candidate users. The market share as well as the forecasted requirements for the next generation of the authentication systems explains the growing interest in specific distinguishing features especially those providing human vital signs.

References

Ahmed, H., Shukla, S., & Rai, H. M. (2014). Static Handwritten Signature Recognition Using Discrete Random Transform and Combined Projection Based Technique. Advanced Computing & Communication Technologies (ACCT), 2014 Fourth International Conference on (pp. 37–41). IEEE. http://dx.doi.org/10.1109/ACCT.2014.76

Ahmed, M. I., Awal, M., & Amin, M. (2012). Biometric authentication using circular segment around optical disc. Informatics, Electronics & Vision (ICIEV), 2012 International Conference on (pp. 178–183). IEEE. http://dx.doi.org/10.1109/ICIEV.2012.6317387

Akram, M. U., Tariq, A., & Khan, S. A. (2011). Retinal recognition: Personal identification using blood vessels. Internet Technology and Secured Transactions (ICITST), 2011 International Conference for (pp. 180–184). IEEE.

Al-Juboori, A. M., Wu, X., & Zhao, Q. (2013). Biometric Authentication System Based on Palm Vein. Computer Sciences and Applications (CSA), 2013 International Conference on (pp. 52–58). IEEE. http://dx.doi.org/10.1109/CSA.2013.19

Alarifi, A., Alkurtass, I., & Al-Salman, A. (2011). Arabic text-dependent speaker verification for mobile devices

using artificial neural networks. Machine Learning and Applications and Workshops (ICMLA), 2011 10th International Conference on (Vol. 2, pp. 350–353). IEEE. http://dx.doi.org/10.1109/ICMLA.2011.168

Alzahrani, H., & Boult, T. E. (2014). Remote authentication using vaulted fingerprint verification. SPIE Defense+ Security (p. 90750K–90750K). International Society for Optics and Photonics. http://dx.doi.org/10.1117/12.2053126

Amayeh, G., Bebis, G., Erol, A., & Nicolescu, M. (2006). Peg-free hand shape verification using high order zernike moments. Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference on (pp. 40–40). IEEE. http://dx.doi.org/10.1109/CVPRW.2006.155

Ashby, C., Bhatia, A., Tenore, F., & Vogelstein, J. (2011). Low-cost electroencephalogram (EEG) based authentication. Neural Engineering (NER), 2011 5th International IEEE/EMBS Conference on (pp. 442–445). IEEE. http://dx.doi.org/10.1109/NER.2011.5910581

Aslan, I., Uhl, A., Meschtscherjakov, A., & Tscheligi, M. (2014). Mid-air Authentication Gestures: An Exploration of Authentication Based on Palm and Finger Motions. Proceedings of the 16th International Conference on Multimodal Interaction (pp. 311–318). ACM. http://dx.doi.org/10.1145/2663204.2663246

Baloul, M., Cherrier, E., & Rosenberger, C. (2012). Challenge-based speaker recognition for mobile authentication. Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the (pp. 1–7). IEEE.

Banerjee, S. P., & Woodard, D. L. (2012). Biometric authentication and identification using keystroke dynamics: A survey. Journal of Pattern Recognition Research, 7(1), 116–139. http://dx.doi.org/10.13176/11.427

Bansod, N. S., Dadhade, S. B., Kawathekar, S. S., & Kale, K. (2014). Speaker Recognition Using Marathi (Varhadi) Language. Intelligent Computing Applications (ICICA), 2014 International Conference on (pp. 421–425). IEEE. http://dx.doi.org/10.1109/ICICA.2014.92

Bayly, D., Castro, M., Arakala, A., Jeffers, J., & Horadam, K. (2010). Fractional biometrics: safeguarding privacy in biometric applications. *International Journal of Information Security, 9*(1), 69–82. http://dx.doi.org/10.1007/s10207-009-0096-z

Belahcene, M., Chouchane, A., & Ouamane, H. (2014). 3D face recognition in presence of expressions by fusion regions of interest. Signal Processing and Communications Applications Conference (SIU), 2014 22nd (pp. 2269–2274). IEEE. http://dx.doi.org/10.1109/SIU.2014.6830718

Bellegarda, J. R., & Silverman, K. E. (2014). Fast, language-independent method for user authentication by voice. Google Patents.

Bertoncini, C., Rudd, K., Nousain, B., & Hinders, M. (2012). Wavelet fingerprinting of radio-frequency identification (RFID) tags. *Industrial Electronics, IEEE Transactions on, 59*(12), 4843–4850. http://dx.doi.org/10.1109/TIE.2011.2179276

Bharadi, V. A., Pandya, B., & Nemade, B. (2014). Multimodal biometric recognition using iris & fingerprint: By texture feature extraction using hybrid wavelets. Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th International Conference (pp. 697–702). IEEE. http://dx.doi.org/10.1109/CONFLUENCE.2014.6949309

Bhatt, S., & Santhanam, T. (2013). Keystroke dynamics for biometric authentication—A survey. Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on (pp. 17–23). IEEE. http://dx.doi.org/10.1109/ICPRIME.2013.6496441

Borg, M. A., Said, S., Ben Amor, B., & Ben Amar, C. (2011). Information fusion for 3D face recognition. Image Information Processing (ICIIP), 2011 International Conference on (pp. 1–6). IEEE. http://dx.doi.org/10.1109/ICIIP.2011.6108980

Bowyer, K. W., Hollingsworth, K. P., & Flynn, P. J. (2013). A survey of iris biometrics research: 2008–2010. Handbook of iris recognition (pp. 15–54). Springer. http://dx.doi.org/10.1007/978-1-4471-4402-1_2

Breebaart, J., Yang, B., Buhan-Dulman, I., & Busch, C. (2009). Biometric template protection. *Datenschutz und Datensicherheit-DuD, 33*(5), 299–304. http://dx.doi.org/10.1007/s11623-009-0089-0

Brunet, K., Taam, K., Cherrier, E., Faye, N., Rosenberger, C., & others. (2013). Speaker Recognition for Mobile User Authentication: An Android Solution. 8ème Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR SSI).

Cai, R., & Hu, D. (2010). Image fusion of palmprint and palm vein: Multispectral palm image fusion. Image and Signal Processing (CISP), 2010 3rd International Congress on (Vol. 6, pp. 2778–2781). IEEE. http://dx.doi.org/10.1109/CISP.2010.5647598

Chakrabarty, D., Prasanna, S. M., & Das, R. K. (2013). Development and evaluation of online text-independent speaker verification system for remote person authentication. International Journal of Speech Technology, 16(1), 75–88. http://dx.doi.org/10.1007/s10772-012-9160-6

Chakraborty, N., & Mondal, S. (2014). An Improved Methodology towards Providing Immunity against Weak Shoulder Surfing Attack. Information Systems Security (pp. 298–317). Springer. http://dx.doi.org/10.1007/978-3-319-13841-1_17

Chen, W.-Y., Kuo, Y.-M., & Chung, C.-H. (2013). Palm Image Recognition Using Image Processing Techniques. Recent Trends in Applied Artificial Intelligence (pp. 572–580). Springer. http://dx.doi.org/10.1007/978-3-642-38577-3_59

Chen, X., Shi, J., Xu, R., Yiu, S., Fang, B., & Xu, F. (2014). PAITS: Detecting Masquerader via Short-Lived Interventional Mouse Dynamics. Applications and Techniques in Information Security (pp. 231–242). Springer. http://dx.doi.org/10.1007/978-3-662-45670-5_22

Chen, X., Xu, F., Xu, R., Yiu, S., & Shi, J. (2014). A practical real-time authentication system with Identity Tracking based on mouse dynamics. Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on (pp. 121–122). IEEE. http://dx.doi.org/10.1109/INFCOMW.2014.6849185

Choi, S., & Zage, D. (2012). Addressing insider threat using "where you are" as fourth factor authentication. Security Technology (ICCST), 2012 IEEE International Carnahan Conference on (pp. 147–153). IEEE. http://dx.doi.org/10.1109/CCST.2012.6393550

Clark, G. D., & Lindqvist, J. (2014). Engineering Gesture-Based Authentication Systems. arXiv preprint arXiv:1408.6010. http://dx.doi.org/10.1109/MPRV.2015.6

Condurache, A. P., Kotzerke, J., & Mertins, A. (2012). Robust retina-based person authentication using the sparse classifier. Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European (pp. 1514–1518). IEEE.

Connell, J., Ratha, N., Gentile, J., & Bolle, R. (2013). Fake iris detection using structured light. Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on (pp. 8692–8696). IEEE. http://dx.doi.org/10.1109/ICASSP.2013.6639363

Conti, V., Vitabile, S., Agnello, L., & Sorbello, F. (2013). Fingerprint and Iris Based Authentication in Inter-cooperative Emerging e-Infrastructures. Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence (pp. 433–462). Springer. http://dx.doi.org/10.1007/978-3-642-34952-2_18

De, P., Dey, K., Mankar, V., & Mukherjea, S. (2013). Towards an interoperable mobile wallet service. Emerging Technologies for a Smarter World (CEWIT), 2013 10th International Conference and Expo on (pp. 1–6). IEEE. http://dx.doi.org/10.1109/CEWIT.2013.6713767

Fatima, J., Syed, A. M., & Akram, M. U. (2013). Feature point validation for improved retina recognition. Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2013 IEEE Workshop on (pp. 13–16). IEEE. http://dx.doi.org/10.1109/BIOMS.2013.6656142

Finzgar, L., & Trebar, M. (2011). Use of NFC and QR code identification in an electronic ticket system for public transport. Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on (pp. 1–6). IEEE.

Fong, S., Zhuang, Y., & Fister, I. (2013). A biometric authentication model using hand gesture images. *Biomedical engineering online, 12*(1), 111. http://dx.doi.org/10.1186/1475-925X-12-111

Friese, I., Heuer, J., & Kong, N. (2014). Challenges from the Identities of Things: Introduction of the Identities of Things discussion group within Kantara initiative. Internet of Things (WF-IoT), 2014 IEEE World Forum on (pp. 1–4). IEEE. http://dx.doi.org/10.1109/WF-IoT.2014.6803106

Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric Anti-spoofing Methods: A Survey in Face Recognition. http://dx.doi.org/10.1109/ACCESS.2014.2381273

Granger, E., Khreich, W., Sabourin, R., & Gorodnichy, D. O. (2012). Fusion of biometric systems using boolean combination: an application to iris–based authentication. *International Journal of Biometrics, 4*(3), 291–315.

http://dx.doi.org/10.1504/IJBM.2012.047645

Hausawi, Y. M., Allen, W. H., & Bahr, G. S. (2014). Choice-based authentication: A usable-security approach. Universal Access in Human-Computer Interaction. Design and Development Methods for Universal Access (pp. 114–124). Springer. http://dx.doi.org/10.1007/978-3-319-07437-5_12

He, B., Luo, Q., & Choi, B. (2007). Bayesian networks for knowledge-based authentication. *Knowledge and Data Engineering, IEEE Transactions on, 19*(5), 695–710. http://dx.doi.org/10.1109/TKDE.2007.1024

Hema, C., & Osman, A. A. (2010). Single trial analysis on EEG signatures to identify individuals. Signal Processing and Its Applications (CSPA), 2010 6th International Colloquium on (pp. 1–3). IEEE. http://dx.doi.org/10.1109/CSPA.2010.5545313

Hema, C. R., Paulraj, M., & Kaur, H. (2008). Brain signatures: a modality for biometric authentication. Electronic Design, 2008. ICED 2008. International Conference on (pp. 1–4). IEEE. http://dx.doi.org/10.1109/ICED.2008.4786753

Huang, C.-H., & Huang, S.-C. (2013). RFID systems integrated OTP security authentication design. Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2013 Asia-Pacific (pp. 1–8). IEEE. http://dx.doi.org/10.1109/APSIPA.2013.6694342

Huang, G. B., Lee, H., & Learned-Miller, E. (2012). Learning hierarchical representations for face verification with convolutional deep belief networks. Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on (pp. 2518–2525). IEEE. http://dx.doi.org/10.1109/CVPR.2012.6247968

Iranmanesh, V., Ahmad, S. M. S., Adnan, W. A. W., Yussof, S., Arigbabu, O. A., & Malallah, F. L. (2014). Online Handwritten Signature Verification Using Neural Network Classifier Based on Principal Component Analysis. The Scientific World Journal, 2014. http://dx.doi.org/10.1155/2014/381469

Jain, A. K., & Nandakumar, K. (2012). Biometric authentication: System security and user privacy. *Computer,* (11), 87–92. http://dx.doi.org/10.1109/MC.2012.364

Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). Introduction to biometrics. Springer. http://dx.doi.org/10.1007/978-0-387-77326-1

Jeffers, J., Davis, S. A., & Horadam, K. J. (2012). Estimating individuality in feature point based retina templates. Biometrics (ICB), 2012 5th IAPR International Conference on (pp. 454–459). IEEE. http://dx.doi.org/10.1109/ICB.2012.6199792

Jeon, J.-H., Oh, B.-S., & Toh, K.-A. (2012). A system for hand gesture based signature recognition. Control Automation Robotics & Vision (ICARCV), 2012 12th International Conference on (pp. 171–175). IEEE. http://dx.doi.org/10.1109/ICARCV.2012.6485153

Jesudoss, A., & Subramaniam, N. (2014). A Survey on Authentication Attacks and Countermeasures in a Distributed Environment. *IJCSE, 5*(2).

Jorgensen, Z., & Yu, T. (2011). On mouse dynamics as a behavioral biometric for authentication. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (pp. 476–482). ACM. http://dx.doi.org/10.1145/1966913.1966983

Jose Albin, A., Nandhitha, N., & Emalda Roslin, S. (2014). Text independent speaker recognition system using Back Propagation Network with wavelet features. Communications and Signal Processing (ICCSP), 2014 International Conference on (pp. 592–596). IEEE. http://dx.doi.org/10.1109/ICCSP.2014.6949910

Karnan, M., Akila, M., & Krishnaraj, N. (2011). Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing, 11*(2), 1565–1573. http://dx.doi.org/10.1016/j.asoc.2010.08.003

Kataria, A. N., Adhyaru, D. M., Sharma, A. K., & Zaveri, T. H. (2013). A survey of automated biometric authentication techniques. Engineering (NUiCONE), 2013 Nirma University International Conference on (pp. 1–6). IEEE. http://dx.doi.org/10.1109/NUiCONE.2013.6780190

Kim, S.-H., Choi, D., Jin, S.-H., & Lee, S.-H. (2013). Geo-location based QR-Code authentication scheme to defeat active real-time phishing attack. Proceedings of the 2013 ACM workshop on Digital identity management (pp. 51–62). ACM. http://dx.doi.org/10.1145/2517881.2517889

Kim, Y.-G., & Jun, M.-S. (2011). A design of user authentication system using QR code identifying method. Computer Sciences and Convergence Information Technology (ICCIT), 2011 6th International Conference on (pp. 31–35). IEEE.

King, R. (2015, January). Retrieved from http://www.biometricupdate.com/201502/special-report-biometrics-in-healthcare

Koong, C.-S., Yang, T.-I., & Tseng, C.-C. (2014). A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices. The Scientific World Journal, 2014. http://dx.doi.org/10.1155/2014/781234

Kumar, A., Hanmandlu, M., Madasu, V. K., & Vasikarla, S. (2011). A palm print authentication system using quantized phase feature representation. Applied Imagery Pattern Recognition Workshop (AIPR), 2011 IEEE (pp. 1–8). IEEE. http://dx.doi.org/10.1109/AIPR.2011.6176353

Lee, J.-C. (2012). A novel biometric system based on palm vein image. *Pattern Recognition Letters, 33*(12), 1520–1528. http://dx.doi.org/10.1016/j.patrec.2012.04.007

Leng, X., Hancke, G. P., Mayes, K., & Markantonakis, K. (2012). Tag group authentication using bit-collisions. Information Security for South Africa (ISSA), 2012 (pp. 1–8). IEEE. http://dx.doi.org/10.1109/ISSA.2012.6320447

Li, M., & Narayanan, S. (2011). Robust talking face video verification using joint factor analysis and sparse representation on gmm mean shifted supervectors. Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on (pp. 1481–1484). IEEE. http://dx.doi.org/10.1109/ICASSP.2011.5946773

Liu, J., Liu, T. ting, & Chen, B. ru. (2014). A Novel Iris Verification System Based on Feature Extraction. Proceedings of the 2013 International Conference on Electrical and Information Technologies for Rail Transportation (EITRT2013)-Volume I (pp. 441–449). Springer. http://dx.doi.org/10.1007/978-3-642-53778-3_43

Ma, Y., & Feng, J. (2011). Evaluating usability of three authentication methods in web-based application. Software Engineering Research, Management and Applications (SERA), 2011 9th International Conference on (pp. 81–88). IEEE. http://dx.doi.org/10.1109/SERA.2011.18

Marasco, E., & Ross, A. (2014). A Survey on Antispoofing Schemes for Fingerprint Recognition Systems. *ACM Computing Surveys (CSUR), 47*(2), 28. http://dx.doi.org/10.1145/2617756

Marcel, S., & Millán, J. del R. (2007). Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 29*(4), 743–752. http://dx.doi.org/10.1109/TPAMI.2007.1012

Marcel, S., Nixon, M. S., & Li, S. Z. (2014). Handbook of Biometric Anti-Spoofing. Springer. http://dx.doi.org/10.1007/978-1-4471-6524-8

Mathew, G., & Thomas, S. (2013). A Novel Multifactor Authentication System Ensuring Usability and Security. arXiv preprint arXiv:1311.4037. http://dx.doi.org/10.5121/ijsptm.2013.2503

Matyas, V., & Riha, Z. (2010). Security of biometric authentication systems. Computer Information Systems and Industrial Management Applications (CISIM), 2010 International Conference on (pp. 19–28). IEEE. http://dx.doi.org/10.1109/CISIM.2010.5643698

Mayrhofer, R., Fuß, J., & Ion, I. (2013). UACAP: A unified auxiliary channel authentication protocol. *Mobile Computing*, IEEE Transactions on, *12*(4), 710–721. http://dx.doi.org/10.1109/TMC.2012.43

Mock, K., Hoanca, B., Weaver, J., & Milton, M. (2012). Real-time continuous iris recognition for authentication using an eye tracker. Proceedings of the 2012 ACM conference on Computer and communications security (pp. 1007–1009). ACM. http://dx.doi.org/10.1145/2382196.2382307

Nseir, S., Hirzallah, N., & Aqel, M. (2013). A secure mobile payment system using QR code. Computer Science and Information Technology (CSIT), 2013 5th International Conference on (pp. 111–114). IEEE. http://dx.doi.org/10.1109/CSIT.2013.6588767

Panjwani, S., Naldurg, P., & Bhaskar, R. (2010). Analysis of Two Token-Based Authentication Schemes for Mobile Banking. Microsoft Research Technical Report.

Patel, B., Patel, D., Patel, S., Patel, R., Tanti, B., & Doshi, N. (2012). A Novel Approach for Email Login System. Advances in Computer Science and Information Technology. Computer Science and Engineering (pp. 282–287). Springer. http://dx.doi.org/10.1007/978-3-642-27308-7_30

Pillai, J. K., Patel, V. M., Chellappa, R., & Ratha, N. K. (2013). Robust and secure iris recognition. Handbook of

Iris Recognition (pp. 183–204). Springer. http://dx.doi.org/10.1007/978-1-4471-4402-1_10

Pokric, B., Krco, S., & Pokric, M. (2014). Augmented Reality Based Smart City Services Using Secure IoT Infrastructure. Advanced Information Networking and Applications Workshops (WAINA), 2014 28th International Conference on (pp. 803–808). IEEE. http://dx.doi.org/10.1109/WAINA.2014.127

Pushpalatha, K., Gautam, A., Kumar, K., & others. (2014). Offline signature verification based on contourlet transform and textural features using HMM. Recent Advances and Innovations in Engineering (ICRAIE), 2014 (pp. 1–6). IEEE. http://dx.doi.org/10.1109/ICRAIE.2014.6909124

Qamber, S., Waheed, Z., & Akram, M. U. (2012). Personal identification system based on vascular pattern of human retina. Biomedical Engineering Conference (CIBEC), 2012 Cairo International (pp. 64–67). IEEE. http://dx.doi.org/10.1109/CIBEC.2012.6473297

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal, 40(3), 614–634. http://dx.doi.org/10.1147/sj.403.0614

Ravi, H., & Sivanath, S. K. (2013). A novel method for touch-less finger print authentication. Technologies for Homeland Security (HST), 2013 IEEE International Conference on (pp. 147–153). IEEE. http://dx.doi.org/10.1109/THS.2013.6698991

Ravi, K., & Palaniappan, R. (2005). Leave-one-out authentication of persons using 40 Hz EEG oscillations. Computer as a Tool, 2005. EUROCON 2005. The International Conference on (Vol. 2, pp. 1386–1389). IEEE. http://dx.doi.org/10.1109/EURCON.2005.1630219

Ray, K. B. (2013). Extracting Region of Interest for Palm Print Authentication. arXiv preprint arXiv:1312.6219.

Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. World Applied Sciences Journal, 19(4), 439–444.

Roberts, C. (2007). Biometric attack vectors and defences. Computers & Security, 26(1), 14–25. http://dx.doi.org/10.1016/j.cose.2006.12.008

Sae-Bae, N., Ahmed, K., Isbister, K., & Memon, N. (2012). Biometric-rich gestures: a novel approach to authentication on multi-touch devices. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 977–986). ACM. http://dx.doi.org/10.1145/2207676.2208543

Sae-Bae, N., Memon, N., Isbister, K., & Ahmed, K. (2014). Multitouch Gesture-Based Authentication. IEEE Transactions on Information Forensics and Security, 9(4), 568–582. http://dx.doi.org/10.1109/TIFS.2014.2302582

Sahu, S. K., Dalai, A. K., & Jena, S. K. (2014). Varying Password Based Scheme for User Authentication. Advanced Computing, Networking and Informatics-Volume 2 (pp. 361–368). Springer. http://dx.doi.org/10.1007/978-3-319-07350-7_40

Saxena, N., Uddin, M. B., Voris, J., & Asokan, N. (2011). Vibrate-to-unlock: Mobile phone assisted user authentication to multiple personal RFID tags. Pervasive Computing and Communications (PerCom), 2011 IEEE International Conference on (pp. 181–188). IEEE. http://dx.doi.org/10.1109/PERCOM.2011.5767583

Shen, C., Cai, Z., Guan, X., Du, Y., & Maxion, R. A. (2013). User authentication through mouse dynamics. Information Forensics and Security, IEEE Transactions on, 8(1), 16–30. http://dx.doi.org/10.1109/TIFS.2012.2223677

Sherman, M., Clark, G., Yang, Y., Sugrim, S., Modig, A., Lindqvist, J., Oulasvirta, A., et al. (2014). User-generated free-form gestures for authentication: security and memorability. arXiv preprint arXiv:1401.0561. http://dx.doi.org/10.1145/2594368.2594375

Shi, X., & Gu, J. (2012). An authentication method resistant to video-recording attacks. Computer Science and Network Technology (ICCSNT), 2012 2nd International Conference on (pp. 1967–1972). IEEE. http://dx.doi.org/10.1109/ICCSNT.2012.6526304

Singh, N. K. (2014). An improved algorithm for efficient iris based system. Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on (pp. 604–607). IEEE. http://dx.doi.org/10.1109/ICCICCT.2014.6993033

Singla, S. K., & Kumar, S. (2013). A review of data acquisition and difficulties in sensor module of biometric systems. Songklanakarin Journal of Science and Technology, 589–597.

Su, F., Zhou, H., Feng, Z., & Ma, J. (2012). A biometric-based covert warning system using EEG. Biometrics

(ICB), 2012 5th IAPR International Conference on (pp. 342–347). IEEE. http://dx.doi.org/10.1109/ICB.2012.6199830

Syed, Z., Banerjee, S., & Cukic, B. (2014). Leveraging Variations in Event Sequences in Keystroke-Dynamics Authentication Systems. High-Assurance Systems Engineering (HASE), 2014 IEEE 15th International Symposium on (pp. 9–16). IEEE. http://dx.doi.org/10.1109/HASE.2014.11

Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). Deepface: Closing the gap to human-level performance in face verification. Computer Vision and Pattern Recognition (CVPR), 2014 IEEE Conference on (pp. 1701–1708). IEEE. http://dx.doi.org/10.1109/CVPR.2014.220

Tian, J., Qu, C., Xu, W., & Wang, S. (2013). KinWrite: Handwriting-Based Authentication Using Kinect. NDSS.

Tome, P., & Marcel, S. (2015). On the Vulnerability of Palm Vein Recognition to Spoofing Attacks. The 8th IAPR International Conference on Biometrics (ICB).

Tomeo-Reyes, I., & Chandran, V. (2013). Iris Based Identity Verification Robust to Sample Presentation Security Attacks. International Journal of Information Science and Intelligent System, 2(1), 27–41.

Topcu, B., Kayaoglu, M., Yildirim, M. K., & Uludag, U. (2012). Fingerprint matching utilizing non-distal phalanges. Pattern Recognition (ICPR), 2012 21st International Conference on (pp. 2400–2403). IEEE.

Veldhuis, R. (2008). Introduction to Biometrics (121090).

Vora, R. A., Bharadi, V., & Kekre, H. (2012). Retinal scan recognition using wavelet energy entropy. Communication, Information & Computing Technology (ICCICT), 2012 International Conference on (pp. 1–6). IEEE.

Wang, J., & Johnson, M. T. (2013). Vocal source features for bilingual speaker identification. Signal and Information Processing (ChinaSIP), 2013 IEEE China Summit & International Conference on (pp. 170–173). IEEE. http://dx.doi.org/10.1109/ChinaSIP.2013.6625321

Wang, L., Geng, X., & Global, I. (2010). Behavioral biometrics for human identification: Intelligent applications. Medical Information Science Reference. http://dx.doi.org/10.4018/978-1-60566-725-6

Watanabe, M. (2008). Palm vein authentication. Advances in Biometrics (pp. 75–88). Springer. http://dx.doi.org/10.1007/978-1-84628-921-7_5

Watanabe, M., Endoh, T., Shiohara, M., & Sasaki, S. (2005). Palm vein authentication technology and its applications. Proceedings of the biometric consortium conference (pp. 19–21).

Wu, T., Turaga, P., & Chellappa, R. (2012). Age estimation and face verification across aging using landmarks. Information Forensics and Security, IEEE Transactions on, 7(6), 1780–1788. http://dx.doi.org/10.1109/TIFS.2012.2213812

Wu, X., Zhang, D., & Wang, K. (2006). Palm line extraction and matching for personal authentication. Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, 36(5), 978–987. http://dx.doi.org/10.1109/TSMCA.2006.871797

Wu, Z., Evans, N., Kinnunen, T., Yamagishi, J., Alegre, F., & Li, H. (2015). Spoofing and countermeasures for speaker verification: a survey. Speech Communication, 66, 130–153. http://dx.doi.org/10.1016/j.specom.2014.10.005

Xi, K., Ahmad, T., Han, F., & Hu, J. (2011). A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment. Security and Communication Networks, 4(5), 487–499. http://dx.doi.org/10.1002/sec.225

Yeom, S.-K., Suk, H.-I., & Lee, S.-W. (2013a). Eeg-based person authentication using face stimuli. Brain-Computer Interface (BCI), 2013 International Winter Workshop on (pp. 58–61). IEEE. http://dx.doi.org/10.1109/IWW-BCI.2013.6506630

Yeom, S.-K., Suk, H.-I., & Lee, S.-W. (2013b). Person authentication from neural activity of face-specific visual self-representation. Pattern Recognition, 46(4), 1159–1169. http://dx.doi.org/10.1016/j.patcog.2012.10.023

Yuan, W., & Tang, Y. (2011). The Driver Authentication Device Based on the Characteristics of Palmprint and Palm Vein. Hand-Based Biometrics (ICHB), 2011 International Conference on (pp. 1–5). IEEE. http://dx.doi.org/10.1109/ICHB.2011.6094336

Zafeiriou, S., & Pantic, M. (2011). Facial behaviometrics: The case of facial deformation in spontaneous smile/laughter. Computer Vision and Pattern Recognition Workshops (CVPRW), 2011 IEEE Computer

Society Conference on (pp. 13–19). IEEE. http://dx.doi.org/10.1109/CVPRW.2011.5981832

Zhang, F., Kondoro, A., & Muftic, S. (2012). Location-based authentication and authorization using smart phones. Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on (pp. 1285–1292). IEEE. http://dx.doi.org/10.1109/TrustCom.2012.198

Zhong, Y., Deng, Y., & Jain, A. K. (2012). Keystroke dynamics for user authentication. Computer Vision and Pattern Recognition Workshops (CVPRW), 2012 IEEE Computer Society Conference on (pp. 117–123). IEEE. http://dx.doi.org/10.1109/CVPRW.2012.6239225

Zhou, Y., & Kumar, A. (2011). Human identification using palm-vein images. Information Forensics and Security, IEEE Transactions on, 6(4), 1259–1274. http://dx.doi.org/10.1109/TIFS.2011.2158423

Zúquete, A., Quintela, B., & Cunha, J. P. S. (2010). Biometric authentication using brain responses to visual stimuli. Proceedings of the International Conference on Bio-inspired Systems and Signal Processing (pp. 103–112). http://dx.doi.org/10.5220/0002750101030112