Instant Journal of Forensic Science
Review Article Open Access

# Biometrics in Criminalistics and Forensics

**Sinisa Franjic**

Independent Researcher

***Corresponding Author:** Sinisa Franjic, Independent Researcher, Email: sinisa.franjic@gmail.com

***Received Date:*** *Feb 22, 2021 /* ***Accepted Date:*** *Mar 19, 2021/* ***Published Date:*** *Mar 22, 2021*

## Abstract

Biometrics is an authentication system that uses the unique physical characteristics of each person to be authenticated by the IT system. This means that when logging in to a computer, instead of entering a username and password, the user authenticates himself with something else that is unique to him and that makes him unique and different from other people. The most commonly used features are fingerprint, hand and face geometry, iris appearance etc. All of these characteristics are unique to each person. The application in criminalistics and forensics is very significant, especially in the part related to identification.

**Keywords**: Biometrics, Biometric Recognition, Authentication, Human Characteristics

**Cite this article as:** Sinisa Franjic. 2021. Biometrics in Criminalistics and Forensics. Int J Forensic Sci. 3: 10-16.

**Copyright:** This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. Copyright © 2021; Sinisa Franjic

## Introduction

The problem of user authentication in identity management systems has a reliable solution provided by biometric recognition [1]. Today, biometric systems have a widespread deployment in various applications-providing a powerful alternative to traditional authentication schemes. However, there are increasing concerns about the security and privacy of biometric technology. A biometric system is vulnerable to a variety of attacks aimed at undermining the integrity of the authentication process. These attacks are intended to either circumvent the security afforded by the system or to deter the normal functioning of the system. Vulnerability in a biometric system results in incorrect recognition or failure to correctly recognize individuals. Their existence in a biometric system is largely dependent on system design and structure, the type of biometrics used, and managerial policies. A high-level categorization of the different vulnerabilities of a biometric system is presented. Vulnerability analysis determines the imposter usage of the vulnerabilities with the aim of breaking the security policy. In the recent past, multimedia systems have undergone enormous developments and with the technological advances in the area, a great number of multimedia applications have emerged [2]. The developments in computer hardware as well as software in terms of performance, capacity and cost have been the enabler for the movement of many concepts of this originally scientific discipline, allocated in the domain stretching from signal processing in electrical engineering to computer science, from theory to practice. One important factor for the success of this technology was the movement from the concept of personalized computers in the early 1980's towards the paradigm of globally networked, ubiquitous infrastructures, which we find today. In the context of challenges arising from this evolution, the new research domain of Multimedia Communications has emerged. Among the various areas of interest in this domain, recently two categories have attracted increasing activity: quality and security for multimedia services such as IP telephony. Video-on-Demand and Digital Watermarking. With respect to security in multimedia services, we find numerous aspects, which need to be addressed in many application scenarios. These aspects include confidentiality/privacy, integrity and authenticity of multimedia content. Also, quite often, the logical binding of multimedia content to human identities is desirable, for example for protecting copyrights in digital media or for the authorization to use a specific multimedia service. Within the forensic identification sciences, there are many evidence types that have been used for human identification, with varying degrees of success [3]. These alleged biometrics include ear-marks, bite-marks, facial mapping and gait analysis-the identification of the characteristic body movements of individuals. Ear-marks occur in quite specific crime scene contexts. Bite-mark evidence, on the other hand, is more common and has been included together with identification of individuals by the direct examination of human dentition, in the field of forensic odontology. Facial mapping and gait analysis are more recent techniques that have become increasingly significant due to the ease with which recorded images, for example, from CCTV cameras, are now available and the development of digital image manipulation tools to facilitate analysis. Nevertheless, all these areas of work are justifiably subject to the same criticisms made of other identification sciences, namely weak underpinning science, rogue experts, subjective interpretation and arbitrary, not to say over-enthusiastic, evaluation.

## System

A reliable identity management system is the need of the day to combat the epidemic growth in identity theft and to meet the increased security requirements in a variety of applications ranging from international border crossings to securing information in databases [1]. Security is “freedom from risk of danger,” whereas computer and data security is “the ability of a system to protect information and system resources with respect to confidentiality and integrity.” Defining biometrics system security is difficult because of the ways biometric systems differ from traditional computer and cryptographic security. Biometric system security can be defined by its absence. Because biometrics is the “automated recognition of individuals based on their behavioral and biological characteristics,” vulnerability in biometric security results in incorrect recognition or failure to correctly recognize individuals. This definition includes methods to falsely accept an individual (template regeneration), affect overall system performance (denial of service), or to attack another system through leaked data (identity theft). Vulnerabilities are measured against explicit or implicit design claims. Establishing the identity of a person is a critical task in any identity management system. Surrogate representations of identity such as passwords and ID cards are not sufficient for reliable identity determination because they can be easily misplaced, shared, or stolen. Commonly used biometric traits include fingerprint, face, iris, hand geometry, voice, palmprint, handwritten signatures, and gait. Biometric systems have a number of desirable properties over traditional authentication systems. They are inherently more reliable than password-based authentication because biometric traits cannot be lost or forgotten (passwords can be lost or forgotten); biometric traits are difficult to copy, share, and distribute (passwords can be announced in hacker web sites); and they require the person being authenticated to be present at the time and point of authentication (conniving users can deny that they shared their password). It is difficult to forge biometrics (it requires more time, money, experience, and access privileges) and it is unlikely for the user to repudiate having accessed the digital content using biometrics. Thus, a biometricsbased authentication system is a powerful alternative to traditional authentication schemes. In some instances, biometrics can be used in conjunction with passwords (or tokens) to enhance the security offered by the authentication system. All these characteristics have led to the widespread deployment of biometric authentication systems. However, there are still issues concerning the security of biometric recognition systems that need to be addressed to ensure the integrity and public acceptance of these systems. In biometric applications, a relatively new technology is emerging, namely the optical scanning of superficial vein patterns [4]. In order to be viable, a biometric parameter has to be easily identifiable but hidden from view so that it cannot be reproduced or simulated. It can be observed that the veins of the human body do not leave external marks like fingerprints, are not easily falsifiable like the voice, cannot be disguised like face traits, and are extremely hard to covertly extract during and after the lifetime of an individual in order to be reused by an impostor. In the same time, the technology used to acquire the vein pattern has reduced costs and is not invasive, requires minimal cooperation from a person, and is largely a noncontact procedure that allows it to be used where hygienic concerns are an issue. Some of the most important requirements for a biometric system are the uniqueness and permanence of the biometric parameter used for recognition. Even in the case of complete uniqueness, a biometric system should be sensitive enough to be able to accurately discriminate between samples acquired from different individuals.

## Recognition

The meaning of “biometrics” is “life measurement” but it is usually used with unique physiological characteristics to recognize an individual [5]. For recognition, a collection of automated methods are used to recognize an individual person based on a physiological or behavioral characteristic. The application that most people think about, when it comes to biometrics, is in security. However, for biometric recognition, a number of biometric traits have been developed and are used for recognition. A biometric system is like a pattern recognition system that makes a personal identification or verification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the “automated methods of identifying or verifying of a living person based on a physiological or behavioral characteristic”. Biometric traits are used for both identification and verification. Depending on the application context, a biometric system may operate in verification or identification mode. In the verification mode, the system confirms or denies a person’s claimed identity by comparing the captured biometric features with the biometric template(s) stored in the system’s database. In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Some biometric characteristics of a person for identification and recognition are fingerprint, hand geometry, face, handwriting, voice, ear, DNA, hand thermogram, hand vein, palmprint, iris, and retina. Each biometric pattern has its strengths and weaknesses, and the choice depends on the application. The disadvantage of biometric recognition systems is chiefly attributed to the imperfect matching in contrast with traditional alphanumeric system [6]. Because of this, sample quality is more important for image-based biometric systems, and so is fingerprint image used for the Automatic Fingerprint Identification System (AFIS). Matching of fingerprint images is generally divided into three classes: correlation-based, image-based, and minutiae matching, among which the last one is acknowledged as the primary solution so far. In this case, good quality sample is basically a prerequisite for extracting reliable and sufficient minutia points, and is hence the essential factor for the overall matching performance. The effect of sample quality to the matching performance is defined as the utility of a biometric sample. Therefore, most of the Fingerprint Quality Assessment (FQA) approaches (or fingerprint quality metrics) rely on two aspects: subjective assessment criteria of the pattern and sample utility. In addition, most of the quality metrics are also evaluated in terms of the utility. However, this property is limited by matching configurations, i.e., sample utility varies as the matching algorithm changes because no matching approach proposed so far is perfect or robust enough in dealing with different image settings though their resolution is similar to each other (normal application requires gray-level images of 500-dpi according to the ISO). A historical example of biometrics is anthropometry, in which measurements of specific parts of the body were used for criminal records, classification, and identification [7]. There are several examples of forensic biometrics that rely on the unique characteristics of individuals for identification. Forensic odontologists (forensic dentists) analyze the unique features, shapes, placement, and dental work for teeth. Facial recognition analysis involves an examination of the unique measurements, proportions, and features of the face and skin. Iris scans capture the unique patterns within the pigmented section of the eye. The forensic sciences rely on these and other biometrics to identify individuals involved in crimes. Fingerprints are the most common biometric used for criminal identification. They were also the first biometrics to be recorded, stored, and searched via computer. Forensic scientists and criminal justice professionals utilize the Automated Fingerprint Identification System (AFIS) to store criminal fingerprint records, perform background checks, determine if an individual has been arrested before, and search for possible matches to latent fingerprints. The latent print examiner (LPE) enters a latent into the AFIS computer by scanning or photographing the fingerprint. The LPE may enhance the fingerprint and tell the computer which direction is up, which finger or hand to search, and where the core and delta are located. The LPE then selects minutiae or double-checks the minutiae selected by the computer. Fingerprint scanning is the acquisition and recognition of a person's fingerprint characteristics for identification purposes [8]. This allows for the recognition of a person through quantifiable physiological characteristics that verify the identity of an individual. Fingerprint recognition is the core identifier for mass-market biometric-ID systems as fingerprint-based systems have a high accuracy rate. Fingerprints are also considered to be "safe." Many users of biometrics devices, when questioned, are suspicious of the safety of using iris and retinal scanning techniques, for example, fearing that such devices will damage human eyesight over time. On balance, this may be a totally unfounded fear, but human concerns can be disproportionate to the actual risk of using such technology, a fact that a vendor must consider when designing and implementing systems.

Without doubt, fingerprints continue to play a huge role in the fight against crime, but fingerprints are becoming increasingly popular as a means of identification and verification in non-law enforcement domains as well. Today, fingerprints are being considered as important biometrics identifiers in worldwide civil applications, such as with federal ID cards, passports, bank cards, and library cards, as well as other less obvious applications, such as school access verification and as a substitute for money in the school cafeteria line.

## Authentication

With the increased interest in security and surveillance, the effective authentication of people has assumed great significance in recent years [9]. Consequently, the development of highly accurate biometric authentication systems has received prominent attention in the research community. Biometric authentication is defined as the process of utilizing unique personal or biometric features to identify a person. Popular biometric features used for person authentication include the face, fingerprint, DNA, retina, etc. However, the use of these features in biometric authentication systems requires the active cooperation of the subject involved, which is often difficult and inconvenient. To avoid the need for active user cooperation, without compromising on the authentication accuracy of the biometric authentication system, researchers have investigated the use of human gait, or walk, as a biometric feature. Specifically, the property of human gait or walk being unique to each individual has been utilized in biometric authentication systems to identify or verify individuals. In recent years, biometric-based authentication is increasingly gaining popularity in a large spectrum of applications, ranging from governmental programs to commercial applications such as logical and physical access control [10]. Compared to the traditional passwordbased authentication systems, the biometrics-based systems have the advantages of easier management (no need to memorizing the passwords and changing them periodically) and better security (biometrics confirm the identity of the user). Surprisingly, however, even the most sophisticated biometric-based authentication systems may be vulnerable to a simple broadcast attack. For instance, to break an iris recognition-based authentication system, a malicious intruder can find a photograph of the face of an authenticated person, printed out on a paper (with sufficiently high printing quality), cut the iris images out and paste it on his eyelids. When being presented to the system, instead of the live captured iris image, the system is fed with the rebroadcast iris image. For the purpose of recognition, these images are just the same, with the rebroadcast images with different noise characteristics from the printing process. Since many biometric-based authentication systems are built to be robust in image noises, such a simple trick will, unfortunately, work for the intruder purpose. A key feature for biometric-based authentication systems withstanding the “rebroadcast” attacks is to enable the systems to differentiate between a rebroadcast and a live image.

## Smartphone Authentication

The first methodology utilizes the knowledge in users’ memory and should be the most widely used techniques such as passwords and personal identification numbers [11]. However, long-term memory limitations are one of the weaknesses, which may result in simple passwords in practice. In addition, passwords can be easily captured by direct observation or various malware techniques. As an alternative, user authentication can be conducted through what users have such as keys and tokens. But such methodology has not been widely used in smartphone authentication, as it is required to deploy additional hardware on phones’ side, which would be expensive for smartphone users. In recent years, research has been focused more on biometric-based authentication on mobile devices, since biometric features are mostly unique and not duplicable or transferable. This methodology can use either physiological or behavioral features for authentication. Physiological features use measurements from the human body such as fingerprint, face, teeth, iris, and retina. By contrast, behavioral features use measurements from human actions such as signature, gait, and keystroke. With the rapid adoption of smartphones, touch dynamics has become a notable topic for smartphone authentication. For example, touchscreens have already become the leading input method on the mobile platform, with more than 78 % of all phones using a touchscreen. Touch dynamics can be described as the characteristics of the inputs received from a touchscreen when a user is interacting with a device (e.g., a touchscreen mobile phone). Intuitively, touch dynamics is different from keystroke dynamics in that touch dynamics has more input types such as multi-touch and touch movement. On the other hand, the inputs of press button up and press button down in keystroke dynamics are similar to the actions of touch press up and touch press down (e.g., single-touch) in touch dynamics. Due to its characteristics, touch dynamics received more attention from the literature.

## Individuals

Authentication technologies refer to some object you have (e.g., a key), information you know (e.g., a password), or something you are (that is a biometric feature) [12]. The most common and traditional authentication method is the use of a password. Its main challenge, however, is that individuals may be required to memorize extreme passwords. Also, passwords can be simply hacked. Biometric technology is an automatic pattern recognition mechanism that compares the measureable biological, physiological, and behavioral features of a person with a stored template to authenticate that person. Biometric systems are appropriate for applications that aim to identify individuals for a specific purpose. They provide a link between a person and his or her identity based on the application context. Biometrics have also been utilized to seek for patterns in normal people, for finding changes in bodily and psychological traits over time and in other health situations, and for providing a basis for ethnic classifications. Physiological characteristics are normally more stable and consistent than behavioral characteristics. Therefore, physical characteristics can be suitable features primarily to identify individuals. Physical characteristics include fingerprint, palm print, hand geometry, finger vein, hand vessels, iris, retina, face, DNA, blood pattern, ear shape, body odor, and skin patterns. Behavioral characteristics include voice, keystroke dynamics, signature and handwriting models, and mouse movements. Behavioral biometric characteristics are changeable according to psychological situations and environmental conditions. These human characteristics will improve through learning over time. They change as human ability improves. Hence, dynamic biometric systems are required to accept the human characteristics' changeability. Behavioral biometric characteristics introduce less invasive recognition methods that increase user acceptance.

## Conclusion

Biometrics is a set of automated methods for uniquely recognizing people based on one or more of their physical characteristics. Although biometrics is primarily used for authentication purposes, it is also applied in other areas related to modern information technology. The whole thing works so that in the beginning, the system records the unique characteristics of each person through a special sensor, digitizes them into a form understandable to a computer and marks the key characteristics. It stores this information in a secure place, and on the occasion of each further authentication, it compares the current and stored data.

## References

1. Mirajakar G. 2014. Security and Reliability Assessment for Biometric Systems. Advances in Biometrics for Secure Human Authentication and Recognition. CRC Press, Taylor & Francis Group, Boca Raton, USA. 4-6.
2. Vielhauer C. 2006. Biometric User Authentication for IT Security-From Fundamentals to Handwriting, Springer Science+Business Media, Inc, New York, USA. 11.
3. Adam C. 2016. Forensic Evidence in Court - Evaluation and Scientific Opinion. John Wiley & Sons, Ltd, Chichester, UK. 243.
4. Crisan S. 2017. A Novel Perspective on Hand Vein Patterns for Biometric Recognition: Problems. Challenges, and Implementations. Biometric Security and Privacy - Opportunities & Challenges in The Big Data Era, Springer International Publishing AG, Cham, Switzerland. 21.
5. Dehghani A, Farzin H, Vahedian H, et al. 2014. Review of Human Recognition Based on Retinal Images. Advances in Biometrics for Secure Human Authentication and Recognition, CRC Press. Taylor & Francis Group, Boca Raton, USA. 34.
6. Yao Z, Le Bars JM, Cherrier C, et al. 2017. Fingerprint Quality Assessment: Matching Performance and Image Quality. Biometric Security and Privacy - Opportunities & Challenges in The Big Data Era, Springer International Publishing AG, Cham, Switzerlan., 1.
7. Daluz HM. 2015. Fingerprint Analysis - Laboratory Workbook, CRC Press, Taylor & Francis Group, Boca Raton, USA. 33.

8. Galloway V, Charlton D. 2007. Fingerprints. Forensic Human Identification-An Introduction, CRC Press, Taylor & Francis Group, Boca Raton, USA. 67.
9. John V. 2014. Human Gait Signature for Biometric Authentication, Advances in Biometrics for Secure Human Authentication and Recognition, CRC Press, Taylor & Francis Group, Boca Raton, USA. 94.
10. Lyu S. 2013. Natural Image Statistics in Digital Image Forensics. Digital Image Forensics-There is More to a Picture than Meets the Eye", Springer Science+Business Media, New York, USA. 253-254.
11. Jiang L, Meng W. 2017. Smartphone User Authentication Using Touch Dynamics in the Big Data Era: Challenges and Opportunities. Biometric Security and Privacy-Opportunities & Challenges in The Big Data Era. Springer International Publishing AG, Cham, Switzerland. 163-164.
12. Noghondar ER. 2014. Legal Aspects and Ethical Issues in the Use of Biometrics - A Study from Norway. Advances in Biometrics for Secure Human Authentication and Recognition. CRC Press, Taylor & Francis Group, Boca Raton, USA. 254-255.