Scientific Research Publishing

International Journal of Intelligence Science, 2022, 12, 1-8
https://www.scirp.org/journal/ijis
ISSN Online: 2163-0356
ISSN Print: 2163-0283

Biometrics as a Matrix: The Short Distance between Crime and Security Systems, Prompting an Artificial Intelligence to Invent Electronic Biometrics ID!

Ahmed Laarfi

Brevard Public School, Brevard, FL, USA
Email: Ahmed.laarfi@outlook.com

How to cite this paper: Laarfi, A. (2022) Biometrics as a Matrix: The Short Distance between Crime and Security Systems, Prompting an Artificial Intelligence to Invent Electronic Biometrics ID! *International Journal of Intelligence Science*, **12**, 1-8.
https://doi.org/10.4236/ijis.2022.121001

Received: November 12, 2021
Accepted: January 8, 2022
Published: January 11, 2022

Abstract

This paper reviews the essential biometrics and develops a way to combine them with the Computer and User Information, giving us an Electronic Biometrics ID. This way, distributed databases contain imperative data from much helpful information that supports more security. We reviewed examples of what these databases would look like, which any responsible party could design to be global. As will be mentioned later, we obtain common international databases whose data are modified according to factors such as the owner of the device, the location of the device, and so on. This is very useful for tracking, and it combines biometrics with data set to give us a comprehensive electronic identification.

Keywords

Biometrics, Security, Privacy, Distributed System, Databases

1. Introduction

"When we describe mankind as a talking animal, we may have wronged the animals!"

People did not have names in the early Stone Age, but they distinguished each other. Unfortunately, I have no references to prove this. Still, logic dictates that they indicated each other in ancient societies even before the invention of speech or writing, and writing must have come after the speech in stages.

Animals from the beginning of the world are silent and do not speak, but our great-grandfathers and we after them knew that every animal in his society knows

every other animal as he is in the human world. Dogs bark only at strangers, whether talking animals or silent animals (Figure 1) [1].

In the cinema of the fifties and beyond, spy films depicted how a person of those days could disguise, and no one would be able to know him, and by straightforward means that do not rise to what science has reached today. The only biometric besides a fingerprint, not available to everyone, is the name, height, and distinguishing marks imprinted like an old seal on a human face. When you passed from one country to another in the era of passports, the name in the passport was the only biometric that allowed you to pass or not pass according to.

Changing the last name can change the person's identity. As for the length can be manipulated when they did not force passengers through airports to become barefoot and sometimes semi-naked.

Now, after the "boom" developments in all sciences and technologies, the last thing to be relied upon is the human name, even though it is the first thing that is asked to identify someone.

There are small things that, in total, if they match, form biometrics, but they cannot be relied upon. Thus, address, zip code, phone number, national security number, and others may be obtained by any hacker in his way and used; they are used to identify any person.

In our modern age, which includes "tomorrow," biometrics appeared. Two people cannot be alike in all the world, and if the similarity occurs in one, the other biometrics cannot be identical between two people.

In the beginning, was the speech, "We used to say: Speak so that I may know you, but today we say, show me your eyes so that I know who you are!"

We now have smart devices that reveal your identity to us. In the romance time, a man or a woman would sail into the other's eyes to feel love and warmth,

At 12:17 ETS on 11/11/21 Retrieved from https://kids.frontiersin.org/articles/10.3389/frym.2018.00046

Figure 1. An ancient-community communications {pre-linguistic eras}.

but now such looks are to know your sincerity from your falsehood [2] [3].

Each person has many biometrics that distinguishes him from others, and the most famous is the fingerprint. Now it is no longer relied on only in the protection systems for the sake of greater confidentiality. Instead, some systems rely more upon biometric, for example, the eye print, in addition to the human voice through which a person's identity can be known.

2. Biometrics and Cybercrimes

2.1. Today's Most Common Biometrics and Their Classification

Here we review the most critical types of biometrics. Undoubtedly, the fingerprint is the oldest type of identity verification. Still, with the development of science and tools, other biometrics have emerged that can be verified by one or a group of people's identity. Of these types of DNA, ear shape, eyes (Iris Recognition and Retina Recognition), Face Recognition, Finger Geometry Recognition, Gait, Odour, Typing Recognition, Vein Recognition, Voice (Speaker Identification and Speaker Verification/Authentication), Signature Recognition, and handwriting Recognition. Height, weight, and blood type are also biometrics, but we cannot rely on weight, especially if it was taken for a while. All of the biometrics were presented are categorized into two parts: physical biometrics and behavioral biometrics.

With computer applications intertwined with most aspects of daily life, it has become imperative to use them in verification procedures for confidentiality. The most common methods to verify identity are handprint, iris scan, and height. However, the problem of penetration of confidentiality remains, despite the complex key to accessing any system, represented by three types of biometrics. Of course, the issue of hacking a multi-input verification system is not an easy matter and is not available to all hackers. Still, the hypothesis of penetration on the weak possibility of it remains. Before these procedures, there was protection for the headquarters, represented in several steps. These steps are protection by security personnel, encrypted passwords with keys with long numbers, smart cards, and surveillance cameras, accompanied by an early warning, to reach system administrators in the event of hacking attempts (**Figure 2**) [4] [5].

2.2. The Era of Cybercrimes

> "The era of the muscle-dependent criminal is over, and he is replaced by a young man, or a child, thin, handsome, intelligent, capable and knowledgeable."

When the "virus" and sisters were developed at the beginning of the computer's spread to corrupt the work of the computer or the programs in it, others made protection systems. The topic has evolved and become daily new viruses are produced that have their fingerprint that is not available in the protection database, so they had to issue an update that includes new types through floppy

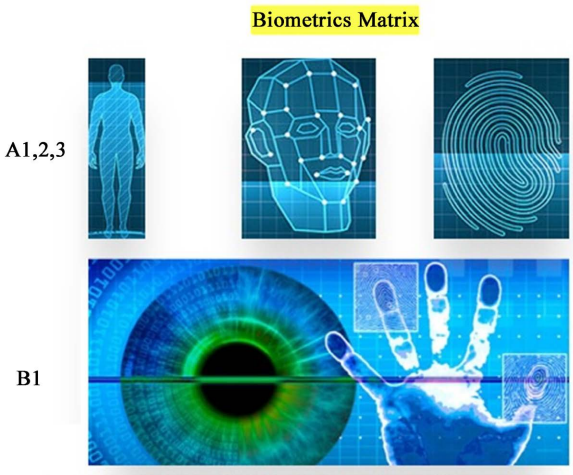

Figure 2. Some types of biometrics.

disks. Then the matter developed after easy access through the network of networks, the Internet, so the topic became just an update whenever required. Crime has existed since the beginning of the world and continues to the end. The fight against criminality has necessarily arisen. Invariably, the criminal is one step ahead of the anti-criminal.

Today, electronic crime has appeared to us, a virtual crime whose owner is characterized by intelligence and knowledge. The inventor of the virus was the first to write a line in the cybercrime book. Then the shape of the world changed in the last quarter-century to be more dangerous than it was before it, as the world is facing clever, educated criminals and "scholars."

3. Artificial Intelligence Systems Are Continually Evolving

The virus is created wherever you find computers and smart systems. However, with the development of artificial intelligence applications and the accompanying "sci-fi fantasy," the risks have increased dramatically and frighteningly, and this science, like any other, has become a double-edged sword.

Ultimately, the DNA remains steadfast and is not subject to penetration or forgery, possibly falsifying the examination results based on fake samples. This is a subject that is easy to discover. But so far, artificial intelligence has not developed a system based on DNA testing, and I expect that such a system will appear to us soon, but without guaranteeing penetrations. Non-cooperation of companies with crime-fighting agencies is one of the most significant issues, while Smartphone companies have critical user databases. Most companies are now struggling between the ethics of not disclosing their users' secrets and their crucial role in protecting society from "smart" crimes. Mobile and non-mobile operators also have the other part of the data, and often they disclose it according

to specific legal rules and procedures.

Indeed, we will not be able to make a unified database. Since all intrusions and crimes are done remotely, it may be beneficial to work with biometrics. Still, it is more beneficial to use a unified serial number for all companies producing the computer and its operating systems and software as a human fingerprint. Also, software that verifies this captured serial number, which cannot be tampered with, is done when someone enters a system or device.

On the human level, we may find a way to reveal a secret, unique fingerprint for every adult in the world. It is possible to combine a person's real identity through his digital identity and work between them. This is the presence of these virtual worlds that may be expected.

4. Proposal for the Development of a Digitized Biometrics System Cyberspace

The available electronic spaces make the world a small village. Yet, increase the margins of freedoms for all, especially those who live in countries that resemble pre-medieval countries regarding the power of authority and the lack of releases. Space without controls turns into anarchy that can be difficult to control. Hence I see that restrictions on verifying the identity of users of digital networks have become a necessity. In the developed world, there is no fear of freedom. As for the consequences of dictators, their space is always at stake, whether or not they verify the identity of network users. There may be countries that have no connection to the electronic world. An electronic fingerprint can be developed in an international serial number that reads the manufacturer, the country of origin, the store of sale, and the buyer's data. It is stored like data in the device. It can become a readable part of the memory. This data can be modified by changing the user's residence or phone. This data also preserves the proprietary rights of the companies producing the software. It also legalizes sales and pays both parties to register. Owners of old devices shall be obliged to contact specified authorities in each country to update their computers to include electronic fingerprint data. Artificial intelligence systems are updated to read and analyze the data and know its source. An international body is established to follow up on fingerprints and issue new fingerprints for old machines. Only the product that meets the authority's specifications is allowed in the market.

It is possible to program an application to compare images, for example, and this is available in Google, where any image can be entered to see if it previously existed or not. The same is the case by taking the fingerprint of the computer user and comparing it with a previously available database, which is only a step in the electronic biometrics system. This system combines natural and digital biometrics and collects them in giant databases. Artificial intelligence systems that serve Computer Vision can also read people's facial expressions, for example, and perform comparison operations [6].

The model we provide is a stored database with specific data from which the

source of any threat can be accessed. So when you buy the computer and turn it on, it takes a period to prepare and create the work environment for the user. It is being asked for the phone and email and then connects you to the Internet of your choice and works for him a password and a secret number and other data and accepted by the country and language and finally the fingerprint and optionally the personal picture other things and other information.

In addition to this data, the user is obliged to enter his valid ID, for example. Also, the user picture and the fingerprint are mandatory. The phone number is later a composite key with the city part in the phone number, for example, 347 for one of the counties of New York with the fingerprint and a number assigned to the computer similar to the VIN for cars so that it constitutes a mixture of natural and digital information.

When the user enters, he receives a message that represents the electronic card of the device and its owner (Table 1, Figure 3 and Figure 4).

Table 1. Electronic metadata combines biometrics with other data stored in distributed databases.

data Input By					
User	Personal	Passwords	Biometrics	Others	Others
Buyer	Buyer	Address	Others	Others	Others
global entity	Company	Country	Serial	Device	Others

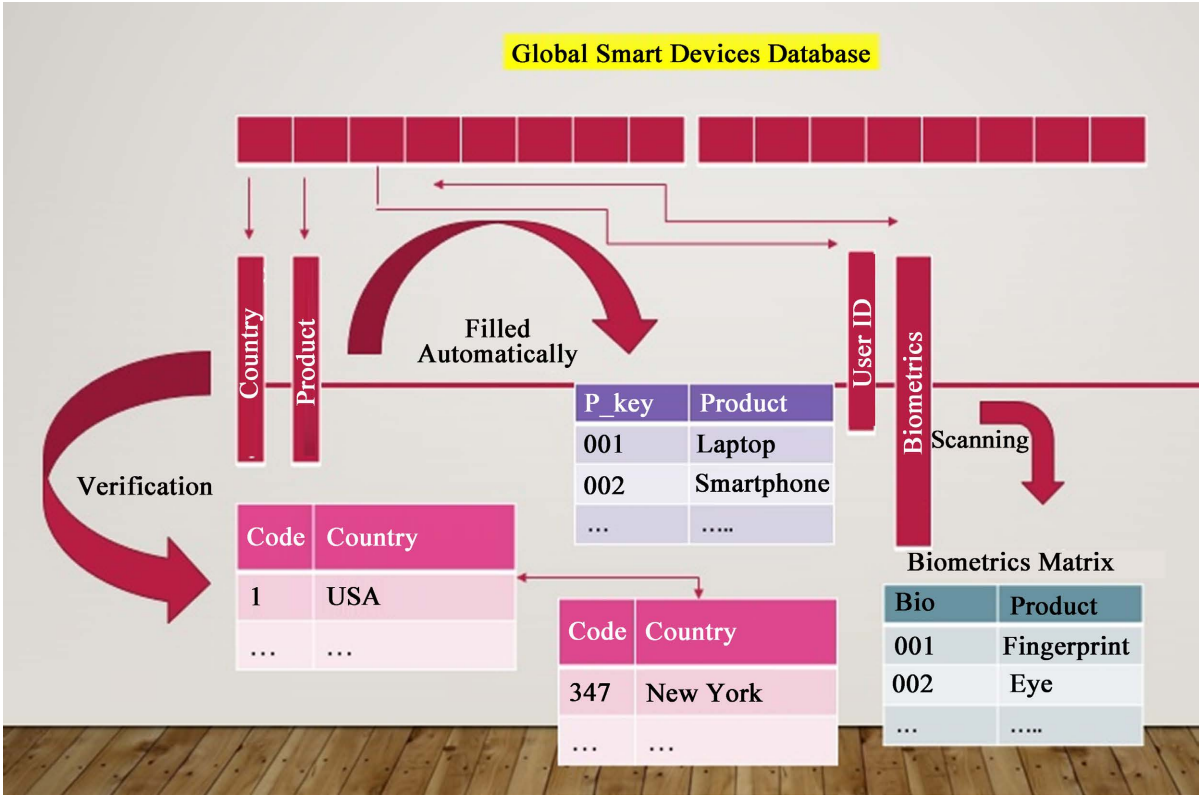

Figure 3. Global data base of smart devices.

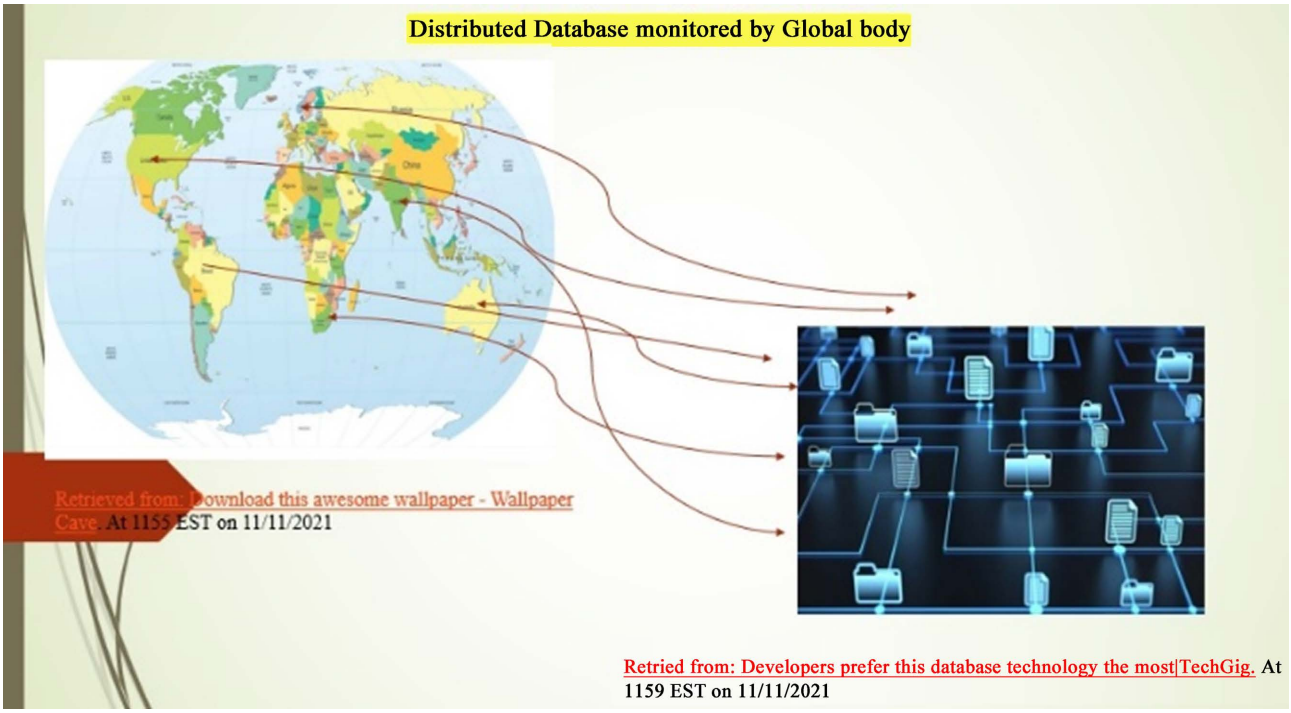

Figure 4. The electronic biometric distributed data bases.

5. Conclusions

The criminal is always one step ahead of the security man. The world has developed critically in the past eight decades, and some people think of an invention and find it the next day in the market, so we say that we live in the future in our present.

A man was known by his name, and this is the first biometrics. Now the names are not enough, and several other biometrics have appeared to reveal the identity of this "name! With scientific and technical development, verification methods have developed, but forgery and hacking are a hypothesis that always exists." Nowadays, the criminal is no longer that ugly, strong, muscular man who may be stupid, but rather a young man and perhaps a handsome, intelligent teenager "scientist" who manages his crimes from a distance from some room on this planet. Therefore, the race between the criminal and the protection systems continues, whether in ordinary or electronic crimes. We expect to see a new invention that aligns digital biometrics with human biometric identifying adults.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Laarfi, A. (2020) Framework for Reasoning with Speech Processing. Institute of Technology (FIT). https://repository.lib.fit.edu/handle/11141/2675/browse?type=author&value=Laarfi%2C+Ahmed

[2] Laarfi, A. and Kepuska, V. (2020) Implementation of a Verbal Compiler: The Need to Develop Audio Language to Keep Pace with Rapid Development Becomes a Necessity. *Global Journal of Human-Social Science*: *G Linguistics & Education*, 20. https://doi.org/10.34257/GJHSSGVOL20IS4PG1

[3] Laarfi, A. and Kepuska, V. (2020) Constructing a Simple Verbal Compiler. *International Journal of Intelligence Science*, **10**, 83-91. https://www.scirp.org/journal/paperinformation.aspx?paperid=102924 https://doi.org/10.4236/ijis.2020.104006

[4] Scheirer, W.J. and Boult, T.E. (2007) Cracking Fuzzy Vaults and Biometric Encryption. *Biometrics Symposium*, 11-13 September 2007, Baltimore. https://doi.org/10.1109/BCC.2007.4430534

[5] Harinda, E. and Ntagwirumugara, E. (2015) Security & Privacy Implications in the Placement of Biometric-Based ID Card for Rwanda Universities. *Journal of Information Security*, **6**, 93-100. https://doi.org/10.4236/jis.2015.62010

[6] Laarfi, A. (2020) Life: A Huge Archive Electronic Archive Has Become an Urgent Necessity in the Face of Enormous Technological Advances. *Journal of Computer and Communications*, **8**, 1-10. https://doi.org/10.4236/jcc.2020.84001