Article **Journal Industrial Engineering**
June 2021, Vol.5 No.14 27-34

Biometric technological security for data and information protection

Seguridad tecnológica biométrica para obtener datos y protección de la información

DOMÍNGUEZ-HERNÁNDEZ. Juan Pablo†*, CRUZ-GÓMEZ, Marco Antonio, TEUTLI-LEON, Margarita and POSADA-SANCHEZ, Ana Elena

Benemérita Universidad Autónoma de Puebla, Faculty of Engineering, Tribology and Transportation Group, Academic Body 189 Disaster Prevention, College of Mechanics and Electrics, Blvd. Valsequillo corner San Claudio Ave. Ciudad Universitaria. Col. San Manuel. CP.72570, Puebla Mexico.

ID 1st Author: *Juan Pablo, Domínguez-Hernández* / **ORC ID**: 0000-0001-5569-3869, **Researcher ID Thomson**: RID-14265 **CVU CONACYT ID**: 1104893

ID 1st Co-author: *Marco Antonio, Cruz-Gómez* / **ORC ID**: 0000-0003-1091-8133, **Researcher ID Thomson**: S-3098-2018, **CVU CONACYT ID**: 349626

ID 2nd Co-author: *Margarita, Teutli-León* / **ORC ID**: 0000-0002-8799-8891**, Researcher ID Thomson:** AAL-8481-2021, **CVU CONACYT ID:** 120326

ID 3rd Co-author: *Ana Elena Posada-Sánchez* / **ORC ID**: 0000-0001-6328-2576**, Researcher ID Thomson:** S-8705-2018, **CVU CONACYT ID:** 543011

DOI: 10.35429/JIE.2021.14.5.27.34 Received January 25, 2021; Accepted June 30, 2021

Abstract

Technological systems based on biometrics are an effective and efficient method for human recognition, data collection, and information protection. The objective of the research is to analyze the security and privacy offered by these systems, which include signature recognition, facial recognition, iris pattern and fingerprint recognition. The mixed analysis methodology will help in implementing protection, showing the strengths and weaknesses of these systems. By differentiating itself as the best at present for data protection, by collecting important information of each human being, through elements that make this technology the most reliable, its description makes it clear that these systems will have a great impact, also renewable energies can be used in the infrastructure avoiding polluting agents. Emphasizing to remain as a precedent of research in information technology. Future generations will see that security is not just about passwords. Currently, the trend is to generate security through biometric traits.

Safety, Protection, Privacy

Resumen

Los sistemas tecnológicos basados en biometría son un método eficaz y eficiente para el reconocimiento del ser humano, la obtención de datos, así como protección de información. El objetivo en la investigación es realizar un análisis de seguridad y la privacidad que ofrecen estos sistemas dentro de los cuales destacan reconocimiento de firmas, facial o rostro, patrón del iris y de huellas dactilares. La metodología de análisis mixto ayudará en implementar protección, al mostrarse las virtudes y debilidades de estos sistemas. Al diferenciarse como los mejores en la actualidad para resguardo de datos, al recopilar información importante de cada ser humano, mediante elementos que hacen de esta tecnología la más confiable, su descripción permite dejar en claro que estos sistemas serán de gran impacto, asimismo pueden usarse energías renovables en la infraestructura evitando agentes contaminantes. Haciendo énfasis para quedar como antecedente de investigación en tecnología de la información. Generaciones futuras verán que no sólo la seguridad son contraseñas. En la actualidad se identifica que la tendencia es generar seguridad mediante rasgos biométricos.

Seguridad, Protección, Privacidad

Citation: DOMÍNGUEZ-HERNÁNDEZ. Juan Pablo, CRUZ-GÓMEZ, Marco Antonio, TEUTLI-LEON, Margarita and POSADA-SANCHEZ, Ana Elena. Biometric technological security for data and information protection. Journal Industrial Engineering. 2021. 5-14:27-34.

* Author's Correspondence (E-mail: juan.dominguezh@alumno.buap.mx)
† Researcher contributing as first author.

Introduction

Biometrics consists of measuring the characteristics of the human body in order to identify an individual. For this, a characteristic endowed with strong variability from one individual to another must be chosen. The need to increase security is a priority worldwide, not only for private companies but also for governments and public institutions. Because of this, intelligent biometric protection systems have become the main security option. *Royer, J (2007).*

On today's emerging technologies, the main emphasis has been focused on properties for device innovation, especially application to new biometrics advances in security. Where they select the electronic and electrical engineering materials for the design specifications and required service conditions of the component. The first step in the selection process requires a study of the application to determine its most important characteristics. Since selection of the electronic and electrical engineering materials are a key factor for design specifications and required service conditions of the component. Once the required properties are known, the appropriate design to be installed can be selected using established network data. *Francois, J (2006).*

Fingerprinting is among the top ten emerging technologies that will change the world according to a report by Massachussets Institute of Technology *[MIT] (2006).* The French biometrics researcher and creator of the FingerPrint fingerprint sensor, says that a key does not prove that a certain person is the one who should have access to something". Biometrics fills that void, such a system verifies identity, since it is unique and unrepeatable, so there is no way to lend it out or lose it.Fingerprint recognition margin of error in the device is related to where the user's biometric data is stored, although it is being considered a minor error in this prototype. *Royer, J (2007).*

Methodology

This research has a mixed analysis approach defined on the differences between quantitative and qualitative technologies, using systematic processes, as well as recorded and estimated data.

The main idea to highlight in its performance is the security and privacy that devices for biometric recognitions offer. The quantifiable data will show the field they have covered over time, including recognition of the units that have this technology. The concepts and background that show the efficiency of a biometric system are supported by the historical files that are created when processing new credentials, files which are the basis for the development of the theory being related to providing a signature; therefore, through photograph or fingerprints it is created an identity, leaving it registered in a unique identification memory for each human being. The scope of the benefits associated to the performance generated in security systems based on the unique traits of individuals, is astounding, as each device is unique, efficient and secure, especially those for exclusive use. Within the research, the most outstanding systems were considered positively, because they are very useful, in terms of data protection. From the data obtained by the biometrics in developments, both quantitative and qualitative, a discussion of findings is generated about the implementation, these systems work, in favor of security, privacy, but above all in data protection. The role played by biometrics for specific cases in society different accesses either to goods and/or services is simple, since each system is adapted to the needs of the utility to be used. Thanks to the existing variants, it can be affirmed that there is a solution in all areas and problems related with each biometric recognition, mainly because it is being unique and unrepeatable, also variations are implemented in the system to avoid errors and thus be more reliable

Face or facial recognition

Currently there are many source codes, that allow a facial analysis in a simple way, the same way as those implemented in social networks, or latest smartphones. The facial recognition is taking over the market, since it has a great utility the use of this technology, which should be promoted, to help public institutions housing a large presence of older adults who by their jobs or lifestyle have lost their fingerprints, putting in doubt and even denying their identity, because the system does not recognize them, however facial recognition will help in identifying the individual.

ISSN 2523-0344

Without neglecting the great advantage that this technology will provide, it is advisable to update year after year, as people get older, because ageing it is giving rise to the limitation that personal traits do not match, but that is in very extreme cases. *Moctezuma, O. (2016), Utreras, P. (2021)*

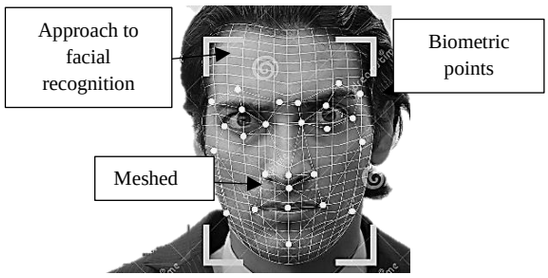

Figure 1 Generation of algorithm for facial recognition
Source:(Emmitroshin ID 179776613, dreamstime.com)

Currently there are many source codes, already developed that allow a facial analysis in a simple way as those implemented in social networks, high-end phones, taking over the market, since it has a great utility in proposal by which the use of this technology should be promoted, to help public institutions in which they have a large presence of older adults who by their jobs or lifestyle lose their fingerprints, putting in doubt and even denying their identity, the system does not recognize them, however under facial recognition will help in identifying the individual. It is advisable to update year after year, as we get older, giving rise to the limitation that our traits do not match, but that is in very extreme cases, without neglecting the great advantage that this technology will provide. *Moctezuma, O. (2016), Utreras, P. (2021).*

Signature recognition

The handwritten biometric signature, made on tablets or smartphones can collect biometric aspects, such as stroke, pressure or speed, which together make a unique signature, unequivocally associated to only one user. This type of technology guarantees the integrity of the signed content, since it ensures that it has not been altered or changed since it was signed. It is the less problematic biometric technology, currently the most widespread in the world, among other advantages, because it is very economical being implemented. *Diaz, V. (2013), Ponce, W. (2021)*

In addition, it should be considered in modern life and current situations where this electronic signature is required. The social isolation has led directly to the use of this tool, which turned out to be very useful, avoiding crowds for public institutions, the response is immediate, also it has the same validity as going for a seal or signature, in the same way there is a contribution in sustainability since do not use paper, therefore pollution will decrease, it is clear that everything is digital, nothing is printed, you should only see detail by detail the great benefit it will make in streamlining procedures, seals, document validation even the agility gotten in terms of response. *Diaz, V. (2013), Mendoza, M. (2021).*

Iris pattern

Iris recognition belongs to the static biometrics, since it is a measurement of physical characteristics in people, it is a secure method, with a 95% reliability rate (a high one), because it accounts for about 266 unique points, while most biometric systems have about 13 to 60 different characteristics. Each eye is unique and remains stable over time and in different climatic environments. *Cortes, O. et. al. (2010).*

A description of a reference mesh is shown in figure 2 with only a few points to consider, in reality it is more extensive, but it is useful to show the approaches that are made to measure the distance, the lines that are perceived belongs to the recognition algorithm. Also, there is a circumference, which corresponds to the approximation made by the iridology camera for taking a shot of the analyzable features. *Cortes, O et. al. (2010).*

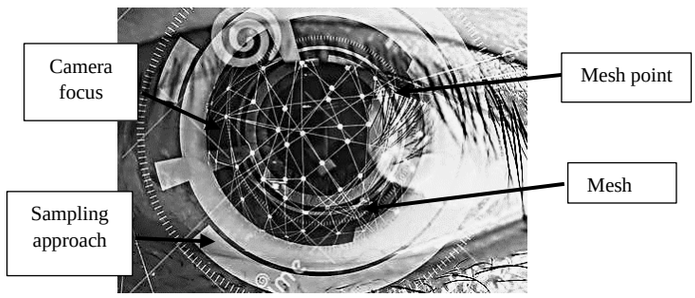

Figure 2 Meshing to obtain the iris pattern
Source:(Bodlennon ID 125922760, dreamstime.com)

ISSN 2523-0344

Fingerprint recognition

This biometric identification method is chosen by excellence, because it is easy to acquire, use and enjoys great acceptance by users. The use of fingerprints to establish a person's identity was originated in the mid-19th century, pioneered by Sir William Herschel. Fingerprint identification is based primarily on the location and direction of terminations, ridges, bifurcations, deltas, valleys and ridges. Figure 3 shows the different lines from which data are taken for single use. *Cortes, O et. al. (2010).*

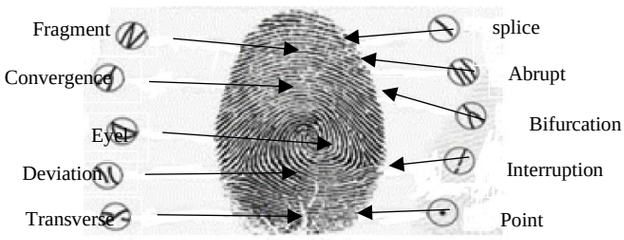

Figure 3 Fingerprint traces
Source: Cortés, O et.al. (2010)

The fingerprint is one of the most used methods to decrypt a device, it serves as an opening and closing method in any system where its installation is needed, that is why it is one of the most used in security matters. *Cortes, O. et. al. (2010).*

Structure of a biometric system

Biometric devices have three basic components. The first deals with analog or digital data acquisition by highlighting some biometric indicator on a person, such as the acquisition of fingerprint images by means of a scanner. The second handles factors like compression, processing, storage and comparison of acquired and stored data. The third component establishes an interface with applications located on the same or another system. Figure 4 shows the flow chart structure which is composed of two modules: registration and identification. *Cortés, O et.al. (2010).*

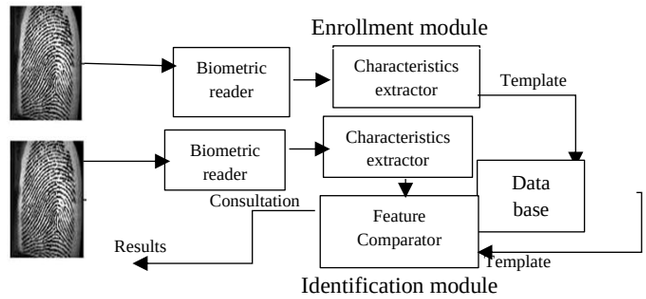

Figure 4 Data record structure
Source: Cortés, O et.al. (2010)

The biometric reader is responsible for acquiring data relative to the chosen biometric indicator and delivering a digital representation of it. The feature extractor takes the representative features of the indicator from the output to the reader. These are stored in the database. The enrollment module is in charge of acquiring and storing signals coming from the biometric reader in order to be able to match a captured signal with the one provided in subsequent entries to the system. Otherwise, the identification module is responsible for the recognition of individuals. The resulting representation is known as a query and it is sent to the feature matcher, which is responsible for matching the query against one or more templates to establish the identity of the person. *Boulgouris, N et.al. (2005).*

Institutions in Mexico using biometric technology

Both public and private institutions have done use of information provided by people, the data are considered confidential and public agencies have taken the lead for digital processing. In any service that it is used to establish personal identity such as credentials, they must comply with a series of requirements, which range from taking photos, signatures and even get fingerprints. *Díaz, V. (2013).*

Therefore, once it is created a historical file as a citizen of Mexican nationality, the personal information appears in the government system. Information includes hospitals and state headquarters, that are the only ones authorized to access the official information that is in the database, with the compromise of using it safely and reliably. There will be those who ask where they get all our information from, we only have to look back to the past, remembering when a photo, signature or fingerprints are provided, thus identifying that all records are analyzed and stored.

ISSN 2523-0344

Table 1 shows examples of documents where the information is related to biometric data, since they are mandatory as requirements in procedures and services of public institutions. *Díaz, V. (2013), Cando, S (2021).*

Institution	Fingerprint	Iris	Facial recognition	Electronic signature
INE (Instituto Nacional Electoral)	Yes	/	Yes	Yes
Visa Processing	Yes	Yes	Yes	Yes
Passport Processing	Yes	/	Yes	Yes
Military ID	Yes	/	Yes	Yes

Table 1 Data and institutions using biometric technology
Source: Procedures and services of public institutions (2020)

Implementation of a fingerprint reader using visual studio

Example of a biometric fingerprint reader

A fingerprint reader (model No. URU2S-U) was used to implement the biometric reader. This device connects to the computer via USB port and is compatible with a wide range of Windows operating system versions. It is easy to install and has a compact and modern design that facilitates its use. Figure 5 shows the fingerprint reader implemented in the published work of *Cortes, O. et.al. (2010).*

Figure 5 Fingerprint reader U.are.U2000
Source: Windows SDK .NET, Digital Person Database

Software development

The portable board for Windows SDK .NET Edition was used for fingerprint processing. This application is a software development tool that allows programmers to integrate fingerprint biometrics into a broad set of operating system applications.

The implemented program performs the following processes and functionalities:

- Enrollment. This point captures a person's fingerprint four times. After capturing the fingerprint, it will perform its extraction on the characteristics of the digital fingerprint features; then it creates a template for the captured fingerprint, and finally it performs the storage in the template for later comparison.

- Verification. The process of comparing a captured fingerprint with a fingerprint template to determine if the two matches.

- De-enrollment of a fingerprint. It is the elimination of a fingerprint template associated with a previously enrolled fingerprint.

Figure 6 shows the form that the Visual Studio program provides the output for the processing of a fingerprint.

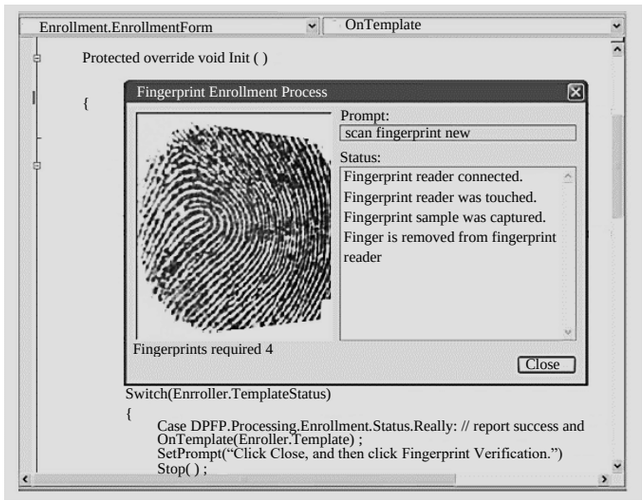

Figure 6 Fingerprint Enrollment Process
Source: Visual Studio Version 1.6 (2021)

Discussion of Results

Nowadays data acquisition is always done with previous consent of the user. Although, usually data have been provided before without having a clear idea of what providing information means, and the bewilderment have come evident when the information is made public.

ISSN 2523-0344

Legal concerns can be found in the Article 15 of the National Registry of Mobile Phone Users, a law whose purpose is provide a legal frame to stop crimes such as extortion, kidnapping or bank fraud; in this sense the reform contemplates fines of up to ninety thousand Mexican pesos for those who fail to register their line, and fines go higher for people who provide false data; although there is concern since legislators mention that they violate human rights, in terms of privacy invasion and obtaining personal data, incurring in an administrative offense for those who request this information.

A clear example is obtaining a digital ID card, using biometric technology. Although people have the right to an identity from birth, there are countries where they have never used an identification card, as it is the case in other countries looking to promote inclusion to exert civil, political, economic and social rights. On the other hand, in Mexico citizens have a multiplicity of documents, credentials and passwords that are required in different situations to have access for multiple services and rights, but without reliability for proving their identity. The ideal record should contain, at least: main name, surname, Unique Population Registry Code (Clave Única de Registro de Población, CURP). The right to identity is enshrined in Article 4 of the Mexican Constitution, which establishes that all Mexicans (including residents of other countries), minors and foreigners residing in the country have the right to an ID having a photograph, place of birth, signature, fingerprint, iris and voice. The right to identity is enshrined in the fourth article of the Constitution. Identity is the set of traits, attributes of the person, which characterize him/her, distinguish him/her from other individuals, and constitute him/her as a subject of rights and obligations.

The implementation of biometric technology will help to provide faster care in private and public centers, for instance, when someone suffering accidents or mishaps, they will no longer be unknown since hospitals are the front line of being able to use information to report those events.

It is also important to mention that biometrics it is a sustainable and very efficient technology, since it does not pollute the environment, as in the case of online procedures, since it avoids the use of paper, and if energy is needed, it can be obtained through solar panels or include rechargeable batteries. The companies that create these systems must use equipment that is not disposable, on the contrary, their designs must be environmentally friendly, reusable, but above all systems must be easy to use, with a plus input since it will also generate jobs, for those persons in charge of taking biometric samples.

It is of outmost importance to continue in favor of the contribution represented by biometric systems implementation, since using it is promoting innovation in technology. However, two of the most particular cases being served are banking and mobile telephony, mentioning. At present it is also useful to provide the requested information, with the confidence that no one else will be able to use the data given to these institutions. Although the scenario becomes quite strange due to fear that the encrypted information is downloaded, and then used as a way of extortion or illicit movements, it is well known that the user will have support to track any movement, verify the location where their documentation was used, since biometrics is so efficient, there will be no doubt of the progress that is reaching the population. It is clear that the law was passed quickly, although it was prepared with great wisdom, patience, but above all with the inclusion of supporting the creation of servers that provide security to the population in general. It is clear that the law was passed quickly, although it was prepared with great wisdom, patience, but above all with the inclusion of supporting the creation of servers that provide security to the population in general. It is clear that the law was passed quickly, although it was prepared with great wisdom, patience, but above all with the inclusion of supporting the creation of servers that provide security to the population in general.

As it was based on democracy, it was submitted to a vote, in which the competent authorities participated, resulting in 54 votes in favor, 49 against and 10 abstentions, which shows how close the decision was taken, leaving even more doubts as to whether the right thing is being done.

ISSN 2523-0344

In public opinions, this method of obtaining data is considered unconstitutional and a violation of human rights, which favors a system of surveillance and harassment with an authoritarian character, unworthy of a democratic country, only countries like China, Tajikistan, Saudi Arabia, Afghanistan, Venezuela have this type of records. It is not that Mexico is proposing to be the same; what is being promoted is a modern, up-to-date country, but above all, one of the safest.

Conclusion

Biometric technology has proven to be a reliable and efficient system, therefore in matters of security, data protection and identity will be technologically something that will revolutionize the world in terms of safeguarding information, but also as an identification method, people should take a look at their cell phone, which is wrapped in a series of high-end engineering technologies. At first glance unlocking by fingerprint recognition, the owner accesses the information, thus giving a proof on how a biometric system works and is becoming more and more a fact from the engineering point of view, where the research is pointing out to reliable security factors to ensure the security in different spheres like international, cultural, social, political and geopolitical without leaving any individual vulnerable

Acknowledgments

I am grateful for their support to the Faculty of Engineering BUAP; Tribology and Transportation Group; Academic Body 189 Disaster Prevention and Sustainable Development. To our families, who in general do not understand our projects as much as we do, the long hours sitting in front of the computer, or our delays in eating, doing or postponing other activities, thank you for your patience.

References

Karami, N., Moubayed, N., & Outbib, R. (2017). General review and classification of different MPPT Techniques. Renewable and Sustainable Energy Reviews, 68, 118. https://doi.org/10.1016/j.rser.2016.09.132

Tutorial biometría, [On line] available at: http://tutorialbiometria.galeon.com/pages/sistemas.html (Accessed April 16, 2021)

One Touch® for Windows® SDK .NET Edition Versión 1.6 in [online] available at: http://www.digitalpersona.com/Biometrics/SDKProducts/One-Touch-for-Windows-SDK/OneTouchfor

Sistemas biométricos: Matching de huellas dactilares mediante transformada de Hough generalizada [online] available at: http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm (Consultado el 16 de abril de 2021)

Karami, N., Moubayed, N., & Outbib, R. (2017). General review and classification of different MPPT Techniques. Renewable and Sustainable Energy Reviews, 68, 1–18.

Moctezuma-Ochoa, Daniela Alejandra. Re-identificación de personas a través de sus características soft-biométricas en un entorno multi-cámara de video vigilancia. *Ingeniería Investigación y Tecnología*, XVII, 02 (2016): 257-271.

N. Boulgouris, D. Hatzinakos, and K. Plataniotis. Gait recognition: a challenging signal processing technology for biometric identification. *IEEE Signal Processing Magazine*, 22(6):78–90, Nov 2005.

A. Jain and A. Ross. Introduction to biometrics. In A. Jain, R. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society*, pages 1–42. Springer, 2008.

H. Thang, V. Viet, N. Dinh, and D. Choi. Gait identification using accelerometer on mobile phone. In *2012 International Conference on Control, Automation and Information Sciences (ICCAIS)*, pages 344–348, Nov 2012.

N. Clarke and S. Furnell. Authentication of users on mobile telephones–a survey of attitudes and practices. *Computers & Security*, 7(24):519–527, 2005.

Díaz Rodríguez, Vanessa, Sistemas biométricos en materia criminal, Instituto de Ciencias Jurídicas de Puebla A. C. Puebla, México, un estudio comparado enero-junio, 2013, pp. 28-47.

ISSN 2523-0344

Cortés Osorio, Jimy Alexander; Medina Aguirre, Francisco Alejandro; Muriel Escobar, José A. Sistemas de Seguridad Basados en Biometría Scientia Et Technica, Universidad Tecnológica de Pereira Pereira, Colombia diciembre, 2010, pp. 98-102.

Jorge Bravo, Por fin tendremos cedula de identidad, El Economista, 11 de diciembre 2020

A. Jain and A. Ross. Introduction to biometrics. In A. Jain, R. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society*, pages 1–42. Springer, 2008.

M. Ehatisham ul Haq, M. Azam, J. Loo, K. Shuang, S. Islam, U. Naeem, and Y. Amin. Authentication of smartphone users based on activity recognition and mobile sensing. *Sensors*, 17(9):1–31, 2017.

Li, B. Y., Mian, A., Liu, W., Krishna, A. (2013, January). Using kinect for face recognition under varying poses, expressions, illumination and disguise. In Applications of Computer Vision (WACV), 2013 IEEE Workshop on (pp. 186-192). IEEE.

F. J. Silva-Mata, D. Muñoz, S. Beretti, V. Mendiola-Lau, I. Talavera., N. Hernández, y. M. Diaz (2016) Alineación de Señales e imágenes durante la aplicación del Análisis de Datos Funcionales, RCF Vol33-1E.

Cando-Segovia, M. R., & Chicaiza, R. P. M. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. 3C TIC. Cuadernos de desarrollo aplicados a las TIC, 17-41.

Mendoza García, M. P. (2021). Protección de datos y herramientas tecnológicas para la prevención del Covid-19: análisis a la luz de dos modelos contrapuestos (España vs Emiratos Árabes Unidos).

Utreras Logacho, P. L. (2021). Gestión de identidad digital de usuarios en servicios web para la protección de la privacidad de la información (Doctoral dissertation, Ecuador-PUCESE-Escuela de Sistemas y Computación).

Ponce Hernández, W. (2021). Mecanismos de protección de la privacidad de los ciudadanos aplicados a la firma manuscrita biométrica.

Moncada-Jiménez, J., Salicetti-Fonseca, A., Carazo-Vargas, P., & Morera-Siércovich, P. L. (2021). La recolección, utilización y almacenamiento de datos biométricos sensibles en deportistas: insumos para la carrera de Educación Física. Revista Educación, 45(1), 640-652

ISSN 2523-0344