BIOMETRICS AS A METHOD OF COMBAT WITH COVID-19

Omarova Madina Djalalovna
postgraduate
Dagestan State University
Makhachkala, Russia
Mutayeva Saida Ibragimovna
Candidate of Philological Sciences, Associate Professor
Dagestan State University
Makhachkala, Russia

Abstract. The main purpose of the following work is to study the ways of reducing the spread of COVID-19 and ending the pandemic. The article presents the benefits and drawbacks of biometrics and some examples of its use in different countries.

Today, biometrics has already become an integral part of the global information technology market and it is used as a convenient and reliable mechanism to ensure information security.

Biometrics is used for identification, authentication, and authorization which are three sequential processes inseparably linked. During identification, we present the system with a unique sample as an identifier, after which the system compares this sample with the template stored in the database, and authentication takes place. If the presented sample matches the template, the user is granted access with a certain set of rights, and authorization occurs.

Keywords: biometrics, identification, contactless technologies, security, health, COVID-19.

Introduction

Biometric authentication is a method of authentication based on the presentation of unique biological characteristics of a person: fingerprint, retina or iris of the eye, face geometry, palm shape. Biometric characteristics also include the shape of the ear, body odor, heartbeat, the pattern of veins on the hands, DNA which are also unique biometric identifiers of a particular person. In short, biometric authentication means that your body becomes the key to access.

In practice, biometric authentication methods have been effectively used in many industries including the military, law enforcement, finance, and e-commerce. They are also used by developers of mobile devices and computers as an alternative to password protection. Biometric authentication methods are actively implemented by banks, providing customer service without presenting a passport, allowing you to link your biometric data to a personal account and make purchases without a bank card or gadget but by face recognition. Facial recognition systems are used in public places, airports, train stations, and they allow law enforcement agencies to fight crime. Biometric data is embedded in electronic passports in many countries around the world.

Today, the issue of switching to contactless technological solutions such as contactless analysis of fingerprints, retinas, voice and behavioral characteristics, and their combination, is particularly acute. Due to these technologies, we can not only verify identity and access many financial, government and other services, pass through airport and railway station security, receive money from ATMs but also protect the health of the population and reduce the risks of COVID-19 spread.

Market experts estimate the global segment of contactless biometric technologies at $6.92 billion in 2019 and forecast an annual growth of 20.3% in the period between 2020 and 2027. A great future for the development of contactless biometrics is seen in the areas of commercial security, public and private sector including the field of payment services.

Benefits

Firstly, it's convenient as the user does not need to remember complex passwords, carry some kind of key card. It is enough to show a finger, eye, ear or face, and access will be obtained. Biometric data is always with you, it is impossible to lose or forget it.

Secondly, biometric data is not as easy as a key or password to steal. At first glance, biometric authentication solves the problem of weak passwords, which according to statistics, 80% of cases are the cause of account hacking.

Thirdly, the use of biometric authentication reduces the likelihood of a virus infection through the PIN pad.

Fourthly, the use of biometric authentication complicates remote hacking. Even knowing the password, an attacker will not be able to gain access to the target system or device if two-factor authentication is configured where biometric data acts as an additional identifier.

Drawbacks

Despite these advantages, biometric authentication methods are associated with certain risks and threats:

Biometric "spoofing". Spoofing is the practice of deceiving a security system by using fake or copied information, particularly biometric information. For example, you can take a picture of a fingerprint from an object and copy it. A fake fingerprint can be used to unlock a mobile device or payment system by allowing attackers to gain access to the user's data and bank account.

Facial recognition systems often used to protect smartphones or tablets are also vulnerable. There are some known cases when the devices protected with their help could be unlocked by simply showing the owner's photo.

Biometrics Application in Different Countries

Sweden

One of the most exciting new areas we are observing is the growing potential of biometric access applications, especially in smart homes and workplaces.

While improving workplace security and remote work has been a long-standing priority for many organizations, the past year has certainly reinforced the need for more secure and convenient access. Biometric access cards with on-card authentication are the examples of increasing security, convenience, and hygiene when entering shared workspaces. Contactless biometric authentication by using the face, iris, or a combination of the two is another convenient means to safely enter buildings and busy hygienic spaces such as hospitals.

Meanwhile, biometric authentication is in high demand as a more convenient and secure authentication method for both consumer and enterprise PCs. The study found that the majority of consumers (66%) are tired of pins and passwords, and 51% would prefer to use biometric data for authentication. By 2026, it is estimated that approximately two-thirds of the 260 million PCs shipped annually will have a touch-sensitive fingerprint sensor.

USA

In early April 2021, it became known that the US Army had been developing a new system of biometric cameras for recognizing the faces of the military. The new software will compare images taken by the camera with a pre-created gallery of approved faces.

The new method will combine a one-to-one identification algorithm to compare a new image with already known photos of a given person, and a one-to-many identification algorithm that compares the resulting image to a broad database in search of a specific person. For army checkpoints, this will be an important factor. The Army intends to introduce the new cameras as a result of working with small businesses as part of a phased development program.

France

Entering 2021, biometric payment cards are no longer beyond the reach, they are actually available with major commercial deployments by French banks BNP Paribas and Crédit Agricole.

The momentum has been steadily gathering pace for several years but it has undoubtedly gained further popularity as a truly contactless, hygienic and secure payment method against the backdrop of current public health measures around the world. Studies show that nowadays a third of consumers when paying in the store are worried about infection from PIN-pads.

Existing biometric technologies

Some of the biometric authentication technologies listed below can be used on a daily basis. Others may be less common. The four most common uses of biometric authentication technology in the modern world are done below:

– Fingerprint recognition uses a person's unique fingerprint to verify their identity. This is one of the most common biometric authentication technologies which is used to protect everything from mobile devices to cars and even buildings.

– Face recognition uses a person's unique facial anatomy to identify them. It is used in a wide variety of places such as smartphones, identity verification for credit card payments, and etc.

– Retinal recognition uses a unique retinal pattern for identification. This type of biometric authentication is more difficult to implement because the scan requires an infrared light source, a camera, that can see infrared radiation and minimal light pollution to ensure accuracy. However, it is one of the most accurate biometric authentication systems available under these conditions. Therefore, it is usually used in situations where security is most important.

– Voice biometrics or voice recognition uses the unique tone and frequency of someone's voice to authenticate them. Today, it is most often used to verify users when they contact a call center for customer support.

New biometric technologies

The two methods of biometric authentication listed below have not been widespread yet, but they are gradually becoming more common:

– Gait recognition allows you to identify a person by the way they walk. Since each person walks a little differently, the way they put one foot in front of the other is an effective way to confirm their identity. We expect gait recognition to become more common in the future as forms of continuous authentication become more popular.

– Vein Recognition: Vein recognition uses a unique pattern of blood vessels on a person's hand (or finger) to identify them. It uses infrared light to map the veins under the skin on the hands or fingers. Vein recognition is extremely accurate, even more accurate than the retina, and it is one of the most advanced biometric identification systems to date.

Conclusion

The field of biometric authentication is promising and rapidly developing, and the number of research and development in this area is growing every year. However, these methods are imperfect and there is always the possibility of errors. It is worth carefully studying all the pros and cons before using biometrics in order to protect your confidential data and money.

The pandemic has given a powerful impetus to the development of contactless technologies including the field of biometric identification. If previously remote recognition of a person by retina, face geometry, voice, or other unique biometric parameters seemed an unreasonably expensive solution, now consumers are willing to install such systems in order to save the business from much more serious costs inevitable in the case of a mass COVID-19 infection of personnel.

In 2020, equipment and software sales for contactless biometrics began to grow and according to experts, it will last for a long time. Thus, according to Markets and Markets, the global market for facial recognition systems will reach $ 7 billion by 2024 with an average annual growth rate of 16.6%.

Reference:

1. Biometrics against the pandemic: website URL: https://www.kommersant.ru/conference/649 (accessed: 11.04.2021). - Text: electronic.
2. 2020. A perfect storm in the biometrics market: site URL: https://plusworld.ru/daily/cat-security-and-id/2020-idealnyj-shtorm-na-rynke-biometrii/ (accessed 11.04.2021). - Text: electronic.
3. Biometrics and Information security: website URL: https://safe-surf.ru/users-of/article/659637/ (accessed: 11.04.2021). - Text: electronic.
4. The US Army introduces a system of facial recognition of the military at the checkpoint. https://www.tadviser.ru/index.php