VOICE IDENTIFICATION SYSTEMS

[1]Fayzieva Dilsora Salimovna, [2]Yuldasheva Nafisa Salimovna
[1]PhD, Tashkent university of information technologies
[2]Doctoral student, Tashkent university of information technologies
https://doi.org/10.5281/zenodo.8395065

Abstract. *This article provides detailed information on the problems and methods of identification of a person based on biometric parameters, and it is presented that the identification of a person based on his voice is safe and inexpensive.*
Keywords: *identification, PIN code, acoustic and vibroacoustic.*

Nowadays, biometric technologies are widely used in various fields. In particular, it is used in areas such as internal affairs, access control and banking. Identification of a person is a very complex issue and it is based on a set of biometric characters. And the set of biometric characters is unique for each individual. This feature is also present in speech signals. Any person has his own important vocal characteristics, which are determined based on the individual structure of the vocal apparatus. A person can easily identify another person by their voice, but creating an automatic speech recognition system requires solving many complex problems. However, the emergence of effective methods of digital signal processing has significantly increased interest in this direction in the world.

The problem of access control is very relevant today. Most access control tools on the market are expensive and require the use of special personal identification techniques. For example, employee ID cards (magnetic, contactless), key chains, special labels, etc. The use of biometric identification allows to avoid technical identification means that can be lost, stolen or given to unauthorized persons.

Biometrics is the science of measuring and analyzing human biological factors. Voice biometrics is the measurement and analysis of the human voice. This technology relies on the principle that the human voice is as unique as a fingerprint, facial image and other biometric features.

The uniqueness of the human voice is related to its physical characteristics and speech characteristics. Using this feature, a person can be identified or identified by analyzing their voice. The user registers from the system by providing samples of his voice. Personal voice templates and a unique benchmark model are created based on the audio recording of the received voice samples. A model or template is called a fingerprint, as in a fingerprint. Voice biometric technology uses algorithms to analyze a person's speech and compare it to pre-created patterns to identify or verify a person. If there is a match between them, the voice biometric system verifies that the person is the person registered with their voiceprint.

Modern non-biometric methods use shared secret knowledge and physical tokens. Secret knowledge can be in the form of a PIN code, a password or an answer to a secret question. Physical tokens include key, ID card, security key fob, driver's license, passport, etc. Unfortunately, traditional methods are vulnerable to social engineering and protection. Tokens are usually copied or stolen. And passwords are often forgotten, left in plain sight, or stolen. In addition, tokens do not guarantee the exact identification of an individual.

In contrast, biometric data is more secure against copying, tampering, alteration or theft. Voice biometrics, on the other hand, is strong in terms of internal security, as it is not possible to reconstruct speech using a collection of voice characters. Even if a hacker were to find it, it would still yield information like a string of meaningless numbers that are functionally useless. Simply put, a model is built for each user based on their voice, and this model is numerical data.

The use of biometrics in combination with other methods results in strong multi-factor authentication. For example, having a mobile phone,

PIN knowledge and identity verification using voice biometrics is a secure way to reduce vulnerability to unauthorized access to systems and services.

In recent years, voice recognition systems have been widely used in various applications. Such systems allow the use of the human voice to control access to services such as automated banking, data (based on user access rights), or territory (government or research institutions). It is advisable to use a voice identification tool for access control devices in service buildings. Because the advantage of this solution is that its hardware and software support is much simpler and cheaper. All you need is a microphone and an analog-to-digital converter to get voice "traces", and almost all modern personal computers and mobile phones are equipped with these devices. The increase in the importance of personal identification systems based on the analysis of voice data is directly related to the speed of information transmission through telecommunication channels, the emergence of systems that allow managing various services through wireless mobile communication channels, and the possibilities of voice identification. Such tasks are important in the control of computer systems using voice commands and in the creation of automatic speech recognition systems.

The emergence of new and more sophisticated technical means for illegal access to voice data (for example, confidential conversations), the improvement of various technical channels for the dissemination of speech data, and the development of research on voice identification give rise to many specific aspects. In particular, new systems and methods of such identification are necessary in the development and testing of devices that protect speech information from leakage through acoustic and vibroacoustic channels, as well as in the assessment of protection against leakage.

The identification of a person based on his voice is closely related to the problems of forensics, such as the analysis of phonograms that preceded him, and such problems arise when it is necessary to identify an unknown voice recording during the investigation of crimes (for example, telephone conversations). Mathematical, technical methods and methods of identification are very effective in conducting phonoscopic investigations, that is, they help in important practical activities, such as searching for a criminal in the presence of sound recordings. It should be emphasized that modern computer crime primarily begins with remote access to data through wireless communication channels. This makes the investigation of computer crimes extremely complex and secretive in nature. In this case, criminals leave virtual traces, not material ones. Therefore, voice recognition systems can be important in the detection and prevention of computer crimes. Such systems can be widely used to solve the problems of voice signal analysis in telecommunication channels.

The degree of similarity between the base and test samples is determined based on distance or probability criteria. Usually, voice identification is done both with and without text. In this case,

identification is based on pre-prepared or system-generated text when text-dependent, and arbitrary text when independent of text.

In addition to fraud detection and risk reduction, voice biometrics has many benefits. However, from the point of view of fraud prevention, the presence of voice biometrics creates a psychological barrier for fraudsters, its use significantly complicates the fraudster's task, the results of its use mean that the business will suffer less from fraud. Hence, voice biometrics are highly effective in managing the risk of fraud.

Weaknesses in PINs, passwords and security issues can lead to the leakage of some public information in organizations and it can put customers at risk. Voice biometrics can reduce this risk and reduce fraud while offering a convenient user interface. However, the best solution is to combine voice biometrics with other methods to create reliable multi-factor authentication solutions that reduce the vulnerability of systems and services to unauthorized access.

Voice can be compared to other biometric data in many ways. Voice has some advantages, for example, the need to use a scanner to identify the user's iris and fingerprint is not required in voice biometrics.

Biometric identification systems based on the voice of a person are the most user-friendly authentication method, provide a high level of recognition and reduce costs by automating the process.

Compared to other identification methods, voice identification has relatively fewer requirements and is more user-friendly. It can easily be done remotely, for example, by phone. Voice recognition does not require the use of specialized expensive equipment, it is enough to have a microphone (now available almost everywhere, on computers, mobile phones). In addition, due to the ease of use of voice authentication, it is in high demand among users compared to other methods of biometric identification. In terms of accuracy, voice identification is generally on par with other methods, and is not inferior to fingerprint, iris, or face identification. Using voice recognition is convenient and reliable in low or poor lighting conditions.

The main advantage of voice is that it is the only biometric technology that can be used remotely through the device. This is particularly effective in unified call centers or self-service systems driven by an interactive voice menu, and in authenticating callers on an access platform. Similarly, it can be used to identify people who are contacting an organization's contact center. Nowadays, there are many cases where fraudsters impersonate bank employees and steal their information. In this case, the use of such technology allows to prevent such situations. The economic justification of using voice biometrics is explained by the following advantages, in particular, reducing the level of fraud and risk, reducing the cost of authentication, and improving the quality of customer service.

The benefits of enhanced security include less damage from fraud, reduced costs of pursuing fraudsters through the legal system, and savings in resources through lower compensation and indemnity payments.

And automating the authentication process makes the process simple and convenient for customers. In addition, eliminating the problem of asking the same secret questions every day will definitely have a positive effect on the mental state of the interviewees. Customers choose their security preferences. For example, they prefer to use voice biometrics rather than remembering their first pet (school / car, etc.).

REFERENCES

1. Лакин Г.Ф. Биометрия. 4-е изд., перераб. и доп.- М.: Высшая школа, 1990.-352 с.
2. H. Beigi. Fundamentals of speaker recognition. Springer US, 2011.
3. Матвеев, Ю.Н. Технологии биометрической идентификации личности по голосу и другим модальностям // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. — 2012. — № 3. — С. 46–61.
4. K. Sreenivasa Rao, Sourjya Sarkar Robust Speaker Recognition in Noisy Environments, Springer, 2014
5. Романенко В.О. Эмоциональные характеристики вокальной речи и их связь с акустическими параметрами // В.О.Романенко // Общество. Среда. Развитие (Terra Humana). – 2011. – № 3. – С. 124–127
6. Абдураззақов Ф.Б, Юлдошев Ю.Ш., Нуримов П.Б. Нутқ сигналларига рақамли ишлов бериш назарияси ва технологияси, Республика илмий-техник анжуманининг маърузалари туплами, ТАТУ, Ташкент, 12-15 март 2019й. Б. 16-18
7. Zoran Gacovski, Biometrics Authentication Methods, 2020, http://www.arclerpress.com.
8. Jain, A. K., & Ross, A. Introduction to Biometrics. Handbook of Biometrics, 1–22. doi:10.1007/978-0-387-71041-9_1
9. S. Z. Li and A. Jain. Encyclopedia of biometrics. Springer Publishing Company, Incorporated, 2 edition, 2015.
10. Замалиев А.И., Кирпичников А.П., Ляшева С.А., Шлеймович М.П. Текстозависимая идентификация и верификация диктора по голосу в системе контроля и управления доступом // Вестник технологического университета. 2016. Т.19, №17. –С. 138 –143.
11. J. H. Hansen and T. Hasan. Speaker recognition by machines and humans, a tutorial review. IEEE Signal Processing Magazine, pages 74–99, 2015.
12. K. Brunet, K. Taam, E. Cherrier, N. Faye, C. Rosenberger, Speaker Recognitionfor Mobile User Authentication: An Android Solution, https://www.researchgate.net/publication/257365356_Speaker_Recognition_for_Mobile_User_Authentication_An_Android_Solution,
13. Козлов А.В. Система идентификации дикторов по голосу для конкурса NIST SRE 2013 // А.В.Козлов, О.Ю.Кудашев, Ю.Н.Матвеев, Т.С.Пеховский, К.К.Симончик, А.К.Шулипа // Труды СПИИРАН. – 2013. – № 2. – С. 350–370.
14. Маматов Н.С., Нуримов П.Б., Самижонов А.Н. Автоматическая идентификация диктора по голосу, ПРОБЛЕМЫ ВЫЧИСЛИТЕЛЬНОЙ И ПРИКЛАДНОЙ МАТЕМАТИКИ №5(23) 2019