Sokolov Maxim Sergeevich
Student
Ural Federal University named after the first
President of Russia B.N. Yeltsin
Russia, Ekaterinburg
Academic supervisor: Ponomareva Elena Vladislavovna

FINGERPRINT AUTHENTICATION METHODS

Abstract. *The number of information systems in the world is growing rapidly and it is necessary to ensure security for each of them. Nowadays, everyone protects his confidential information, for example, in the smartphone. To protect it, fingerprints are used together with passwords. Due to the popularity of the fingerprint system in the secret objects and among ordinary users, cybercriminals invent new ways to bypass the system or deceive it. The purpose of the study is to compare fingerprinting methods for authentication and identify the most secure system, resistant to fake fingerprints and to the intruders.*

Keywords: *fingerprint, biometric systems, reliability, fake fingerprint, fingerprint scanner, fingerprint spoof detection.*

Соколов Максим Сергеевич
Студент
Уральский федеральный университет имени первого
Президента России Б.Н. Ельцина
Россия, г. Екатеринбург
Научный руководитель: Пономарева Елена Владиславовна

МЕТОДЫ СНЯТИЯ ОТПЕЧАТКОВ ПАЛЬЦЕВ ДЛЯ АУТЕНТИФИКАЦИИ

Аннотация. *В последнее время количество информационных систем в мире стремительно растет и для каждой необходимо обеспечивать безопасность. В современном мире каждый человек защищает свою конфиденциальную информацию, например, находящуюся в телефоне. Для ее защиты используются вместе с паролями отпечатки пальцев. Из-за популярности этой системы среди обычных пользователей и использования ее в режимных объектах, злоумышленники старательно изобретают новые пути обхода системы или ее обмана. Целью исследования является изучение безопасности различных методов сканирования отпечатков пальцев.*

Ключевые слова: *отпечаток пальца, биометрические системы, надежность, поддельный отпечаток пальца, сканер отпечатков пальцев, обнаружение подделки отпечатков пальцев.*

Introduction

The development of biometric technologies of person identification by an increasing number of objects and information flows that must be protected from unauthorized access, namely: forensic science; access control system; personal identification system; electronic Commerce system; information security (network access, PC login); time tracking and registration of visitors; voting system; the electronic payments; authentication on Web resources; various social projects that require identification of people; civil identification projects (crossing state borders, issuing visas to visit a country), etc. The modern world is characterized by increased requirements for security systems and one of the main directions of it is inventing effective personal identification devices and provides security of the authentication process.

Due to the popularity of the fingerprint system, cybercriminals invent new ways to bypass the system or deceive it. That’s why it is necessary to study the security of various fingerprint scanning methods.

Scanning methods

1. Implicit authentication method for smartphone users based on rank aggregation and random forest.

The most recent behavior-dependent methods rely on the assumption that individuals tend to have consistent and stable behavior profiles. There are many assumptions, which are to collect GPS data, accelerometer output, wi-fi networks and many other; or a system which is based on the behavior features related to the way a user's phone is picked-up or a method utilizing touchscreen events containing action, screen coordinates and timestamps.

Thus, there are many approaches to extend the typical user authentication. But some methods are not optimized and have a terrible performance. That's why there was developed a method to compare authentication approaches to choose the best one. Based on the result, a new approach that uses the fewer features than the others was developed. This method provides 97% accuracy (Fig. 1) which is not the best result, but using these fewer features means that the smartphone's limitations (i.e., memory size, battery life, and computational capability) could be addressed [1].

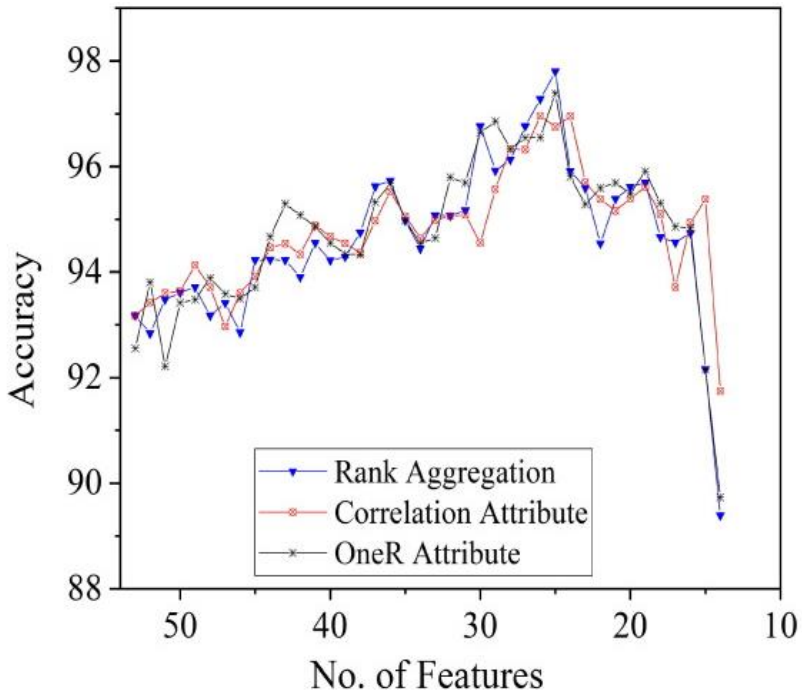

Fig. 1 - Classification accuracy rates and different number of features

2. Fingerprint liveness detection through fusion of pores perspiration and texture features

To detect the core points in valley regions there are some difficulties, such as dust, oil and impairments being on the glass surface of the optical sensor. Therefore, a post-processing step is required to generate the refined pore map. Next step is sorting on the basis of the intensity value to discard last 5% weak points.

This algorithm uses the neural network to enhance the training on fingerprint datasets and gets the positive results over 99.5% accuracy. This is the best result among the other methods [2].

3. Anti-spoofing method for fingerprint recognition using patch based deep learning machine

Failure in preventing the spoofing may compromise confidential information and methods of spoofing detection can be classified into two classes:

- Hardware-based – fingerprint reader takes fingerprints with high resolution and can track the features like blood flow, skin distortion and odor.
- Software-based – where algorithm rely only on input image.

A novel approach was created to determine fake fingerprints using Neural Network. This is a software-based method, which extracts the features from image and then extracts the features again and again while it is possible. This method is called Deep Boltzmann Machine (Fig. 2). Based on Deep Neural Network it aids to understand data in depth.

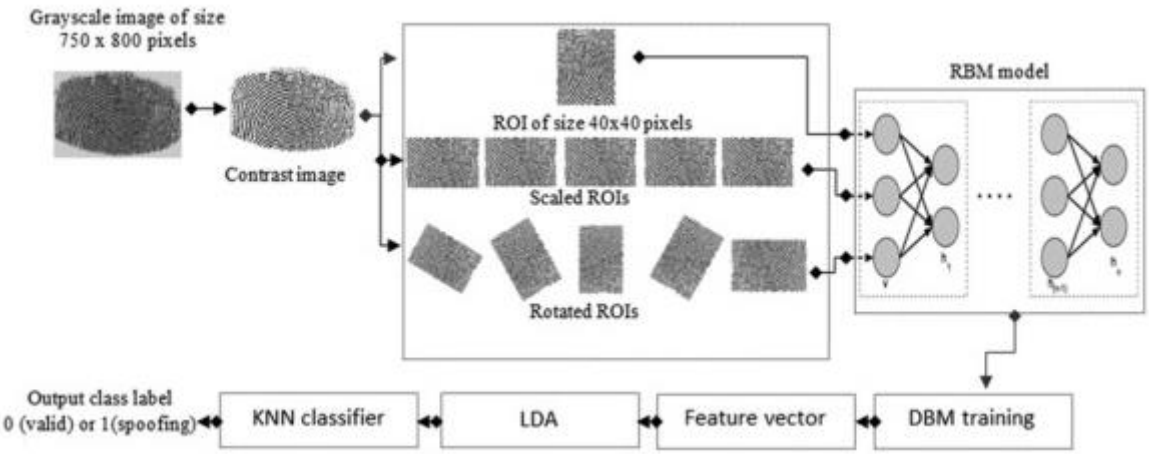

Fig. 2 - Framework of the method named Deep Boltzmann Machine

Various parameters were used to train the Neural Network to get the high accuracy. The results show us that in comparison with the other methods, this approach is the second by Average Classification Error metric [3].

4. A Novel Image Compression Based Method for Multispectral Fingerprint Biometric System

The approach uses Multispectral technology which collects multiple images of user in a single interaction. The images are captured under different illumination conditions with different wavelengths and different orientation. Then Wavelet Decomposition extracts the desired feature of the image and analyzes it based on the idea of expressing an image as a linear combination of specific function set called wavelet transform which is obtained by shifting and dilating one single function called Mother wavelet. Then it uses a compression technique called Huffman coding which will reduce the amount of memory by reducing the number of bits without losing the important data.

In other words the proposed system consists of two phases: Enrollment and Matching (Fig. 3). Enrollment includes fingerprint, wavelet transform and Image compressing Huffman coding. Then the template is stored in database. Matching also includes fingerprint, and Image compressing Huffman coding, then algorithm matches the resulting template and the templates from the database using a method called hamming distance. This method compares the parameters and makes the decision to give the access or not [4].

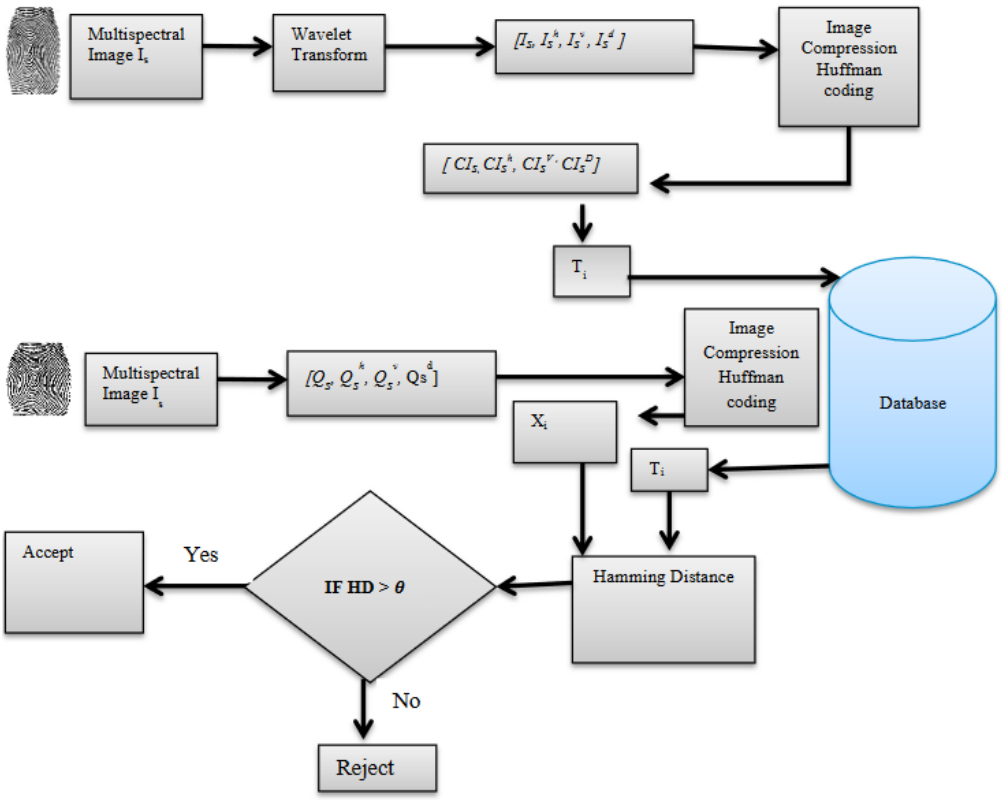

Fig. 3 - General framework of a system

Conclusion

In this paper we have focused on different methods of analyzing and matching the fingerprints and security which they provide. Identification system should provide not only the best accuracy but be oriented on system limitations too. The Fingerprint liveness detection algorithm yields an accuracy of over 99.5%, which makes this method the most secure but the Implicit authentication method provides the best performance with 97% accuracy. The methods can be combined into a system that provides fairly effective templates secure by novel image compression method and best accuracy by the Fingerprint liveness detection approach.

REFERENCES

1. Mohamed W. Abo El-Soud, Tarek Gaber, Fayez AlFayez, Mohamed Meselhy Eltoukhy. Implicit authentication method for smartphone users based on rank aggregation and random forest. – 2020. – Text: electronic. – URL:

https://www.sciencedirect.com/science/article/pii/S1110016820303902 (Reference date 15.12.2020).

2. Diwakar Agarwal, Atul Bansal. Fingerprint liveness detection through fusion of pores perspiration and texture features. – 2020. – Text: electronic. – URL: https://www.sciencedirect.com/science/article/pii/S1319157820304833 (Reference date 15.12.2020).

3. Diaa M. Uliyan, Somayeh Sadeghi, Hamid A. Jalab. Anti-spoofing method for fingerprint recognition using patch based deep learning machine. – 2020. – Text: electronic. – URL: https://www.sciencedirect.com/science/article/pii/S2215098619300527 (Reference date 15.12.2020).

4. Annu Sharma, Shwetank Arya, Praveena Chaturvedi. A Novel Image Compression Based Method for Multispectral Fingerprint Biometric System. – 2020. – Text: electronic. – URL: https://www.sciencedirect.com/science/article/pii/S1877050920311637 (Reference date 15.12.2020).