

**Sokolov Maxim Sergeevich**

Student

**Research advisor: Ponomareva Elena Vladislavovna**

Ural Federal University

Russia, Yekaterinburg

## **FINGERPRINT AUTHENTICATION SECURITY**

**Abstract:** *The development of biometric technologies of person identification is determined by an increasing number of objects and information flows that must be protected from unauthorized access. The modern world is characterized by increased requirements on security systems. 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. 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

Научный руководитель: Пономарева Елена Владиславовна

Кафедра иностранных языков и перевода

Уральский федеральный университет

Россия, г. Екатеринбург

## **БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ ОТПЕЧАТКОВ ПАЛЬЦЕВ ПРИ АУТЕНТИФИКАЦИИ**

**Аннотация:** *Развитие биометрических технологий идентификации личности обусловлено увеличением числа объектов и потоков информации,*

которые необходимо защищать от несанкционированного доступа. В современном мире предъявляются все большие требования к системам безопасности. Из-за популярности системы отпечатков пальцев 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.

## 1. Introduction

Until recently, various cryptographic techniques such as PIN-codes, graphic keys, passwords, for example, to unlock the smartphone (unlike the PIN-code is that you can specify a larger number of symbols) have been used to protect personal data. Such methods can be reliable, but in some cases the safety of such techniques can be undermined by the elementary human factor. For example, an intruder can simply spy on the entered PIN-code or graphic key, and then, remembering it, use the smartphone in the absence of the owner.

**The general structure of a biometric identification system is shown in Figure 1.**

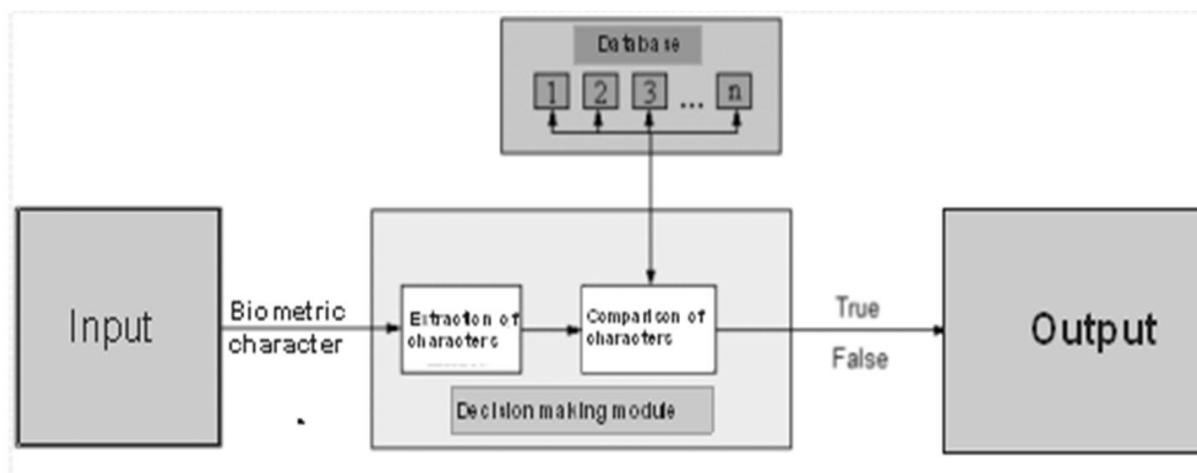


Fig. 1. Structure of a biometric identification system [1]

Basic biometric identification system includes a sensing module that ensures scanning of biometric character. Then the decision module compares the biometric data

with data in database and in the output graphical or other interface allows access or not.

An alternative to such a cryptographic technique was the technology of biometric identification by fingerprint. Like any cryptographic information security technology, the fingerprint scanner has advantages and disadvantages and various methods of scanning the fingerprint provide different results. All these methods are aimed at increasing the reliability of the system and make it safer to get the access.

## **2. Scanning methods**

2.1. A smart computing algorithm for finger vein matching with affine invariant features using fuzzy image retrieval

A few significant images from database are retrieved at this method, in decreasing order of similarity with the query image. In order to use fuzzy measures, intensity levels need to be shifted to a fuzzy plane where the intensity values are modified as real numbers between 0 and 1. Alteration of crisp values into fuzzy values for the linguistic fuzzy sets comes under fuzzification. Each linguistic term is associated to a grade by a membership function. By fuzzification, we mean the process of converting an object into a fuzzy object. A crisp set may be fuzzified by attaching a membership grade to each element of the set.

For fuzzifying database images and query image, gamma membership function is used on the histogram count of the intensity levels in images. Each pixel in the image is fuzzified by fuzzifying the corresponding intensity level's histogram count [2].

Affine Scale Invariant Feature Transform (ASIFT) converts image statistics into affine invariant coordinates by rotating the current image using the longitude and latitude angles. ASIFT detects key points, uses them for matching and compares the distances between these points. False Acceptance Rate (FAR), False Rejection Rate (FRR) and tracing the receiver operating characteristic curve were used for evaluating and comparing the performance of the proposed system and existing algorithms.

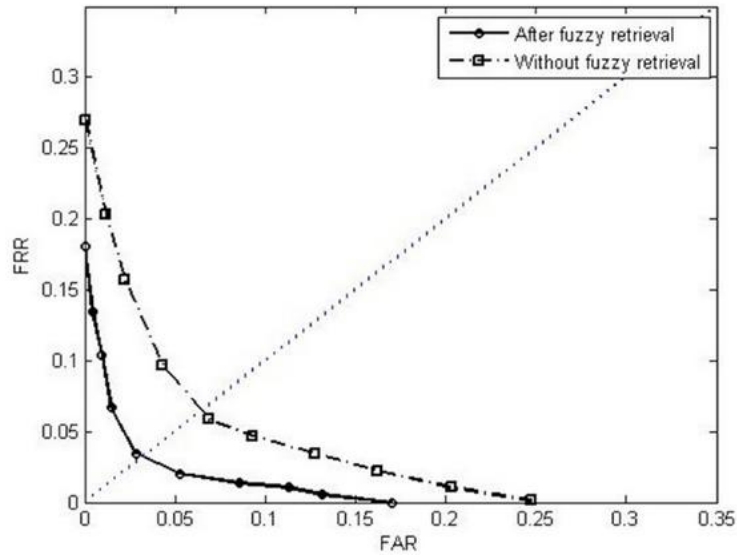


Fig. 2. Performance of ASIFT algorithm after fuzzy retrieval

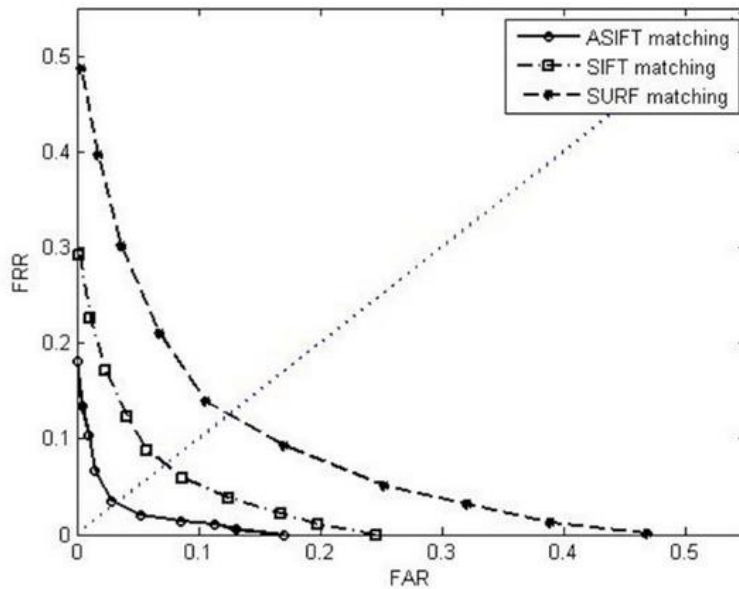


Fig. 3. Comparison of ASIFT, SIFT and SURF matching methods

The affine invariant feature method using fuzzy image retrieval provides the better performance (Fig. 2) and reduces the error rates in comparison with different methods (Fig. 3).

## 2.2. An Efficient Enhancement Technique using Wave Atom Transform and MCS Algorithm

Based on existing works in this specialized field that proposed the improvements in standard fingerprinting method by enhancing the image significant using effective two-stage scheme (Fig. 4) and simplify the optimal detector.

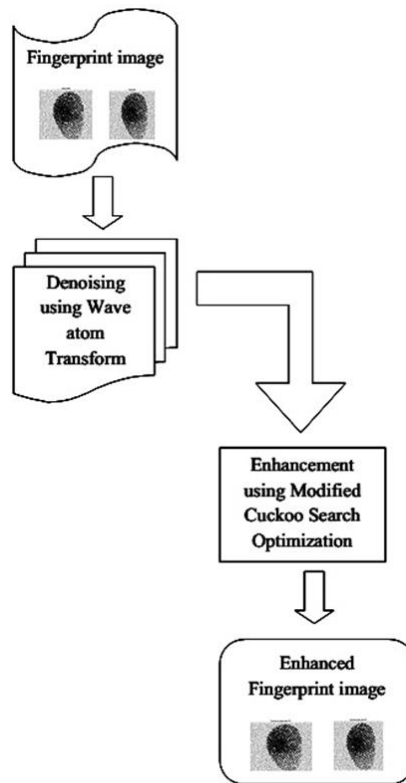


Fig. 4. Scheme Representation of Proposed Fingerprint Enhancement Technique.

New methodology consists of Denoising image using Wave Atom Transform and Enhancing using Modified Cuckoo Search (MCS) (Fig. 5). Wave Atom Transform implies the right and left circular shift process of calculation the coefficient and MCS improves the current image by some formulas which associated with generation of Cuckoo and used as an optimizer to look for the best gray level distribution which in turn aid in delivering improved enhancement to ant sort of images [3].










S. No.	Inputs	Image after denoising	Output Enhanced image (MCS)
1			
2			
3			

Fig. 5. MCS enhancing results

### Conclusion

In this paper we have focused on different methods of taking the fingerprints, security which they provide. Personal identification system must be reliable and resistant to introduction of intruders. ASIFT algorithms which are used in every fingerprint system reduce the size of the databases, lower the error rates and make the system more secure. All of the above methods can be combined in one system which will provide a better result.

### REFERENCES

1. Adamek M., Matysek M., Neumann P. Security of Biometric Systems / Procedia Engineering. № 100. 2015. С.169-176. Режим доступа: <https://www.sciencedirect.com/science/article/pii/S1877705815003823> (дата обращения: 15.12.2019)
2. Joseph P. R. B., Ezhilmaran D. A smart computing algorithm for finger vein matching with affine invariant features using fuzzy image retrieval / Procedia Computer Science. № 125. 2018. С. 172-178. Режим доступа:

<https://www.sciencedirect.com/science/article/pii/S1877050917327886> (дата обращения: 15.12.2019)

3. Borraa S. R., Reddyb G. J., Reddy E. S. An Efficient Fingerprint Enhancement Technique using Wave Atom Transform and MCS Algorithm /Procdeia Computer Science. № 89. 2016. С. 785-793. Режим доступа: <https://www.sciencedirect.com/science/article/pii/S1877050916311267> (дата обращения: 15.12.2019).