

**ANALYSIS OF MODELS AND ALGORITHMS FOR INCREASING SECURITY
LEVELS BASED ON THE INTRODUCTION OF BIOMETRIC AUTHENTICATION**

Xudayberganov Temur Rustamovich

Tashkent University of Information Technologies, Urgench branch,
Head of the Department of Information Security

doctordrebek@gmail.com

+998 97 211 53 05

Davlatmuratov Valijon To'liqin ugli

Tashkent University of Information Technologies, Urgench branch,
Master's student in Information Security

valijon.web@gmail.com

+998 94 237 03 73

Abstract: This article shows the importance of biometric authentication systems in increasing security. The study analyzes the developments of scientists such as Dr. John Daugman, Dr. Anil K. Jain, Dr. Tieniu Tan and Dr. Arun Ross, and examines the effectiveness of their algorithmic approaches and techniques. Methods for processing iris, fingerprint, face image and other biometric features, including Gabor filtering, Fourier transform, Haar cascade algorithms and Bayesian statistics, have provided high accuracy and reliability in authentication systems. The results confirmed the important role of these methods in increasing the effectiveness of biometric authentication systems. In the future, the integration of these systems with artificial intelligence and multi-modal approaches is expected to open up new opportunities.

Keywords: biometric authentication, Gabor filtering, Fourier transform, Haar cascade algorithm, Bayesian statistics, modal systems.

Аннотация. В статье показана важность систем биометрической аутентификации в повышении безопасности. В исследовании анализируются разработки таких ученых, как доктор Джон Даугман, доктор Анил К. Джейн, доктор Тиениу Тан и доктор Арун Росс, а также изучается эффективность их алгоритмических подходов и методов. Методы обработки радужной оболочки глаза, отпечатков пальцев, изображений лица и других биометрических признаков, включая фильтрацию Габора, преобразование Фурье, каскадные алгоритмы Хаара и байесовскую статистику, обеспечили высокую точность и надежность в системах аутентификации. Результаты подтвердили важную роль этих методов в повышении эффективности систем биометрической аутентификации. В будущем ожидается, что интеграция этих систем с искусственным интеллектом и многомодальными подходами откроет новые возможности.

Ключевые слова: биометрическая аутентификация, фильтрация Габора, преобразование Фурье, каскадный алгоритм Хаара, байесовская статистика, модальные системы.

Introduction

The rapid development of information technologies has made issues related to the security of information systems increasingly urgent. Every day, new methods emerge that create potential cyber threats and attack risks, posing serious challenges for both organizations and users. Ensuring data security requires the implementation of effective authentication mechanisms. Traditional authentication systems based on passwords and PIN codes often fail to provide sufficient protection; therefore, biometric authentication methods are now considered effective solutions that meet modern security requirements. Biometric authentication ensures a high level of security by analyzing the user's biological or behavioral characteristics. Such systems utilize features like fingerprints, facial images, voice patterns, or iris textures for identity verification. This study aims to develop a mathematical model and algorithm that enhance security in information systems through the application of biometric authentication methods. The proposed model plays a crucial role in maintaining the principles of confidentiality, integrity, and availability within information systems.

Methodology

Research in the field of biometric authentication is rapidly evolving. Below are some of the prominent scholars and their research findings that have significantly contributed to advancements in this area. The studies of these researchers have played an essential role in achieving major breakthroughs in biometric authentication and have been widely applied to enhance the security of information systems.

Dr. John Daugman has made pioneering contributions to the development of iris recognition technology in biometric authentication systems [1][2][3]. His methodology primarily consists of two main components: Gabor filtering techniques and Hamming distance calculation [2][4].

Gabor Filtering Technique: This technique is used to digitally identify the unique patterns of the human iris. It analyzes local frequency and orientation variations within the image using Gabor filters, which are defined by the following general mathematical expression [2]:

$$G(x, y) = \exp\left(-\frac{x^2 + y^2}{2\sigma^2}\right) \cdot \cos(2\pi u_0 x + \phi),$$

Hamming Distance Calculation: The Hamming distance is used to measure the degree of similarity between the encoded iris template and a newly captured iris image. It quantifies how many bits differ between the two binary iris codes. The smaller the Hamming distance, the higher the similarity between the two patterns, indicating a greater likelihood that both samples belong to the same individual.

$$H = \frac{1}{N} \sum_{i=1}^N (C_i \oplus T_i),$$

C_i va T_i template and new image bits, respectively, \oplus - XOR operation, N number of bits [4].

Dr. Anil K. Jain has developed sophisticated algorithms for biometric data recognition, including fingerprints, facial images, and irises.[5] This technique, which uses spectral analysis of images, allows for high-resolution processing of biometric patterns.[5] The following formula is used to extract the frequency domain features of an image

$$F(u, v) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) e^{-2\pi i(ux+vy)} dx dy.$$

Wavelet Decomposition: Wavelet techniques are used to analyze images at multiple scales and extract important features. This method helps to efficiently encode biometric data. In addition, Dr. Tieniu Tan has developed innovative algorithms for face recognition and gait pattern identification. This method is based on the principle of extracting the main features of the face in an image. It is used to detect facial features (eyes, nose, lips). The algorithm is based on the following linear function for face recognition:

$$R(x, y) = \sum_{i=1}^N w_i h_i(x, y),$$

here h_i – Haar features, w_i – their weight [6].

Optical flow analysis: The direction and speed of movement in an image are measured to analyze walking style. The optical flow technique is based on calculating the movement trajectory of each pixel[6].

Results

The conducted research has demonstrated significant advancements in the development of biometric authentication systems. Dr. John Daugman's iris recognition algorithms are distinguished by their high accuracy and reliability [1][2]. Through the use of Gabor filtering techniques, the unique patterns of the iris were precisely identified, while the Hamming distance provided an effective means for comparing these patterns. The results indicated that this approach achieves over 99% accuracy in user identification within authentication systems [3]. Dr. Anil K. Jain applied Fourier transformation and Wavelet decomposition techniques in biometric data processing, which considerably enhanced the accuracy of facial and fingerprint image analysis. These methods successfully identified micro-details in fingerprints and extracted distinctive features from facial images [5]. The outcomes confirmed the high potential of these techniques for improving the efficiency of biometric authentication systems [5]. Dr. Tieniu Tan utilized the Haar cascade algorithm and optical flow techniques for face and gait recognition. This approach enabled real-time facial detection and the identification of unique gait characteristics. These technologies have been successfully implemented in large-scale security systems, such as airports and train stations, demonstrating strong practical applicability. Dr. Arun Ross conducted research on multimodal biometric systems, improving authentication accuracy by integrating multiple biometric traits. Using modality fusion algorithms and Bayesian statistical models, he achieved an effective correlation between different biometric

characteristics [7]. The results showed that this approach ensured reliability levels exceeding 98% in biometric authentication systems [8]. Overall, these studies have made significant contributions to enhancing the efficiency and reliability of biometric authentication systems. Their global adoption is steadily expanding, opening new possibilities for developing security technologies that meet modern protection requirements [1][5][8].

Discussion

Biometric authentication systems have become one of the most reliable and effective tools in the field of modern security. These systems enhance the accuracy of user identification while reducing security risks. This study analyzed the developments of four leading scholars in biometric authentication and discussed the outcomes achieved through their scientific approaches.

Dr. John Daugman's iris recognition algorithms represent one of the most significant achievements in authentication systems. His approaches, particularly Gabor filtering techniques and Hamming distance computation, not only improved recognition accuracy but also significantly increased the processing speed of iris patterns. The practical application of these techniques opened new opportunities for enhancing the reliability and robustness of security systems.

Dr. Anil K. Jain, a leading researcher in biometric data processing and recognition, successfully employed Fourier transformation and Wavelet decomposition to extract fine-grained features of fingerprints and facial images. These techniques contributed to improving the performance of biometric systems and accelerating the authentication process. The findings indicate that such approaches not only strengthen security but also have a considerable impact on the advancement of data processing technologies.

Dr. Tieniu Tan's research on face recognition and gait analysis has been particularly valuable for security systems handling large-scale data. By utilizing the Haar cascade algorithm and optical flow techniques, it became possible to detect facial images and gait characteristics in real time. This technology introduced new directions for identifying unique human biometric traits and demonstrated high efficiency in practical security applications.

Dr. Arun Ross made significant contributions by developing multimodal biometric systems that enhance both accuracy and reliability in authentication. Through modality fusion algorithms and Bayesian statistical models, he combined multiple biometric features to achieve higher precision and robustness. This approach not only compensates for the weaknesses of single-modality systems but also provides more reliable solutions for complex security infrastructures.

The overall analysis shows that biometric authentication systems possess great potential in addressing modern security challenges. The continuous development of algorithms for processing iris, facial, and fingerprint features not only improves security levels but also allows authentication systems to adapt more effectively to human needs. The integration of these technologies with artificial intelligence (AI) in the future is expected to open new horizons for creating more intelligent, adaptive, and secure authentication systems.

Conclusion

Biometric authentication technologies stand out as a modern and reliable approach to ensuring the security of information systems. In this study, biometric authentication algorithms developed by four leading researchers — Dr. John Daugman, Dr. Anil K. Jain, Dr. Tieniu Tan, and Dr. Arun Ross — were analyzed. Their contributions have played a crucial role in accurately processing biometric data, identifying users, and ensuring reliable authentication processes.

Biometric methods based on iris recognition, facial analysis, fingerprint scanning, and gait identification have significantly improved the efficiency of security systems. In particular, multimodal authentication approaches, which combine multiple biometric features, have further enhanced accuracy and reliability.

The findings of the study show that biometric authentication not only simplifies user identification but also eliminates vulnerabilities inherent in traditional authentication methods. In the future, the integration of these systems with artificial intelligence and machine learning technologies is expected to lead to the creation of smarter, more adaptive, and more secure authentication systems.

References

1. Daugman, J. (2004). *How iris recognition works*. IEEE Transactions on Circuits and Systems for Video Technology.
2. Daugman, J. (1993). *High confidence visual recognition of persons by a test of statistical independence*. IEEE Transactions on Pattern Analysis and Machine Intelligence.
3. Bowyer, K.W., Hollingsworth, K., & Flynn, P.J. (2008). *Image understanding for iris biometrics: A survey*. Computer Vision and Image Understanding.
4. Wildes, R.P. (1997). *Iris recognition: An emerging biometric technology*. Proceedings of the IEEE.
5. Jain, A.K., Ross, A., & Nandakumar, K. (2011). *Introduction to biometrics*. Springer Science & Business Media.
6. Tan, T., Huang, Y., & Zhang, Z. (2005). *Face recognition and gait recognition*. Handbook of Face Recognition.
7. Daugman, J. (2002). *Biometric personal identification system based on iris analysis*. U.S. Patent No. 6,307,943.
8. Ross, A., Nandakumar, K., & Jain, A.K. (2006). *Handbook of Multibiometrics*. Springer.