Application of Computer Vision Methods for Information Security

Jaroslav Kultan[1], *Serik Meruyert*[2], *Tleumagambetova Danara*[3], *Duisegaliyeva Nassipzhan*[4]

DOI: https://doi.org/10.53349/re-source.2025.is1.a1389

Abstract

Computer vision methods based on machine and deep learning are extensively used in information security for data protection and user authentication. Key applications include biometric authentication (face, iris, fingerprint recognition), which enhances security compared to traditional methods, and real-time video surveillance to detect suspicious behaviour and cyber threats like deepfakes and hacking attempts. Ensuring confidentiality also requires encryption at all processing stages. In the context of teaching computer science, particularly in areas related to cybersecurity and cyber-attacks this research serves as a valuable didactic method. By incorporating real-world applications of computer vision into education, instructors can enhance security measures to protect sensitive data. Through practical experiments, students gain hands-on experience with biometric technologies, deepening their understanding.

This article examines modern computer vision methods for information security, focusing on facial recognition and anti-spoofing in student registration portals, with an emphasis on data protection. Experimental work with students from L.N. Gumilyev Eurasian National University and Almaty University of Technology compared facial recognition to traditional password-based registration. Results demonstrated over 95% accuracy in facial recognition with anti-spoofing, significantly reducing unauthorized access attempts and strengthening data security. These findings indicate that this technology streamlines registration, provides

[1] University of Economics in Bratislava, Bratislava, Slovakia.
E-Mail: jaroslav.kultan@euba.sk

[2] E.N. Gumilyov Eurasian National University, Astana, Kazakhstan.
E-Mail: serik_meruerts@mail.ru

[3] E.N. Gumilyov Eurasian National University, Astana, Kazakhstan.
E-Mail: danara1310@gmail.com

[4] E.N. Gumilyov Eurasian National University, Astana, Kazakhstan.
E-Mail: nasipzhan@mail.ru

enhanced security, and reduces the risks associated with manual or password-based systems on educational platforms.

Keywords: Computer Vision, Information Security, Biometric Authentication

1 Introduction

With advances in technology and the exponential growth of digital information, information security has become increasingly critical. Computer vision, driven by machine and deep learning, is now a key tool for data protection and user authentication. These technologies enable real-time visual data analysis, facilitating applications in biometric authentication and automated video surveillance.

Computer vision methods are applied in network security for detecting attacks or building security solutions, such as phishing attempt detection, malware detection, and traffic anomaly detection (Zhao, J et al., 2020, S. 15). One of the priority areas is biometric authentication, including facial recognition, iris recognition, and fingerprints. These methods not only simplify the identification process, but also increase the reliability of authentication, making them more effective compared to traditional passwords and PIN codes.

„Biometric authentication systems offer increased security and user convenience compared to traditional methods„ (Basare, A. et al., 2023). Computer vision is also actively used in video surveillance systems, where real-time video stream analysis allows you to detect suspicious behaviour and quickly respond to potential security threats. Such systems can detect anomalies in human behaviour or record unauthorized actions, which makes them an important element of modern security systems.

Face anti-spoofing (FAS) is essential for securing face recognition systems against physical attacks. Recent research has focused on long-distance surveillance scenarios, where low image resolution and noise interference pose significant challenges. Deep learning-based face anti-spoofing achieves remarkable performance and dominates the area, covering various novel components and applications (Yu, Z. et al., 2021). At the same time, data privacy issues are becoming a serious challenge, since computer vision systems often process personal information. This requires the implementation of additional measures, such as data encryption and protection at all stages of their processing, to prevent leaks and violations of users' privacy rights.

Computer vision methods are increasingly applied in network security for detecting phishing attempts, malware, and traffic anomalies. These methods leverage the growth of convolutional neural networks to build more secure networked systems (Zhao, J. et al., 2020).

Face anti-spoofing (a.k.a. presentation attack detection) has recently emerged as an active topic with great significance for both academia and industry due to the rapidly increasing demand in user authentication on mobile phones, PCs, tablets, and so on (Li, H. et al., 2018).

This article is devoted to the analysis of modern methods and approaches in the use of computer vision to improve information security, a discussion of the risks and vulnerabilities of these technologies, as well as the prospects for their use in information portals, including student registration through facial recognition using anti-spoofing.

This paper is a valuable resource for computer science educators who seek to integrate modern technologies into the educational process, demonstrating to students the practical application of computer vision in ensuring information security. Additionally, the analysis of biometric authentication methods and their vulnerabilities aids in developing students' critical thinking and skills in assessing the security of systems in use.

1.1 Computer Vision in Information Security: Fundamentals of Machine and Deep Learning

Computer vision systems, capable of analysing visual data, are crucial in information security. Machine and deep learning methods form the foundation, enabling accurate object recognition and classification. These technologies are widely applied for data protection and user authentication, enhancing security and convenience.

"Computer vision methods are used in network security to detect attacks, build security solutions, and analyse traffic anomalies" (Zhao, J. et al., 2020). Techniques such as retrieval, indexing, annotation, and relevance feedback are applied to visual data for security purposes. These methods are used in surveillance, biometrics recognition, and digital watermarking to enhance security measures (Tao, D. et al., 2009). Machine and deep learning are the core of modern computer vision methods. Machine learning includes algorithms that can learn from a data set, identifying patterns and making predictions without strict instructions. Key algorithms for computer vision tasks include convolutional neural networks (CNN), which are used for image classification and object recognition, and recurrent neural networks (RNN), which are able to process sequences of images and videos, which is especially useful for analysing video streams in real time.

Deep learning methods like Convolutional Neural Networks, Deep Boltzmann Machines, Deep Belief Networks, and Stacked Denoising Autoencoders outperform previous state-of-the-art machine learning techniques in computer vision tasks like object detection, face recognition, and human pose estimation (Voulodimos, A., et al., 2018). Computer vision tasks also use platforms and libraries such as TensorFlow, PyTorch, and OpenCV, which provide a wide range of tools for building and training models. Using such platforms allows for the development of more complex and accurate models that are suitable for specific information security tasks, including biometric authentication and video surveillance.

1.2 Role in data protection and user authentication

Computer vision algorithms are already successfully used to ensure data security and user authentication. One of the most popular applications is biometric authentication, which allows identifying users by unique physical characteristics, such as a face or fingerprints. This approach significantly reduces the risk of unauthorized access, since biometric data is much more difficult to forge compared to passwords or PIN codes.

Computer vision applications can improve security surveillance by managing face detection, motion detection, person identification, tracking, access control, and interpretation of movement (Abdulhussein, A. et al., 2020). Biometric authentication is increasingly being adopted for data protection due to its ability to provide secure and convenient user identification. This method leverages unique physiological and behavioural traits to verify identities, offering a robust alternative to traditional password-based systems. Combining multiple biometric factors enhances security while maintaining user comfort and reducing login time (Vlasov, K. et al., 2023).

In addition, computer vision algorithms are used to automatically analyse video streams, where they help detect suspicious behaviour and anomalies. For example, the system can recognize attempts of unauthorized access to objects or record suspicious activity in protected areas. This makes video surveillance systems more accurate and reliable, reducing the workload of the operator and minimizing the risk of human error.

Face spoofing detection is crucial for maintaining the integrity of face recognition systems, especially in surveillance scenarios where the risk of spoofing attacks is high. Various methods have been proposed to address this challenge, each leveraging different techniques to improve detection accuracy and robustness. Face spoofing detection in surveillance videos can be effectively achieved using colour texture analysis, which shows excellent results compared to the state-of-the-art methods (Boulkenafet, Z. et al., 2016).

Consider the diagram in Fig. 1, which highlights key applications of computer vision in information security, including image classification, object detection, biometric authentication, and anomaly detection. This visual representation emphasizes the role and relative importance of these applications in enhancing data protection and strengthening security systems.

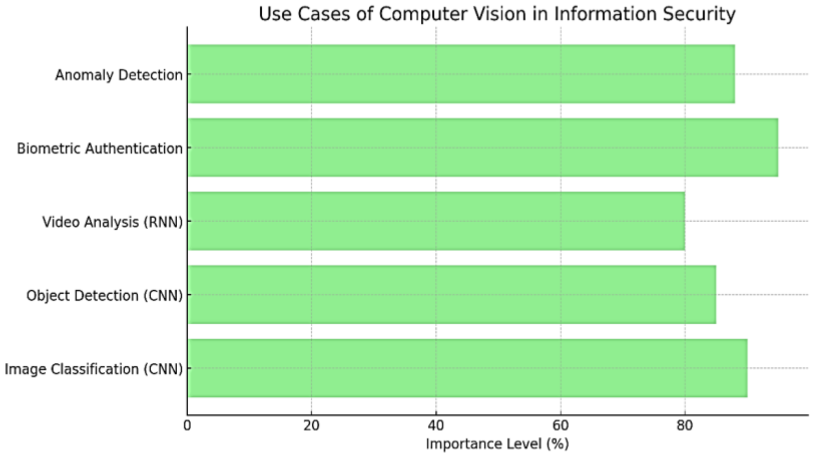


Figure 1: Use Cases of Computer Vision in Information Security.

Computer vision is an important foundation in safety detection due to its advantages in timeliness, accuracy, and intuition (Hu, C. et al., 2022). Thus, machine and deep learning methods in computer vision provide powerful tools for improving data security and strengthening authentication systems, making them indispensable in modern information security systems.

2 Biometric Authentication

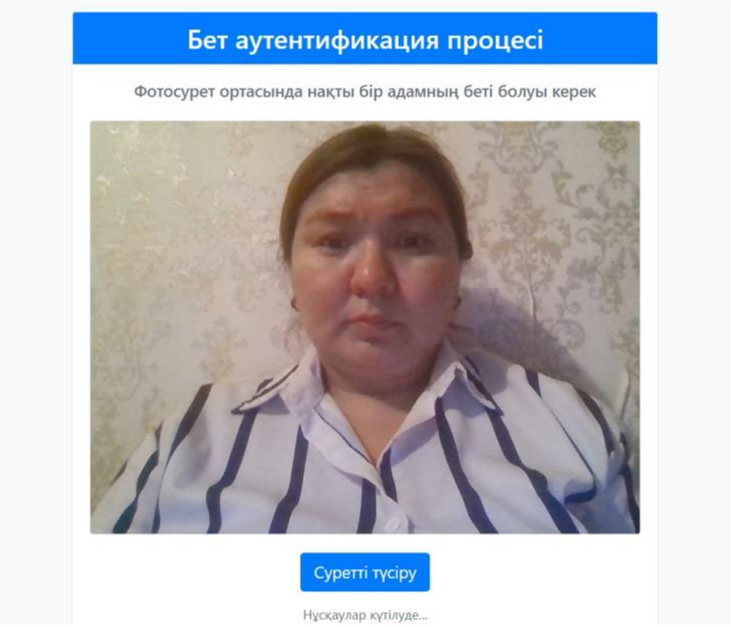
Biometric authentication identifies users through unique physical traits, offering higher security than traditional methods like passwords or PINs, as biometric data is hard to counterfeit. Computer vision enables various biometric methods, such as facial, iris, and fingerprint recognition.

This chapter presents some identification methods, their application possibilities, and their advantages over classic data protection methods.

2.1 Facial Recognition: Methods and Applications

Facial recognition, a widely used biometric authentication method, employs deep learning algorithms like convolutional neural networks (CNNs) to analyse unique facial features, such as eye distance and chin shape. These systems generate a digital model of the face, which is matched to stored templates for precise identification.

Computer vision methods, particularly convolutional neural networks (CNNs), are being used to detect phishing attempts and malware by analysing visual features of websites and software (Zhao, J. et al., 2020). Deep Learning-Based Methods: Recent advancements have seen the use of convolutional neural networks (CNNs) and other deep learning frameworks to significantly improve face detection and recognition accuracy, even in challenging conditions (Mamieva, D. et al., 2023).



Бет аутентификация процесі

Фотосурет ортасында нақты бір адамның беті болуы керек

Нұсқаулар күтілуде...

Figure 2: Demonstration of the face authentication process.

The image (Fig. 3) shows the screen of a biometric authentication system that recognizes the user's face for access. The system asks the user to take a photo of their face, and this image is verified in real time. This process highlights the convenience and accuracy of biometric authentication for secure access. Facial recognition is used to provide secure access to devices, objects, and systems. For example, the technology is widely used in smartphones to unlock the device, as well as in access control systems where the user's face serves as a "key" for entry.

Video surveillance with facial recognition helps identify suspicious individuals in real time, making this technology useful for ensuring security in public places. Face recognition is an efficient technique for identifying and verifying individuals in various fields, but faces challenges in unconstrained environments like pose, illumination, ageing, occlusion, expression, plastic surgery, and low resolution (Oloyede, M. et al., 2020).

2.2 Iris and fingerprint recognition

In addition to facial recognition, other biometric methods such as iris and fingerprint recognition are also widely used in security systems. Iris authentication on mobile devices is feasible using spatial histograms, but recognition accuracy is strongly affected by capture conditions (Barra, S. et al., 2015). Iris Recognition: This method is based on the analysis of the unique pattern of the iris, which remains unchanged throughout a person's life. The iris contains many individual characteristics, making it an ideal identifier. This method is especially in demand for protecting access to critical facilities and in situations where a high degree of accuracy is required.

Recent advancements in iris recognition have leveraged deep learning methods, including convolutional neural networks (CNNs) and capsule networks. These methods enhance the robustness and accuracy of iris recognition systems, even under varying lighting conditions and with limited training samples (Zhao, T. et al., 2019). Additionally, artificial neural networks have been explored, achieving high accuracy through various data partitioning techniques and pre-processing methods (Sibai, F. et al., 2011).

Fingerprint Recognition: One of the most common methods of biometric authentication is fingerprint recognition, due to its ease of use and high accuracy. Fingerprint image quality and password authentication require improvement, with graphical passwords showing promise for enhancing password method (Yusuf, N. et al., 2020). The unique line pattern on each person's fingers is used for identification in devices such as smartphones, laptops, and ATMs. This method is used for both personal security and large-scale systems that require large-scale identification.

Fingerprint recognition relies on two fundamental premises: the uniqueness and persistence of fingerprint patterns. Studies have shown that while the uniqueness of fingerprints is well-supported, the persistence over time can be influenced by factors such as the time interval between fingerprint captures and the quality of the fingerprint images. “Genuine match scores tend to decrease over longer time intervals, but recognition accuracy remains stable for up to 12 years if the fingerprint quality is high" (Yoon, S. & Jain, A., 2015). Biometrics-based authentication schemes, such as fingerprints or iris scans, do not have the drawbacks associated with passwords and smart cards, making them more attractive for multi-server environments (He, D. & Wang, D. 2015).

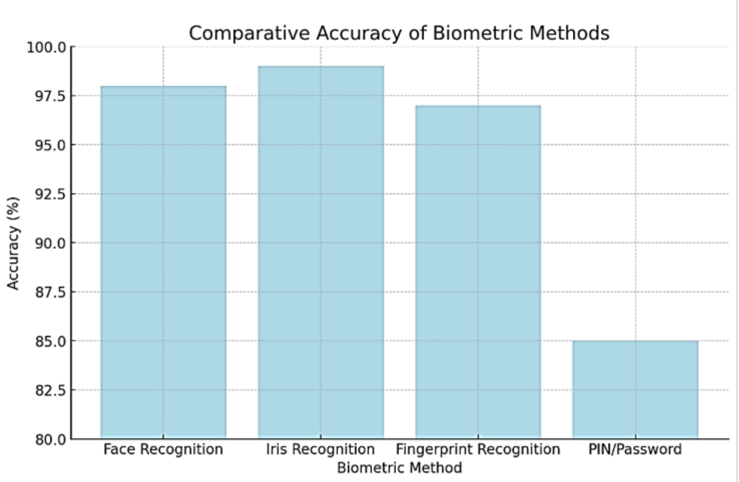


Figure 3: Accuracy of Different Biometric Authentication Methods.

As shown in Fig. 3, various biometric authentication methods such as facial recognition, iris recognition, fingerprint recognition and PIN/Password demonstrate different accuracy, providing a reliable level of security. Comparative accuracy of biometric methods shows that facial, iris and fingerprint recognition biometric methods are superior to traditional passwords and PIN codes in accuracy. These methods significantly reduce the likelihood of unauthorized access, making them more effective than traditional security methods.

2.3 Advantages over Traditional Methods

Biometric authentication has several key advantages over traditional security methods such as passwords and PINs:

- High reliability and security: Biometric data is unique to each person, making it virtually impossible to counterfeit. This significantly reduces the likelihood of unauthorized access and fraud.
- Ease of use: Unlike passwords, which can be forgotten or lost, biometric characteristics are always available to the user. The authentication process through biometrics is usually faster and more convenient for the user.
- Reduced risk of data leakage: Unlike passwords, biometric data is difficult to steal or forge, which reduces the likelihood of data leakage. For example, when using facial authentication in smartphones, the user does not need to enter a password that can be peeked at or stolen.

Consequently, biometric authentication not only provides a higher level of security, but also significantly simplifies the identification process, which makes it a promising alternative to traditional data protection methods.

3 Application of computer vision in video surveillance

Computer vision technologies enhance information security through data protection, biometric authentication, and real-time video analysis. Using machine and deep learning, these methods improve user identification and cyber threat detection. In video surveillance, they enable the detection of suspicious behaviours and unauthorized access, reducing the need for continuous human monitoring.

The application of computer vision in video surveillance has seen significant advancements, leveraging artificial intelligence (AI) and deep learning to enhance the capabilities of traditional surveillance systems (Idrees, H. et al., 2018). These technologies are crucial for securing confidential spaces, like government facilities and campuses, where facial recognition with anti-spoofing can add security, and behaviour analysis can flag unusual activities.

As part of the educational process, studying these technologies helps students understand modern security methods, develop critical analysis skills, and emphasizes the importance of protecting personal data. This awareness fosters responsible attitudes toward privacy and confidentiality in the digital environment.

3.1 Real-time video stream analysis

Real-time video stream analysis is based on deep learning algorithms that allow processing and interpretation of video coming from cameras with minimal delay. Algorithms such as convolutional neural networks (CNN) are used for object recognition and face identification, and recurrent neural networks (RNN) are used to analyse temporal changes, such as behaviour and movement of objects. Systems can detect behavioural anomalies, such as people staying in prohibited areas or aggressive actions and instantly notify the operator of possible violations. Behaviour Analysis from Video Streams: Systems designed for event detection from video streams use modular blocks to detect and track moving objects. These systems stabilize image sequences, extract regions with residual motion, and infer object trajectories to analyse behaviours in real-time. The system detects and tracks moving regions in a video stream, stabilizes the image, and infers their trajectories to generate likely scenarios.

Real-time video stream analysis has become increasingly critical with the proliferation of IoT devices and the growing demand for low-latency applications such as video surveillance, augmented reality, and autonomous vehicles. Effective management and orchestration of video delivery in multi-tier edge/cloud environments are essential for reducing latency and network congestion. Properly distributing video streams according to their requirements can significantly improve the end-user Quality of Experience (QoE). In 2022, 82% of all internet traffic will be dominated by video streaming, and proper management and orchestration of video delivery can considerably increase end-user quality of experience (Gama, E. et al., 2021). The use of video stream analysis is widely used in public places such as airports, shopping malls and transport hubs, where it is important to promptly identify suspicious activity and prevent possible incidents. In such systems, computer vision algorithms can automatically track and record activity, freeing the operator from the need for constant monitoring.

3.2 Detection of suspicious behaviour and cyber threats

Computer vision can detect suspicious behaviour, indicating potential threats. Algorithms trained on large data sets identify deviations like aggressive actions, unauthorized access, and unusual crowd behaviour. One of the current threats is the use of deepfake attacks, in which fake videos are used to deceive video surveillance systems or for disinformation. Computer vision combined with artificial intelligence techniques can identify such fakes by analysing the tiny details and inconsistencies that occur when deepfake videos are created.

Convolutional Vision Transformers, combining CNN and Vision Transformer architectures, have achieved competitive results with 91.5% accuracy on the Deepfake Detection Challenge Dataset (Wodajo, D. & Atnafu, S. 2021). Human ability to detect deepfake images is only slightly above chance, with an overall accuracy of 62%. Confidence in detection is high but not correlated with accuracy, indicating the need for automated detection methods (Bray, S. et al. 2022).

Face anti-spoofing (FAS) is crucial for securing face recognition systems against various physical and digital attacks. This process involves detecting and preventing attempts to deceive face recognition systems using fake representations such as photos, videos, or masks. Image Quality and Resolution: Surveillance scenarios often involve low image resolution and noise interference, which pose significant challenges for FAS. Techniques like Contrastive Quality-Invariance Learning (CQIL) have been proposed to address these issues by enhancing image quality and learning robust features under varying conditions (Fang, H., et al., (2023).

Anti-Spoofing Process in Facial Recognition is an important element of computer vision aimed at protecting against counterfeiting, including deepfake threats. This process includes the stages of image capture, liveness verification, and counterfeit detection, which allows the system to recognize a real person in front of the camera and prevent the use of fake images or videos to fool CCTV. When combined with artificial intelligence, anti-spoofing helps the system analyse the smallest details and detect inconsistencies characteristic of deepfake videos, minimizing the risk of disinformation and unauthorized access.

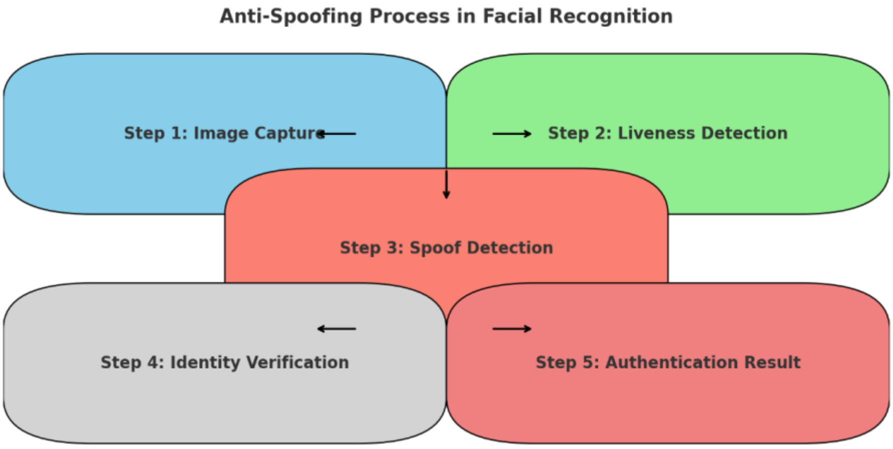

Anti-Spoofing Process in Facial Recognition
Step 1: Image Capture
Step 2: Liveness Detection
Step 3: Spoof Detection
Step 4: Identity Verification
Step 5: Authentication Result

Figure 4: Use Cases of Computer Vision in Information Security.

This Fig. 4 is a step-by-step diagram illustrating the anti-spoofing process in facial recognition, from image capture to authentication and final identification.

The following steps are included:
Step 1: Image Capture – the system captures an image of the user's face.
Step 2: Liveness Check – it is verified that the person in front of the camera is real and not a photo.
Step 3: Forgery Detection – the system detects deception attempts, such as using a photo or video on the screen.
Step 4: Identity Verification – the face is compared with templates in the database.
Step 5: Authentication Result – the system accepts or rejects the access request.

The diagram clearly shows how the system recognizes the real user and excludes forgeries, providing protection against attacks using fake images. The anti-spoofing process in facial recognition involves a combination of contour detection, deep supervision, temporal analysis, semi-supervised learning, generalizable representations, quality-invariance learning, domain adaptation, spoof trace disentanglement, and fine-grained detection. These methods collectively enhance the robustness and accuracy of face anti-spoofing systems, ensuring better security and reliability in face recognition applications (Wang, H. et al., 2023).
These technologies are also used to protect video surveillance systems from being hacked. For example, algorithms can detect suspicious activity on the network, such as attempts to unauthorizedly access cameras and recordings, and warn operators of possible cyberattacks.

3.3 Capabilities and Limitations

While computer vision greatly expands the capabilities of video surveillance, there are certain limitations.

Capabilities:

- High accuracy and automation: Deep learning algorithms allow for high-precision video analysis, automating the threat detection process.
- Real-time response: Fast processing of video streams allows for immediate response to suspicious activity, increasing the effectiveness of security systems.

Limitations:

- Technical challenges: Cameras may have problems in low light, crowded conditions, or adverse weather conditions, which may reduce recognition accuracy.
- Privacy issues: Video surveillance involves data privacy, as cameras record people's movements and actions. It is important to comply with legal regulations and ensure the protection of collected information, especially in public spaces (add citation on privacy issues in video surveillance systems).

As a result, the use of computer vision in video surveillance provides significant opportunities to improve security but requires attention to data privacy and technical limitations.

4 Protection against cyber threats and attacks using deep fakes (deepfakes)

The objective of this section is to analyse some of the threats posed by deepfakes and outline their mitigation methods. Identifying deepfakes is the first step, using deep learning to detect digital artifacts like facial inconsistencies (Müller, N. et al., 2023)

The next step is to protect video surveillance systems from hacking, employing biometric authentication, encryption, and network monitoring to secure data (Vennam, P. et al., 2021).

The final part of this chapter discusses algorithms for cyberattack detection, such as CNNs and RNNs, which help detect anomalies in video frames and patterns of suspicious activity (Wodajo, D. & Atnafu, S., 2021).

4.1 Algorithms for detecting fake videos

Modern deepfake technologies pose significant risks for information security by creating realistic fake videos and images that can deceive, spread disinformation, or exploit systems. Detecting such fakes and safeguarding surveillance systems from hacking are top priorities in cybersecurity.

Deepfake detection and anti-spoofing methods have made significant strides, particularly with the use of deep learning techniques. However, challenges such as generalization, computational complexity, and explainability remain. Future research should focus on developing more robust, efficient, and interpretable models to effectively combat the evolving threat of deepfakes (Müller, N. et al., 2023).

To counter deepfake attacks, anti-spoofing algorithms have been developed alongside deepfake detection methods. Anti-spoofing techniques help systems recognize real users versus fake or manipulated visuals, preventing unauthorized access through fake images or videos. Algorithms that detect digital artifacts — such as unnatural facial movements, lighting mismatches, and lip-sync errors — work in tandem with anti-spoofing to secure surveillance and biometric systems.

4.2 Protecting video surveillance systems from hacking

Video surveillance systems often become targets for cyberattacks, where unauthorized users may attempt to access camera feeds or manipulate stored data. Anti-spoofing complements other methods of system protection, such as:

- *User authentication:* Biometric and multi-factor authentication with anti-spoofing prevents unauthorized individuals from accessing the system.
- *Encryption of video streams:* Data transmitted from cameras is encrypted to prevent interception or tampering.
- *Network activity monitoring:* Algorithms that monitor suspicious activity detect hacking attempts and prevent unauthorized access. Conducting systematic reviews of threats, vulnerabilities, and attacks on video surveillance systems and summarizing countermeasures can provide practical security checklists and recommendations for improving system security (Vennam, P. et al., 2021).

These measures significantly reduce hacking risks and secure data in video streams.

4.3 Examples of algorithms for detecting deepfakes and other cyberthreats

Various algorithms have been developed to detect deepfakes and other cyberthreats:

- *Convolutional Neural Networks (CNNs):* Detect anomalies in video frames by analysing image details, often revealing distortions in fakes.
- *Recurrent Neural Networks (RNNs):* Process time sequences to detect unnatural changes in movement and frame sync, characteristic of deepfakes.
- *Combined CNN and RNN models:* By merging spatial and temporal analysis, these models achieve high accuracy in real-time video analysis.
- *Digital Forensics and Anti-Spoofing:* Techniques in digital forensics and anti-spoofing analyse inconsistencies and protect systems from fake data manipulation, thus strengthening surveillance and information security overall (add citation for anti-spoofing and forensics methods).

These algorithms, including anti-spoofing, enhance deepfake detection, protect surveillance systems, and are essential for robust information security.

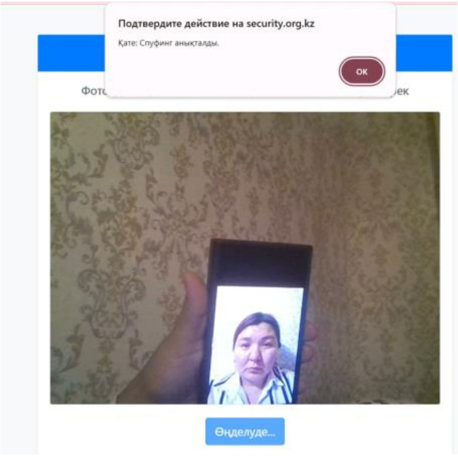
5 Ensuring Data Privacy in Computer Vision Systems

Computer vision systems in information security process sensitive biometric data, such as facial images and fingerprints, requiring stringent data privacy and anti-spoofing measures. Anti-spoofing technology provides an essential layer of protection by verifying that biometric data is authentic, preventing unauthorized access through fake images or videos. Data privacy efforts include minimizing data collection, informing users about data usage, and obtaining consent, especially in public spaces where surveillance may not be apparent. Data encryption, anonymization, and pseudonymization further mitigate privacy risks.

Adhering to legal frameworks, such as GDPR, and ethical standards is critical to maintain transparency, protect user rights, and build trust in computer vision technologies for security.

6 Experimental work based on educational programs

As part of this study, experimental work was conducted to evaluate the effectiveness of computer vision technology for student registration in educational programs at L.N. Gumilyov Eurasian National University and Almaty Technological University. The primary goal was to test a facial recognition system with anti-spoofing functionality to ensure secure and reliable student authentication on the educational portal.



Подтвердите действие на security.org.kz

Қате: Спуфинг анықталды.

Figure 5: Anti-spoofing.

The image (Fig. 5) illustrates an attempt to fool the system by presenting a photo of a face on a phone. The anti-spoofing technology detected this attempt, flagged it as fraudulent, and blocked access. This example demonstrates how anti-spoofing prevents unauthorized access by distinguishing real users from impostors using fake images.

The experiment involved students enrolled in various programs, such as "6B01511 - Computer Science," "7M01511 - Computer Science," and "M094 - Information Technology." The portal utilized advanced facial recognition algorithms combined with anti-spoofing technology, which uses deep learning to ensure that only a real person—and not an image or video—can gain access. Students' facial images were scanned and matched with stored biometric data in the database to verify their identities. Face anti-spoofing methods often assume that training and testing samples come from the same domain, which limits their generalization capability. An unsupervised domain adaptation scheme addresses this by learning classifiers for target domains based on training samples from different source domains. This approach minimizes the Maximum Mean Discrepancy between latent features in source and target domains, enhancing the generalization capability of anti-spoofing systems in cross-domain scenarios (Qin, Y., et al., 2021).

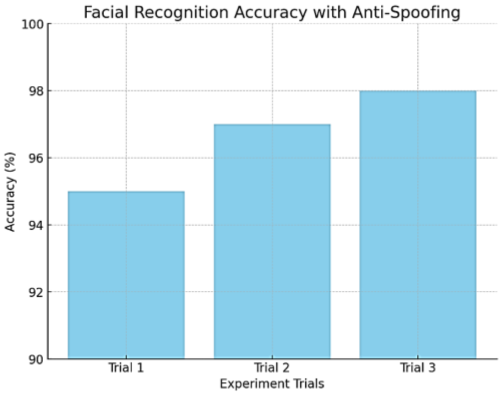


Figure 6: Anti-spoofing.

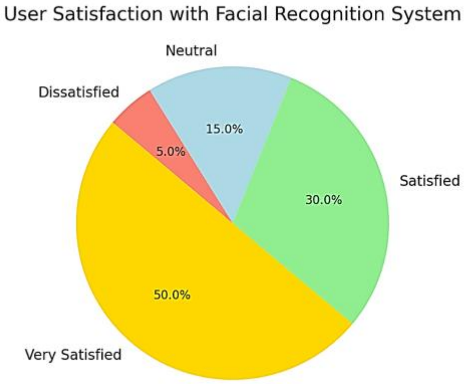


Figure 7: Anti-spoofing.

The Facial Recognition Accuracy with Anti-Spoofing diagram (Fig. 6) shows the results of three trials of the facial recognition system with anti-spoofing, conducted under real-world conditions on a learning portal. The system achieved a recognition accuracy rate exceeding 95% and successfully prevented over 98% of unauthorized access attempts using fake images. The User Satisfaction with Facial Recognition System pie chart (Fig. 7) shows the results of a survey of users assessing their satisfaction with the facial recognition system on the educational portal. The majority of users (50%) indicated a high level of satisfaction, citing the convenience and reliability of the system. Another 30% of users expressed satisfaction, rating the system as easy to use and secure. About 15% remained neutral, and 5% expressed dissatisfaction, noting rare cases of recognition errors.

These results show that most users rated the facial recognition system positively, especially due to the convenience and enhanced security provided by the anti-spoofing technology. Compared to traditional password-based access methods, the facial recognition system demonstrated enhanced security by reducing login time, improving data accuracy, and eliminating password-related issues. Additionally, anti-spoofing enhanced data integrity by preventing common types of visual fraud. These findings indicate that computer vision and anti-spoofing technology can effectively streamline student registration, improve data security, and minimize unauthorized access risks. This approach provides a robust alternative to traditional methods, offering increased protection of student data and better control over attendance and access to educational materials.

7 Conclusion

This study highlights the significant potential of computer vision in information security, especially for data protection and user authentication. Modern machine and deep learning methods effectively tackle challenges in biometric authentication, video surveillance, and defence against cyber threats like deepfake attacks. Experimental work conducted with educational programs using facial recognition and anti-spoofing confirmed high accuracy and robust security in student authentication, demonstrating the practical application of these technologies in registration and access control on educational portals.

Despite these advantages, certain risks and limitations remain. Computer vision systems can be impacted by technical constraints, such as challenging lighting conditions or high-density environments, which may reduce recognition accuracy. Additionally, processing biometric data requires strict adherence to privacy standards, as handling personal information raises privacy and ethical concerns. To mitigate these risks, encryption, anonymization, and access control measures are essential for preventing data breaches. Anti-spoofing technologies, particularly those leveraging deep learning, multi-perspective feature learning, and neural architecture search, are crucial for enhancing the security of facial recognition systems against deepfake and other spoofing attacks. “These advanced methods provide robust, real-time, and comprehensive solutions for detecting and mitigating various types of spoofing attacks, ensuring the reliability and security of facial recognition systems across diverse scenarios” (B, F., Suresh et al., 2023).

The future of computer vision in information security appears promising. Expected improvements in algorithms will likely enhance recognition accuracy and reduce dependency on environmental factors. Furthermore, advancements in anti-spoofing and digital forensics will strengthen defences against emerging cyber threats, including deepfakes. As computer vision technology evolves, it will play an increasingly critical role in building secure systems and protecting data, solidifying its position as an indispensable tool in the future of information security.

The didactic value of this article lies in providing computer science educators with relevant examples of practical applications of computer vision in information security. Studying technologies like anti-spoofing and biometric authentication enables students to better understand modern threats and data protection methods, as well as evaluate the ethical aspects of working with personal information. The inclusion of cases related to the security of educational platforms helps students develop critical thinking skills and problem-solving abilities in the field of cybersecurity.

References

Zhao, J. (2020). A Review of Computer Vision Methods in Network Security. Masood, R., Seneviratne, S. *IEEE Communications Surveys & Tutorials, 23,* pp. 1838–1878. https://doi.org/10.1109/COMST.2021.3086475.

Basare, A. (2023). Biometric Authentication System. In Bhojak, D., & Solanki, D. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2023.54246.

Yu, Z. (2021). Deep Learning for Face Anti-Spoofing: A Survey. In Qin, Y., Li, X., Zhao, C., Lei, Z., & Zhao, G. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 45*, pp. 5609–5631. https://doi.org/10.1109/TPAMI.2022.3215850.

Li, H. (2018). Unsupervised Domain Adaptation for Face Anti-Spoofing. In Li, W., Cao, H., Wang, S., Huang, F., & Kot, A. *IEEE Transactions on Information Forensics and Security*, *13*, pp. 1794–1809. https://doi.org/10.1109/TIFS.2018.2801312.).

Tao, D. (2009). Visual information analysis for security. *Signal Process.* In Yuan, Y., Shen, J., Huang, K., & Li, X. *89*, pp. 2311–2312. https://doi.org/10.1016/J.SIGPRO.2009.06.023

Voulodimos, A. (2018). Deep Learning for Computer Vision: A Brief Review. In Doulamis, N., Doulamis, A., & Protopapadakis, E. *Computational Intelligence and Neuroscience*, https://doi.org/10.1155/2018/7068349

Abdulhussein, A. (2020). Computer Vision to Improve Security Surveillance through the Identification of Digital Patterns. In Kuba, H., & Alanssari, A. *International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, pp. 1–5. https://doi.org/10.1109/ICIEAM48468.2020.9112022

Vlasov, K (2023). Using biometric data to protect information. In Tolstykh, O., & Isaev, O. *Herald of Dagestan State Technical University. Technical Sciences*. https://doi.org/10.21822/2073-6185-2023-50-3-46-56

Boulkenafet, Z. (2016). Face Spoofing Detection Using Colour Texture Analysis.Komulainen, J., & Hadid, A. *IEEE Transactions on Information Forensics and Security*, *11*, pp. 1818–1830. https://doi.org/10.1109/TIFS.2016.2555286.

Hu, C. (2022). Application Strategy of Security Detection Technology in the Background of Computer Vision. Qiu, W., & Wu, W. *The Frontiers of Society, Science and Technology*. https://doi.org/10.25236/fsst.2022.041002

Mamieva, D. (2023). Improved Face Detection Method via Learning Small Faces on Hard Images Based on a Deep Learning Approach. Abdusalomov, A., Mukhiddinov, M., & Whangbo, T. *Sensors (Basel, Switzerland)*, *23*. https://doi.org/10.3390/s23010502.)

Oloyede, M. (2020). A review on face recognition systems: recent approaches and challenges. Hancke, G., & Myburgh, H. *Multimedia Tools and Applications*, *79*, 27891–27922. https://doi.org/10.1007/s11042-020-09261-2.).

Barra, S. (2015). Ubiquitous iris recognition by means of mobile devices.Casanova, A., Narducci, F., & Ricciardi, S. *Pattern Recognit. Lett.*, 57, 66-73. https://doi.org/10.1016/j.patrec.2014.10.011.

Zhao, T. (2019). A Deep Learning Iris Recognition Method Based on Capsule Network Architecture. Liu, Y., Huo, G., & Zhu, X. *IEEE Access*, 7, 49691-49701. https://doi.org/10.1109/ACCESS.2019.2911056

Sibai, F. (2011). Iris recognition using artificial neural networks. Hosani, H., Naqbi, R., Dhanhani, S., & Shehhi, S. *Expert Syst. Appl.*, *38*, pp. 5940–5946. https://doi.org/10.1016/j.eswa.2010.11.029

Yusuf, N. (2020). A survey of biometric approaches of authentication. Marafa, K., Shehu, K., Mamman, H., & Maidawa, M., *10*, pp. 96–104.

https://doi.org/10.19101/ijacr.2019.940152.

Yoon, S., & Jain, A. (2015). Longitudinal study of fingerprint recognition. *Proceedings of the National Academy of Sciences*, *112*, 8555–8560. https://doi.org/10.1073/pnas.1410272112

He, D., & Wang, D. (2015). Robust Biometrics-Based Authentication Scheme for Multiserver . *IEEE Systems Journal*, 9, pp. 816–823. https://doi.org/10.1109/JSYST.2014.2301517

Idrees, H., Shah, M., & Surette, R. (2018). Enhancing camera surveillance using computer vision: a research note. *ArXiv*, abs/1808.03998. https://doi.org/10.1108/PIJPSM-11-2016-0158.

Gama, E. (2021). Video Streaming Analysis in Multi-tier Edge-Cloud Networks. Araújo, L., Immich, R., & Bittencourt, L. *2021 8th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 19–25. https://doi.org/10.1109/FiCloud49777.2021.00011

Wodajo, D., & Atnafu, S. (2021). Deepfake Video Detection Using Convolutional Vision Transformer. *ArXiv*, abs/2102.11126

Bray, S. (2022). Testing Human Ability To Detect Deepfake Images of Human Faces.Johnson, S., & Kleinberg, B. *J. Cybersecur.*, *9*. https://doi.org/10.48550/arXiv.2212.05056

Fang, H. (2023). Surveillance Face Anti-Spoofing. Liu, A., Wan, J., Escalera, S., Zhao, C., Zhang, X., Li, S., & Lei, Z. *IEEE Transactions on Information Forensics and Security*, *19,* pp. 1535–1546. https://doi.org/10.1109/TIFS.2023.3337970

Wang, H. (2023). Face Anti-spoofing Method Based on Deep Supervision. Liu, L., & Jia, A. *Proceedings of the 2023 2nd Asia Conference on Algorithms, Computing and Machine Learning*. https://doi.org/10.1145/3590003.3590023

Müller, N. (2023). Complex-valued neural networks for voice anti-spoofing. Sperl, P., &, K. *ArXiv*, abs/2308.11800. https://doi.org/10.21437/interspeech.2023-901

Vennam, P. (2021). Attacks and Preventive Measures on Video Surveillance Systems: A Review. C., P., M., T., Kim, Y., & N., P. *Applied Sciences*. https://doi.org/10.3390/APP11125571

Qin, Y. (2021). Meta-Teacher For Face Anti-Spoofing. Yu, Z., Yan, L., Wang, Z., Zhao, C., & Lei, Z. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *44*, pp. 6311–6326. https://doi.org/10.1109/TPAMI.2021.3091167

Suresh, B., F. (2023). People Identification Through Facial Recognition and Anti-Spoofing Using Deep Learning. G., Hemalatha, S., & Veronica, S. *International Journal of Scientific Research in Science, Engineering and Technology*. https://doi.org/10.32628/ijsrset2310539