

FACIAL BIOMETRIC AUTHENTICATION ENHANCED BY EMOTIONAL AND DEMOGRAPHIC CONTEXTS

Eva KUPCOVÁ, Matúš PLEVA, Zuzana SOKOLOVÁ, Jakub BAJO

Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics
Technical University of Košice, Letná 9, 040 01 Košice, Slovak Republic, Tel. +421 55/602 3307

E-mails: eva.kupcova@tuke.sk, matus.pleva@tuke.sk, zuzana.sokolova@tuke.sk, jakub.bajo@student.tuke.sk

ABSTRACT

This paper presents a cloud-based facial biometric authentication system integrating demographic and emotional attributes to enhance verification robustness under compression and distortion. A prototype web platform was implemented using cloud-based services, combining facial recognition with demographic and emotional analysis. The system was experimentally evaluated under multiple image degradation scenarios, including lossy and lossless compression, blurring, and block partitioning. Results show that recognition accuracy remains above 98% under mild compression, but decreases significantly under severe distortions, with match rates dropping below 25% in extreme cases. Additional experiments demonstrate reliable gender classification (95%) and moderate performance for age and emotion estimation. The contribution of this work lies in demonstrating the practical feasibility of combining identity verification with contextual biometric features in resource-constrained environments, while also outlining the limitations and security implications of such systems.

Keywords: Biometric authentication, Face recognition, Emotion detection, Age and gender estimation, Image compression

1. INTRODUCTION

Biometric authentication is an important part of modern information security. Facial recognition has become widely used because it is non-intrusive, easy to operate, and suitable for remote verification. Its accuracy, however, is affected by illumination, image quality, and facial expressions, which can reduce reliability in real-world conditions [1].

To mitigate these limitations, additional information extracted from the face, such as emotional state, estimated age, and gender, can support decision-making when the primary facial match is uncertain or degraded. Emotion detection is relevant because facial expressions directly influence geometric and textural features used during authentication. Strong expressions may shift key landmarks or partly occlude characteristic regions, lowering the similarity score even for the correct identity. By considering emotional context, the system can better distinguish between an actual mismatch and a temporary expression change, improving robustness when image quality or user behaviour varies. Ethical and privacy considerations remain essential when deploying such technologies [2].

Facial recognition is also increasingly used on mobile and IoT devices with limited resources, where efficient image processing and compression are necessary to maintain accuracy. Although modern networks provide high transmission speeds, compression remains relevant because many devices operate under bandwidth limitations, intermittent connectivity, or power-saving constraints. Cloud-based biometric systems also process large numbers of requests, making reduced data size important for lower latency and storage costs. Understanding the impact of compression on recognition accuracy is therefore essential for reliable real-world deployment.

The goal of this article is to design and evaluate a web-based facial authentication prototype that integrates

demographic and emotional attributes as supplementary biometric signals. The study examines whether these contextual features improve robustness under varying image quality conditions, evaluates the reliability of gender, age, and emotion estimation, and discusses the security and privacy implications of using commercial cloud services. Given the limited dataset size, the work has a pilot character and provides a basis for future research.

2. RELATED WORK

Several recent studies highlight challenges in facial biometrics relevant to this work. In liveness detection and spoofing resistance, Li et al. [3] showed that commercial verification APIs remain vulnerable to deepfake-based attacks, particularly with low-quality input. Yu et al. [4] proposed a joint framework combining visual features with physiological signals, such as remote photoplethysmography (rPPG), to enhance resilience against spoofing. These findings indicate that unimodal face verification is insufficient under adversarial conditions.

Privacy-preserving face recognition represents another key research direction. Wang et al. [5] introduced an edge-based framework applying local differential privacy to protect biometric data during collection and transmission. Recent surveys further emphasize anonymization, differential privacy, and secure storage as critical safeguards for cloud-deployed biometric systems [6].

Evaluation studies also demonstrate that face recognition performance deteriorates under real-world degradations. In paper by Verdoliva [7] provided a comprehensive overview of deepfake detection and media forensics, showing that compression, resizing, and noise substantially reduce reliability.

Based on these insights, this study evaluates cloud-hosted facial recognition under various compression and degradation scenarios while assessing the auxiliary

contribution of contextual demographic and emotional features.

3. BIOMETRIC IDENTIFICATION SYSTEMS

A biometric system generally operates in three phases: enrollment, where raw biometric data are processed into a reference template; verification, in which a newly captured sample is compared with the stored template to confirm identity; and identification, which involves searching a database of templates to find the closest match [8]. The performance of such systems is typically evaluated using metrics such as the False Acceptance Rate (FAR), False Rejection Rate (FRR), and the Equal Error Rate (EER), which provide an objective measure of reliability.

Among the available biometric modalities, face recognition has emerged as a widely adopted solution due to its ease of acquisition and user acceptability. However, its accuracy is often reduced by factors such as poor illumination, varying facial expressions, and image compression artifacts. Compared to modalities such as iris or fingerprint recognition, which generally achieve

higher permanence and uniqueness, face recognition is more sensitive to environmental conditions but offers clear advantages in usability and deployment flexibility [9].

For this reason, current research trends aim to enhance facial authentication by combining it with supplementary signals. Attributes such as emotion, age, or gender, although not unique identifiers on their own, can provide valuable contextual evidence when integrated with primary facial features. This approach motivates the present work, where the role of contextual attributes is analysed with respect to their potential to increase recognition robustness under degraded image conditions. As shown in Table 1, face recognition provides a favorable balance between usability and accuracy, although its performance is generally lower than fingerprint or iris recognition. This trade-off motivates the search for supplementary contextual attributes that may strengthen decision reliability.

In the context of this study, these principles form the conceptual basis for the experimental design described later in Section 8. The goal is to evaluate how auxiliary facial attributes can compensate for recognition accuracy losses caused by image degradation.

Table 1 Comparison of selected biometric modalities. Values indicate typical ranges under standard conditions.

Modality	Uniqueness	Acquisition effort	FAR (%)	FRR (%)
Fingerprint	High	Medium	<0.5	1–5
Iris	Very high	Low	<0.2	<1
Voice	Low	High	2–5	2–5
Face	Medium	Very high	1	1–3

4. CLOUD COMPUTING

Cloud computing delivers IT services, including data storage, servers, and software, over the internet, utilizing external databases for cost savings, scalability, and security [10]. The primary service models are Software as a Service (SaaS), which provides cloud-hosted applications accessible via web/API with automatic updates and scalability [11]; Platform as a Service (PaaS), which offers developers the necessary infrastructure and tools for application development and deployment without resource maintenance overhead [12]; and Infrastructure as a Service

(IaaS), which grants remote access to core computing resources (servers, networks, storage) for flexible scaling and capital expense reduction [13]. Organizations select from three main cloud types: the Public Cloud, where a provider manages resources over the public internet [14]; the Private Cloud, dedicated to a single customer, offering enhanced security and customization [15]; and the Hybrid Cloud, which combines public and private environments to optimize resource utilization and workload shifting [16]. The selection of a cloud type is driven by operational mode, data control, cost, security, and flexibility (see Table 2).

Table 2 Summary of cloud storage types

Type	Characteristics	Examples	Advantages / Limitations
Public	Operated by third parties with online access	Google Drive, Dropbox	+ Low cost, high availability – Limited control, potential privacy risks
Private	Internally managed, full control over data	ownCloud, Nextcloud	+ Enhanced security, customization – Higher cost, maintenance overhead
Hybrid	Combination of public and private infrastructures	Azure Stack	+ Flexible, balanced approach – Increased complexity, management effort

In biometric applications, cloud platforms enable large-scale computation for feature extraction, embedding comparison, and model deployment, but also introduce concerns regarding data confidentiality and integrity. For example, commercial services such as AWS Rekognition or Microsoft Azure Face API perform recognition through REST interfaces, transferring encoded facial data to external servers. This design facilitates scalability but poses privacy and compliance challenges.

In this work, the cloud serves not only as a computational backend for recognition tasks but also as a security-critical environment for storing and processing biometric embeddings. Therefore, the following section discusses typical risks associated with handling biometric data in cloud infrastructures.

5. SECURITY RISKS OF BIOMETRIC DATA

Biometric data are a crucial component of modern authentication systems, particularly in cloud environments where securing access to sensitive data and services is paramount. Their key advantages lie in their uniqueness and permanence, which eliminate issues such as forgotten passwords. However, these benefits come with significant security risks. The most prominent categories of threats include interception during communication, impersonation through spoofing, and direct compromise of biometric databases.

One major threat to biometric systems is the Man-in-the-Middle attack. This type of attack involves a third party secretly intercepting and possibly altering the communication between the user and the authentication system. Such attacks commonly occur in public spaces with unsecured Wi-Fi networks, where unencrypted data can be easily captured. Attackers aim to steal sensitive information like passwords or personal data, or to manipulate credentials for unauthorized access [17].

Another critical risk arises from face spoofing attacks, where attackers attempt to deceive face recognition systems by impersonating legitimate users. These attacks are generally divided into 2D and 3D categories. The 2D attacks include using printed photos, digital screen images, cut-out photos to simulate movement, deformed photos, and replaying videos that display natural facial behaviors such as blinking or head movements. These techniques exploit the limitations of many face recognition systems [18]. On the other hand, 3D attacks involve the use of realistic masks or replicas that imitate the full three-dimensional structure of a face, as well as more sophisticated methods like makeup or plastic surgery. These are much harder to detect using conventional anti-spoofing techniques [18].

Perhaps the most critical threat is the attack on biometric databases, where biometric templates are stored. Successful breaches can lead to severe privacy violations, identity theft, and misuse of biometric data. Attackers may steal biometric information for impersonation, sell it on black markets, or generate fake biometric templates to gain unauthorized access. Additionally, attackers might insert fake biometric data into the database, modify

legitimate templates to block access, or corrupt the data to disrupt system operations [19]. To mitigate these threats, several security measures are essential. Encrypting biometric data during storage and transmission is critical to prevent unauthorized disclosure. Employing multi-factor authentication that combines biometrics with other verification methods, such as one-time passwords or physical tokens, strengthens security considerably [20]. Systems should also implement continuous monitoring and regular software updates to quickly identify and address vulnerabilities [21]. Advanced liveness detection methods are necessary to distinguish between real users and spoofing attempts [18]. Finally, raising user awareness about potential security risks, such as avoiding public Wi-Fi for authentication and protecting biometric data on social media, helps reduce exposure to attacks [22].

An advanced technique called fuzzy encryption integrates secret cryptographic keys with biometric data. This method allows reliable reconstruction of the key during each authentication, despite the inherent variability in biometric measurements. Auxiliary data collected during enrollment assist in this process, but they must be carefully designed to avoid leaking sensitive biometric information, thereby preserving user privacy [23].

In summary, while biometric authentication offers strong security advantages due to the uniqueness of biometric traits, it is vulnerable to various sophisticated attacks, including man-in-the-middle interception, face spoofing, and database compromises. Implementing robust security strategies is therefore essential to protect biometric data, ensure user privacy, and maintain the integrity of authentication systems. The next section discusses technological measures and encryption mechanisms that address these vulnerabilities in more detail.

6. TECHNOLOGICAL CHALLENGES

Encryption techniques are essential for protecting biometric data against traditional threats, but must evolve to counter advanced attacks using big data and artificial intelligence. The main methods are symmetric and asymmetric encryption. Symmetric encryption uses a single key for both encryption and decryption, processing data in blocks for efficient handling of large datasets. Its main drawback is secure key distribution, since exposure of the key compromises data privacy [24].

Asymmetric encryption employs a public key for encryption and a private key for decryption. The public key is openly shared, while the private key remains confidential, enabling secure communication even when the encryption key is public. The authenticity of the public key must be verified to prevent manipulation by unauthorized parties [24]. This approach underpins Public Key Infrastructure, where the public key encrypts data and the private key decrypts it. For digital signatures, the private key signs and the public key verifies. Although mathematically linked, the keys have distinct roles and cannot substitute for each other. Asymmetric encryption ensures confidentiality, authentication, and integrity in digital communication [24]. For a more detailed

understanding of the differences, technical parameters, and practical implications of encryption methods in specific applications, see [25, 26].

Today, many companies use multiple cloud platforms simultaneously to leverage the strengths of different providers, enhancing efficiency, flexibility, and service reliability. However, multi-cloud environments introduce complexity, requiring advanced resource management and consistent security across platforms [27]. Key security challenges include managing vulnerabilities, regulating data transfers, handling identity and access management, and enforcing control mechanisms. Organizations must protect personal data, ensure privacy, address interoperability, and comply with regulations despite the distributed and heterogeneous nature of cloud infrastructures [28]. Consistent encryption, access control, and protection mechanisms across all cloud providers are essential to safeguard data confidentiality and integrity [27].

Federated access management enables unified access control across multiple cloud services by establishing mutual trust between identity and service providers. Trust relationships, either direct or third-party mediated, support secure, seamless access and collaboration within interconnected cloud environments [27].

In summary, the key technological challenge is to integrate modern encryption, cloud security, and biometric reliability into a single coherent framework. The following section describes the practical implementation of such a framework in the form of a cloud-based facial authentication platform.

7. DEVELOPMENT OF A FACIAL BIOMETRIC WEB PLATFORM

Building upon the concepts introduced in Section 6, a web-based platform was developed to support user authentication through facial biometrics. The system enables user registration and subsequent identity verification by capturing and comparing facial images. During registration, users provide a facial image and basic identification data, which are securely stored and later used for authentication. The platform was designed with two main objectives: achieving high recognition accuracy and ensuring robust protection of biometric and personal data. These principles make the system suitable for applications in security, digital identity management, and as a complementary factor in multimodal authentication frameworks.

7.1. System architecture

The system architecture is based on Amazon Web Services (AWS) technologies, leveraging Amazon Rekognition for facial analysis and comparison. AWS DynamoDB serves as the main database for metadata storage, while biometric images are stored in Amazon S3.

Data protection is ensured through AES-256 server-side encryption (SSE), and key management is handled via AWS Key Management Service (KMS), supporting both AWS-managed and customer-managed keys. This configuration provides flexibility for security policy customization and compliance with regulatory standards.

7.2. Front-End implementation

The front-end interface was implemented using the React framework, chosen for its modularity, responsiveness, and ability to interact with backend services in real time. During registration, users can upload facial images either by drag-and-drop or manual selection. Submitted data are immediately encrypted and transferred to DynamoDB and S3. Registered users can then authenticate by capturing a live image through a webcam, which is compared with their stored template. The system returns the user's name, confidence score, and additional analytical parameters such as estimated age range, gender, and emotional state. If no valid face is detected, the process is automatically halted and a warning message is displayed.

7.3. Security and liveness detection

To prevent spoofing attacks, a liveness detection mechanism differentiates live human input from non-genuine sources, such as printed or digital photos. Failed liveness checks result in authentication denial and an alert. This component substantially enhances the reliability of the biometric process and prevents unauthorized access.

All communication between the client and backend services is secured via HTTPS using TLS 1.2/1.3, ensuring end-to-end encryption. Biometric templates and metadata stored in AWS S3 and DynamoDB are encrypted with AES-256 SSE managed by AWS KMS. Access permissions follow the least-privilege principle through AWS Identity and Access Management policies, minimizing potential misuse.

7.4. Backend workflow

The backend integrates multiple AWS services into an event-driven architecture. Amazon S3 handles image storage, DynamoDB manages structured metadata, and AWS Lambda functions orchestrate communication between components. Upon registration or authentication, Lambda triggers data processing workflows that include image retrieval, feature extraction, and face matching via Rekognition. Each detected face is represented as a numerical embedding, and verification relies on the Euclidean distance between embeddings with an adjustable confidence threshold. Figure 1 illustrates the overall workflow, showing the interaction of recognition, encryption, and storage layers within the AWS ecosystem.

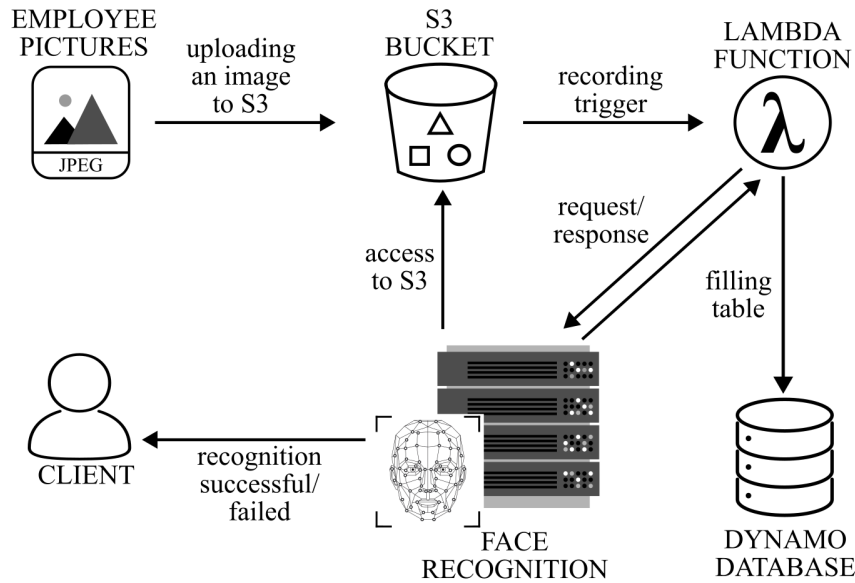


Fig. 1 Architecture of the AWS-based facial recognition system

7.5. Scalability and performance

By combining managed cloud services with end-to-end encryption and real-time inference, the proposed system achieves low latency, horizontal scalability, and high availability. The serverless design eliminates the need for persistent infrastructure, reducing maintenance overhead and potential attack surfaces. This architecture provides a scalable and privacy-preserving foundation for secure biometric authentication.

8. EXPERIMENTAL RESULTS

This section presents and discusses the experimental evaluation of the proposed cloud-based biometric platform, focusing on how image compression and degradation influence facial recognition accuracy, as well as the reliability of contextual attributes such as gender, age, and emotion. The experiments were designed to validate the hypothesis introduced in Section 1, namely that contextual information can improve recognition robustness under degraded conditions.

The AWS Rekognition service was tasked with comparing the similarity between a reference (uncompressed) photograph and various compressed or degraded versions of the same image. The objective was to assess how specific compression types and their intensities affect recognition accuracy. The evaluation focused on quantifying the relationship between image degradation level and recognition accuracy using a balanced dataset of 10 participants and 50 image samples. In addition to facial similarity testing, AWS Rekognition's gender, age, and emotion classifiers were evaluated.

All tests were conducted under consistent network and lighting conditions to ensure reproducibility and simulate realistic cloud-based authentication scenarios. The results provide insight into the practical reliability of combining

facial recognition with contextual attributes in real-world deployments and highlight areas where further optimization may be required.

8.1. Testing procedure

To evaluate the robustness of AWS Rekognition under varying image conditions, ten experimental trials were conducted. The dataset comprised 50 frontal facial images from 10 volunteers (5 males, 5 females) captured under controlled indoor lighting with a 1080p webcam. Each participant contributed five photos with neutral expressions and minor head pose variations (yaw $\pm 10^\circ$), with an average resolution of 1280×720 pixels.

For the compression and degradation experiments, one representative image per participant was selected, yielding 10 reference images. Each reference image underwent ten distinct transformations simulating different types and levels of degradation. In each trial, the system compared the reference image with its modified version to assess the impact on recognition performance. Transformations included JPEG and WebP compression (quality factors 10%, 50%, 90%), PNG bit-depth reductions via color quantization, Gaussian blur (kernel size 3×3), and block partitioning (block size 16×16 pixels), all implemented using OpenCV and Pillow in Python 3.10. Spatial dimensions were preserved to isolate degradation effects from scaling artifacts.

The design intentionally ranged from mild compression, simulating realistic cloud transmission, to extreme degradation representing worst-case conditions. This allowed a detailed analysis of AWS Rekognition's tolerance thresholds and practical reliability for real-world deployments. Table 3 summarizes the ten test cases and their resulting face-match similarity percentages.

Table 3 Facial match accuracy for different image compression methods

Trial	Compression Type	Parameters	Match Percentage
1	JPEG	90% quality	99.4%
2	JPEG	50% quality	92.8%
3	JPEG	10% quality	65.3%
4	WebP	90% quality	98.7%
5	WebP	50% quality	87.1%
6	PNG	8-bit palette	93.5%
7	PNG	4-bit palette	74.2%
8	Binarized PNG	1-bit monochrome	22.6%
9	Blur	Gaussian filter 3px	59.8%
10	Block compression	16x16 blocks	48.3%

8.2. Evaluation of results

To ensure statistical reliability, each similarity measurement was repeated 5 times per image, and reported match values represent the mean of 50 observations per compression category. The standard deviation across runs did not exceed $\pm 1.5\%$, confirming reproducibility. Average recognition latency per request was 1.2 seconds (± 0.3 s), including upload, inference, and response retrieval.

AWS Rekognition maintained high accuracy under mild lossy compression, with JPEG and WebP images at 90% quality achieving match rates above 98%. Moderate compression at 50% quality reduced accuracy to 87–93%, while extreme compression or severe degradations, such as binarization, Gaussian blur, or block artifacts, caused accuracy to drop to 22–60%. These results confirm that, although Rekognition is robust to typical web compression, it becomes unreliable when fine facial textures are lost, corroborating observations in [7].

Considering all transformations, the mean facial match score was 74.17%, with a standard deviation of 23.96%, indicating that performance is highly sensitive to visual quality and highlighting the need for adaptive confidence thresholds in practical deployments.

Gender Classification. AWS Rekognition demonstrated consistently high accuracy in gender classification. Out of 60 test images, 57 were correctly identified, resulting in an overall accuracy of 95%. All male participants were correctly classified, while a few misclassifications occurred among female participants, particularly in cases where facial features were less distinct or ambiguous (see Table 4).

Table 4 Results of gender classification testing

Gender	Image Count	Correctly Identified	Accuracy
Male	30	30	100%
Female	30	27	90%
Total	60	57	95%

Age Estimation. Age estimation performance was evaluated using the Mean Absolute Error (MAE) and accuracy within a ± 5 year range. The system achieved its best performance for younger participants, with an MAE of 3.2 years and an accuracy of 85%, whereas performance decreased for older individuals, with an MAE of 7.8 years and an accuracy of 40%.

This observed bias is consistent with findings from prior studies, which indicate that commercial age estimation models are predominantly trained on datasets containing a larger proportion of younger subjects [29]. Each age group was evaluated using 20 test images, corresponding to 3–4 participants per category, ensuring an equal number of attempts across all groups. This evaluation setup makes the results comparable across age ranges and prevents bias from unequal sampling. The detailed results are shown in Table 5.

Table 5 Age estimation results using regression

Age Group	Mean Absolute Error	Accuracy ± 5 years	Number of Attempts
18–30 years	3.2 years	85%	20
31–45 years	6.1 years	60%	20
46–60 years	7.8 years	40%	20
Overall	5.7 years	61.7%	60

Emotion Recognition. For emotion detection, AWS Rekognition was evaluated on six basic Ekman categories: joy, sadness, anger, surprise, disgust, and neutral [29]. The model achieved high accuracy for clear expressions, with joy correctly recognized in 95% of cases and surprise in 90%. Performance was lower for more ambiguous expressions, such as disgust, which was correctly identified in 55% of cases.

Misclassifications were frequently assigned to the neutral category, indicating that the system tends to make conservative predictions when confidence is low. The detailed classification results are summarized in Table 6.

Table 6 Multi-class emotion classification results

Emotion	Attempts	Correct Classifications	Accuracy
Joy	20	19	95%
Sadness	20	16	80%
Anger	20	14	70%
Surprise	20	18	90%
Disgust	20	11	55%
Neutral	20	17	85%
Total	120	95	79.2%

8.3. Discussion

Overall, the results highlight both the robustness and limitations of AWS Rekognition. While the system performs reliably under mild compression and in gender classification tasks, its performance degrades sharply under heavy distortions or subtle emotional expressions.

These findings empirically confirm that contextual cues (gender, emotion, age) can stabilize recognition outcomes when the primary biometric signal is partially degraded, thereby validating the central hypothesis of this study.

To contextualize these results, the performance of AWS Rekognition was conceptually compared with open-source frameworks such as OpenCV and FaceNet. In related studies, OpenCV-based recognition typically achieved 80–85% accuracy under moderate JPEG compression, while FaceNet's deep embeddings maintained 90–92%. The AWS-based approach exceeded both under mild degradations (98–99%), demonstrating the advantage of commercial cloud models trained on massive datasets.

However, the lack of algorithmic transparency and limited reproducibility remain critical drawbacks for scientific and forensic use.

In particular, the proprietary nature of AWS Rekognition prevents access to the underlying model architecture, training datasets, and feature extraction mechanisms. As a result, it is not possible to independently verify the fairness, bias, or internal decision criteria of the system.

These constraints limit the interpretability of the obtained results and make direct comparison with open-source models, such as FaceNet or ArcFace, only conceptual rather than methodological. For rigorous biometric benchmarking, future studies should therefore include at least one transparent baseline system that allows reproducible evaluation under identical conditions.

Furthermore, the experiments also illustrate why contextual attributes are useful in practical scenarios. Compression and degradation can lower the facial similarity score, even when the identity is correct. Emotional expression introduces similar uncertainty by temporarily shifting facial features. In both cases, contextual signals—particularly emotion, age, or gender—provide an additional source of evidence that can prevent false rejections and improve overall stability of the authentication pipeline.

8.4. Future recommendations

Future research should focus on expanding dataset diversity by including different lighting conditions, ethnicities, and poses, and on testing system robustness against real-world attacks such as print, replay, and deepfake spoofing. It is also important to examine emerging image compression techniques (e.g., AVIF, HEIC, neural codecs) to achieve better quality–size efficiency. Further improvements may be gained through adaptive authentication with fallback mechanisms such as two-factor verification, as well as through multimodal biometrics that combine facial, voice, or behavioral signals. Finally, strengthening privacy protection using differential privacy or homomorphic encryption would support secure cloud-based processing of sensitive biometric data.

In summary, the experiments show that while cloud-based biometric services can maintain high recognition reliability under controlled compression, they require careful adaptation and additional contextual analysis to

ensure trustworthy and privacy-preserving deployment in real-world conditions.

9. CONCLUSIONS

This study investigated the potential of enhancing facial biometric authentication by incorporating demographic and emotional attributes within a cloud-based environment. The prototype implementation demonstrated that contextual features such as gender, age, and emotion can complement traditional face recognition and partially mitigate the effects of degraded image quality. The experimental evaluation showed that the system maintains satisfactory performance under mild image compression, while stronger distortions lead to recognition accuracy falling below acceptable levels.

Methodologically, the results indicate that commercially available cloud services can serve as a proof-of-concept platform for biometric research. At the same time, their use introduces limitations regarding reproducibility and the assessment of algorithmic transparency. The study also highlights the critical importance of dataset diversity, robust security measures, and privacy-aware design in the deployment of practical biometric systems.

Future work should aim to address these limitations by evaluating larger and more heterogeneous datasets, employing open-source algorithms for benchmarking, and expanding the security analysis to include adversarial attacks and deepfake scenarios. Investigating advanced privacy-preserving techniques, including differential privacy and homomorphic encryption, would further enhance compliance with data protection regulations.

The proposed system establishes a foundation for secure web-based identity verification platforms. Incorporating emotional and demographic context can improve user experience and increase trust in biometric authentication. Extending this approach to multimodal authentication schemes that integrate facial biometrics with additional modalities such as voice, gesture, or behavioral traits is expected to enhance resilience against spoofing attacks and enable adaptive, context-aware authentication in real-world applications.

ACKNOWLEDGEMENT

The research was supported by the Ministry of Education, Research, Development and Youth of the Slovak Republic under the projects KEGA 049TUKE-4/2024 & KEGA 041TUKE-4/2025, by the Slovak Research and Development Agency under the projects APVV-22-0414 & APVV-22-0261, as well as by the Erasmus+ MetaCog 2024-1-FI01-KA220-HED-000247530 project and KeDiTeWiBreTNe 09I05-03-V02-00019 project.

REFERENCES

- [1] SOEKARTA, R. – KU-MAHAMUD, K. R.: *Recent facial image preprocessing techniques: A review*, *Engineering Proceedings*, vol. 84, no. 1, p. 39, 2025. [Online]. Available:

- <https://www.mdpi.com/2673-4591/84/1/39>.
doi: 10.3390/engproc2025084039
- [2] TANWAR, S. – TYAGI, S. – KUMAR, N. – OBAIDAT, M. S.: *Ethical, legal, and social implications of biometric technologies*, in *Biometric-based physical and cybersecurity systems*, Springer, 2018, pp. 535–569.
 - [3] LI, C. – WANG, L. – JI, S. – ZHANG, X. – XI, Z. – GUO, S. – WANG, T.: “Seeing is Living? Rethinking the Security of Facial Liveness Verification in the Deepfake Era,” in *Proc. 31st USENIX Security Symposium (USENIX Security 22)*, pp. 2673–2690, 2022.
 - [4] YU, Z. – CAI, R. – LI, Z. – YANG, W. – SHI, J. – KOT, A. C.: “Benchmarking joint face spoofing and forgery detection with visual and physiological cues,” *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 5, pp. 4327–4342, 2024.
 - [5] WANG, M. – QIN, Y. – LIU, J. – LI, W.: “Privacy protection framework for face recognition in edge-based IoT,” *Frontiers in Psychology*, vol. 13, 2022. doi: 10.3389/fpsyg.2022.1018137
 - [6] DEY, M. – MONDAL, A., Et al.: “Ensuring privacy in face recognition: a survey on data generation, inference and storage,” *SN Applied Sciences*, vol. 7, no. 2, 2025. doi: 10.1007/s42452-025-06987-2
 - [7] VERDOLIVA, L.: “Media Forensics and DeepFakes: An Overview,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 5, pp. 910–932, 2020. doi: 10.1109/JSTSP.2020.3002101
 - [8] JAIN, A. K. – ROSS, A. – PRABHAKAR, S.: “An introduction to biometric recognition,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.
 - [9] TIWARI, S. – RAJA, R. – WADAWADAGI, R. S. – NAITHANI, K. – RAJA, H. – INGLE, D.: “Emerging biometric modalities and integration challenges,” in *Online Identity—An Essential Guide*, IntechOpen, 2024.
 - [10] SADEEQ, M. M. – ABDULKAREEM, N. M. – ZEEBAREE, S. R. M. – AHMED, D. M. – SAMI, A. S. – ZEBARI, R. R.: IoT and cloud computing issues, challenges, and opportunities: A review. In *Qubahan Academic Journal*, volume 1, number 2, pages 1–7, 2021.
 - [11] RAHMAN, A. – SUBRIADI, A. P.: Software as a service (SaaS) adoption factors: individual and organizational perspective. In *2022 2nd International Conference on Information Technology and Education (ICIT&E)*, pages 31–36, IEEE, 2022.
 - [12] GOHIL, R. – PATEL, H.: Comparative analysis of cloud platform: Amazon Web Service, Microsoft Azure, and Google Cloud Provider: A review. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pages 1–5, IEEE, 2024.
 - [13] ALETABI, H. – ABDALLAH, M.: A proposed cloud quality model (IaaSQual) for “Infrastructure as a Service (IaaS)” from user’s perspective. In *2023 International Conference on Information Technology (ICIT)*, pages 695–699, IEEE, 2023.
 - [14] DENG, H. – QIN, Z. – WU, Q. – GUAN, Z. – DENG, R. H. – WANG, Y. – ZHOU, Y.: Identity-based encryption transformation for flexible sharing of encrypted data in public cloud. *IEEE Transactions on Information Forensics and Security*, 15:3168–3180, IEEE, 2020.
 - [15] DHAYA, R. – UJWAL, U. J. – TRIPTI SHARMA – PRABHDEEP SINGH – KANTHAVEL, R. – SENTHAMIL SELVAN – KRAH, D.: Energy-efficient resource allocation and migration in private cloud data centre. *Wireless Communications & Mobile Computing (Online)*, 2022, Hindawi Limited, 2022.
 - [16] AZAD, M. W. A. – SHANNIGRAHI, S. – STERGIOU, N. – ORTEGA, F. R. – MASTORAKIS, S.: Cledge: A hybrid cloud-edge computing framework over information centric networking. In *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, pages 589–596, IEEE, 2021.
 - [17] ASLAN, Ö. – AKTUĞ, S. S. – OZKAN-OKAY, M. – YILMAZ, A. A. – AKIN, E.: “A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions,” *Electronics*, vol. 12, no. 6, p. 1333, 2023.
 - [18] ANTHONY, P. – AY, B. – AYDIN, G.: “A review of face anti-spoofing methods for face recognition systems,” in *2021 International Conference on INnovations in Intelligent SysTems and Applications (INISTA)*, 2021, pp. 1–9.
 - [19] SAI, G. H. – TYAGI, A. K. – SREENATH, N.: “Biometric security in Internet of Things based system against identity theft attacks,” in *2023 International Conference on Computer Communication and Informatics (ICCCI)*, 2023, pp. 1–7.
 - [20] MEHRAJ, H. – JAYADEVAPPA, D. – HALEEM, S. L. A. – PARVEEN, R. – MADDURI, A. – AYYAGARI, M. R. – DHABLIYA, D.: “Protection motivation theory using multi-factor authentication for providing security over social networking sites,” *Pattern Recognition Letters*, vol. 152, pp. 218–224, 2021.
 - [21] LEMBKE, J. – RAVI, S. – ROMAN, P. L. – EUGSTER, P.: “Secure and reliable network updates,” *ACM Transactions on Privacy and Security*, vol. 26, no. 1, pp. 1–41, 2022.
 - [22] VIGNESH, S. – DURGASHIVANI, S. – HARIDA, W.: “Create an Intrusion Detection System to Detect Threats in Public WiFi Networks,” in *2025 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, vol. 3, pp. 1–6, 2025.

- [23] WANG, M. – QIN, Y. – LIU, J. – LI, W.: “Identifying personal physiological data risks to the Internet of Everything: the case of facial data breach risks,” *Humanities and Social Sciences Communications*, vol. 10, no. 1, pp. 1–15, 2023.
- [24] GUDIMETLA, SANDEEP REDDY: Data Encryption in Cloud Storage. *International Research Journal of Modernization in Engineering Technology and Science*, vol. 6, 2024, pp. 2582–5208.
- [25] LEVICKÝ, D. – BRODA, M. – ŠIMKO, E.: *Kybernetická bezpečnosť*. 1. vyd. Košice: Technická univerzita v Košiciach, 2025. 160 s. ISBN 978-80-553-4770-7.
- [26] LEVICKÝ, D.: *Aplikovaná kryptografia*. 1. vyd. Košice: Elfa, 2018. 437 s. ISBN 978-80-8086-265-7.
- [27] SOMASUNDARAM, P.: “Enhancing security in multi-cloud environments through federated access control,” *International Journal of Computer Engineering and Technology (IJCET)*, vol. 14, no. 2, pp. 90–96, 2023.
- [28] POOKANDY, J.: “Multi-factor authentication and identity management in cloud CRM with best practices for strengthening access controls,” *International Journal of Information Technology and Management Information Systems (IJITMIS)*, vol. 12, no. 1, pp. 85–96, 2021.
- [29] COPPINI, S. – LUCIFORA, C. – VICARIO, C. M. – GANGEMI, A.: “Experiments on real-life emotions challenge Ekman’s model,” *Scientific Reports*, vol. 13, no. 1, p. 9511, 2023.

Received October 20, 2025, accepted December 4, 2025

BIOGRAPHIES

Eva Kupcová is currently a Ph.D. student at the Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics, Technical University of Košice. She is in the third year of her doctoral studies, expected to be completed in 2026. Her research focuses on the cryptographic protection of biometric data. She obtained her master’s degree in 2023 with a thesis titled “Implementation of the OPAQUE Protocol for IoT Devices”, which was awarded as the best master’s thesis by the company Ness.

Matúš Pleva received his Ph.D. in telecommunications from the Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics, Technical University of Košice, in 2010. He is currently an Associate Professor in informatics and Head of the Department. His research interests include acoustic modeling, acoustic event detection, speaker recognition, speech processing, human–machine interaction, embedded systems and parallel computing, security and biometrics, computer networking, and IoT. He is a member of ACM and HiPEAC.

Zuzana Sokolová received her Ph.D. from the Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics, Technical University of Košice, in August 2024. She is currently working as an Assistant Professor at the same department. Her research focuses on natural language processing, particularly on the detection of hate speech, offensive language, and toxic language. In July 2021, she was awarded a certificate for outstanding university work related to Artificial Intelligence from Huawei.

Jakub Bajo received his bachelor’s degree from the Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics, Technical University of Košice. His research interests focus on security and biometric systems.