https://doi.org/10.17221/35/2025-RAE

Camera systems and their user recognition reliability when entering an agri-food complex

Jaroslav Mrázek[1]*, *Jakub Vošáhlík*[2], *Eva Olmrová*[1], *Martin Pexa*[1], *Zdeněk Aleš*[1], *Jakub Čedík*[1]

[1]*Department for Quality and Dependability of Machines, Faculty of Engineering, Czech University of Life Sciences Prague, Prague, Czech Republic*

[2]*Department of Technological Equipment of Constructions, Faculty of Engineering, Czech University of Life Sciences Prague, Prague, Czech Republic*

**Corresponding author: mrazekjaroslav@tf.czu.cz*

Citation: Mrázek J., Vošáhlík J., Olmrová E., Pexa M., Aleš Z., Čedík J. (2025): Camera systems and their user recognition reliability when entering an agri-food complex. Res. Agr. Eng., 71: 105–112.

Abstract: This study evaluates the efficiency of various facial recognition camera systems used to control access in agri-food production environments, focusing on their ability to identify individuals based on biometric facial traits. It is also important to prevent the movement of unwanted persons into the production premises in the agri-food complex. The main goal was to assess how these factors influence the recognition performance and to determine the most reliable system for preventing unauthorised entry. The results show notable performance disparities between the devices tested. It can be concluded in this research that there are statistically significant differences between the maternal, professional and semi-professional systems. The device that is most suited is the HIKVISION iDS-2CD8426G0/F-I, achieving the best average performance score. This is based on usual recognition times. These tests indicate that the HIKVISION DS-2DE7232IW-AE(S5), which obtained an average rating of 2.216789, is the second-best acceptable device. With a score of 2.842113, HIKVISION DS-2CD2H45FWD-IZS (2.8–12 mm) (B) received, without a doubt, the lowest ranking. Given the outcomes, systems with superior recognition capabilities like the iDS-2CD8426G0/F-I are best to use for critical access control applications and to also minimise the use of facial coverings in sensitive areas to ensure reliable identification and higher levels of security of agri-food complexes.

Keywords: security; agricultural buildings; ergonomics; facial recognition; face detection

In connection with the risks associated with property crime, there is a growing need to secure sensitive agro-industrial facilities, such as pharmaceutical, chemical or food factories, by restricting access only to verified persons. Biometric facial recognition offers a promising method to secure access to high-risk agricultural structures against unauthorised entry. Because illegal behaviour can result in serious negative effects (chemical leak, escape of viruses and bacteria, theft of regulated materials, etc.). (Hartová & Hart 2017, Rouast et al. 2019)

It makes sense to leverage the current methods for recognising a person's identification by recognising their facial characteristics for this purpose. Such technologies are primarily implemented to block access by individuals lacking the proper au-

Supported by the grant support – CZU: Project No. 31190/1414|1633/4134; TAČR FW – TREND: FW06010124 – Predictive maintenance of machinery using statistical and operational data in Industry 4.0.

thorisation. Cameras designed for this purpose are typically equipped with advanced sensors that can capture footage in a 1 080 p resolution or higher, functioning reliably in both daylight and night-time conditions. These systems are usually also coupled with artificial intelligence and machine learning algorithms to improve their accuracy and ideally reduce the rate of false alarms. (Pramerdorfer and Kampel 2016; Hartová et al. 2018; Al-Obaydy & Suandi 2019; Benjamin at al. 2023).

Simple camera systems employ an extra storage capacity that guarantees the formula's output for identity identification. Higher-end recording devices often combine built-in facial recognition software with compact memory units such as Micro SSD cards for efficient data management (Mahdi et al. 2017; Wang et al. 2018; Tan et al. 2019).

One commonly used technique in facial recognition software is the Eigenfaces algorithm, which leverages Haar-like features to analyse and classify facial structures. In terms of interference and obstructive recognition, facial recognition is a large and difficult task. Changes in facial expression, angle rotation, distance to the scanned face, and, in particular, head and face covers are examples of these issues. These factors primarily influence the likelihood of mistaken rejections and the time required to identify an individual (Nagano et al. 2019; Li and Deng 2020; Vošáhlík & Hart 2020).

In addition to camera systems with a facial recognition function, there are other biometric methods that can be used to protect agricultural buildings. Fingerprinting is one of the most common biometric methods because it is highly accurate and reliable, which is a widely used and proven technology in many other areas. Today, this biometric security system is commonly used to protect access to mobile phones or instead of traditional keys when entering the home. Compared to facial recognition, which is also a common part of mobile phone protection, fingerprinting has the disadvantage that it requires physical contact with the sensor, which can be hygienically problematic in the agri-food complex. Another possible problem lies in the possibility of moisture or dirt affecting the quality of the sensing (Karu & Jain 1996; Jiang et al. 2006; Yang et al. 2024).

Within the European Union and the General Data Protection Regulation (GDPR), biometric data falls into a special category of personal data where the user's explicit consent is required, or the existence of another legal reason, such as security. One of the most problematic areas is to ensure the maximum security of the data to prevent misuse, as biometric data are unique and unmistakable, and if leaked, cannot be remedied (Vojkovic & Milenkovic 2018; Jasserand 2022).

Another important topic when using cameras with facial recognition is the line between security and privacy. For example, if cameras are used to monitor an employee throughout their shift, it may be an invasion of privacy. However, if the cameras are used only to evaluate entry into secure zones, they should be ethically acceptable (Smith & Miller 2022; Beltrán & Calvo 2023; Hasan et al. 2023).

Highly organised thieves steal expensive tractors and loaders. Criminals also steal expensive GPS guidance tractor kits, which typically cost around 10 000 GBP. While initial claims predicted a 20% rise in tractor thefts by the end of 2023, the National Farmers Union (NFU) Mutual's latest report from 2024 shows that although tractor theft actually fell by 9%, there was a dramatic 137% increase in GPS thefts, highlighting a shift in the criminal focus towards high-value, easily portable farm technology. Installing such systems can help to significantly reduce the number of thefts and also to increase, with the right choice of camera recognition system, the friendliness of the end users who have access to the agri-food facility.

The main aim of the article is to evaluate the applicability and effectiveness of camera systems in recognising and identifying individuals based on facial features within an agri-food complex.

MATERIAL AND METHODS

The face recognition camera systems chosen for the test series are: HIKVISION (Hangzhou Hikvision Digital Technology Co., Ltd., China), models DS-2CD2H45FWD-IZS (2.8–12 mm) (B), DS-2DE7232IW-AE(S5), and iDS-2CD8426G0/F-I for professionals. The DS-2CD2H45FWD-IZS (2.8–12 mm) (B) is the least expensive of the aforementioned models and is primarily intended for use by the general population. The HIKVISION model DS-2DE7232IW-AE is a representation of a semi-professional gadget. A camera system designed for professional use in identifying individuals based on their facial features, the HIKVISION iDS-2CD8426G0/F-I, is the third tested gadget.

https://doi.org/10.17221/35/2025-RAE

Table 1. Technical specifications of the individual cameras

Camera	Type	Resolution	IR illumination range	Features	Effective identification range
HIKVISION iDS-2CD8426G0/F-I	Bi-spectral (RGB + IR)	1920 × 1080 (visible), 640 × 480 (IR)	up to 5 m	face detection, dual imaging	3–5 m
HIKVISION DS-2DE7232IW-AE(S5)	PTZ IP camera	1920 × 1080 (2 MP)	up to 150 m	auto-tracking, motion detection	up to 100 m (tracking), 15–25 m (identification)
HIKVISION DS-2CD-2H45FWD-IZS (B)	IP camera with motorized zoom	2688 × 1520 (4 MP)	up to 30 m	120 dB WDR, motion detection	10–20 m

The complete specifications of the individual cameras are listed in Table 1, and their design is shown in Figure 1.

The measurement was carried out to find the typical amount of time required by the camera system to identify a person. It was important to provide the most constant settings in order to correctly assess the average time value of the facial recognition camera systems. A room with white walls that was not filled with distracting objects (paintings, photos, or animals) was utilised. The temperature in the room was kept at 23 °C. With the CEM DT-3809 light meter, the light intensity for the measurement was determined to be 374 lux with a 10% tolerance.

The camera units were positioned on a table and directed toward the centre of the room, where the test participants entered. While evaluating the systems' recognition timing, each person opened the door, stepped into the room, and stood approximately 80 cm in front of the camera lens. After each measurement, the individual exited the space and paused for 30 sec before the next scanning attempt.

To achieve precise and consistent timing data, a personal computer was utilised to record how long the system took to identify each participant. A maximum window of 10 sec was allocated for each recognition attempt; if the system failed to identify the person within that period, the attempt was labelled as "unsuccessful".

The recorded data reflected the duration required by the camera system to detect and identify an individual based on their unique facial characteristics. A total of five distinct test types were carried out. These involved recording the time necessary to recognise an unobstructed face, as well as the recognition time when the individual wore glasses. Another test focused on identifying a face partially covered by a scarf around the neck and chin, while a separate scenario examined the recognition with a baseball cap obscuring part of the face. The final test assessed how long it took the system to identify a person based solely on their facial features. Five people underwent the measurement (2 men and 3 women). Ten measurements were taken repeatedly for each subject and each gadget throughout each test. To ensure the utmost level of accuracy, each test was run twice. Consequently, each test on a single individual using one device produced a dataset comprising 100 recorded measurement values. On all the devices, all the individuals, and in all the tests, 1 500 recorded readings were assessed in accordance with unpaired *t*-test statistics. The recognition

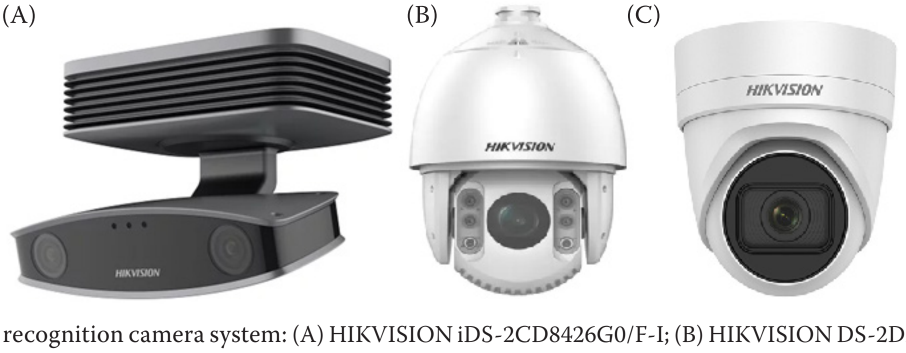

Figure 1. Tested recognition camera system: (A) HIKVISION iDS-2CD8426G0/F-I; (B) HIKVISION DS-2DE7232IW-AE(S5); (C) HIKVISION DS-2CD2H45FWD-IZS (2.8–12 mm)

system already had pre-recorded profiles of the test persons and the recognition time was examined.

Statistical analyses were conducted using the Statistica program, employing unpaired t-tests for group comparisons and both Friedman's test and Kendall's coefficient of concordance to assess the conformity and consistency of the individual measurement results.

(H_0): Facial obstructions have no significant effect on the speed or accuracy of the facial recognition in camera-based identification systems.

(H_1): Facial obstructions significantly affect the speed and/or accuracy of the facial recognition in camera-based identification systems.

RESULT AND DISCUSSION

The HIKVISION iDS-2CD8426G0/F-I system achieved the fastest identification time among the three evaluated facial recognition cameras (Figure 2) and consistently delivered the highest recognition accuracy in all the test scenarios. In the test without any facial covering, the mean recognition duration was 0.87 s. When glasses were worn, the average identification time extended to 2.06 s. In the third scenario, where a scarf partially covered the face, the system recorded an average time of 1.46 s. For the fourth test, which included a baseball cap as the facial obstruction, the mean duration reached 3.37 s. The final test, combining all the previous obstructions, resulted in an average processing time of 6.09 s.

A mediocre average time value was obtained for the second device under evaluation, the HIKVISION DS-2DE7232IW-AE(S5) (Figure 3). The device's average recognition time in the initial test, which did not cover the face, was 2.04 s The average time in the second test was 2.87 s when wearing glasses. These readings reached 2.24 s in the third. The average recognition time for the baseball cap in the fourth test was 3.68 s. The average recognition time in the last test, when all the preceding components were combined, was 6.47 s.

The slowest recognition times were attained by the third device under evaluation, the HIKVISION DS-2CD2H45FWD-IZS (2.8–12 mm) (B) (Figuer 4), where 2.87 s were spent in the first test without a face cover. It reached 5.11 s in the second test while wearing glasses. The third test, a scarf-covering one, finished in 4.01 s. It received an average recognition value of 6.84 s in the fourth test while wearing a baseball cap. It achieved 8.19 s in the last and most difficult test as a result of the application of all the earlier components.

The measured values were subjected to unpaired statistical *t*-tests using the Statistica program. The following outcomes were attained by applying the measured data in accordance with these tests. Except for a few tests, every test's *P*-value was higher than 0.05 ($P > 0.05$). (Table 2). With the exception of the experiments, we can reject the idea that different devices with varied face masks will provide equal measurement times.

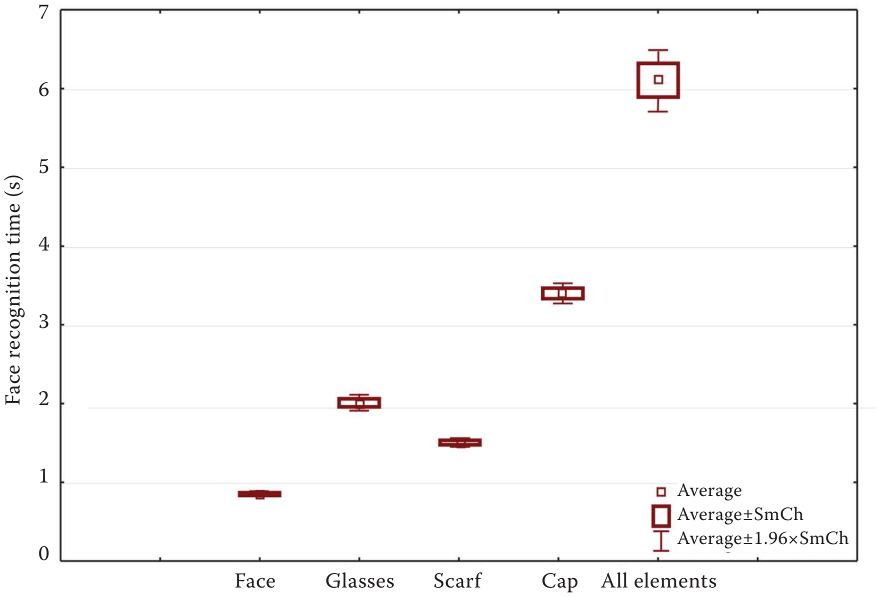

Figure 2. Results of the average recognition time by the HIKVISION iDS-2CD8426G0/F-I

https://doi.org/10.17221/35/2025-RAE

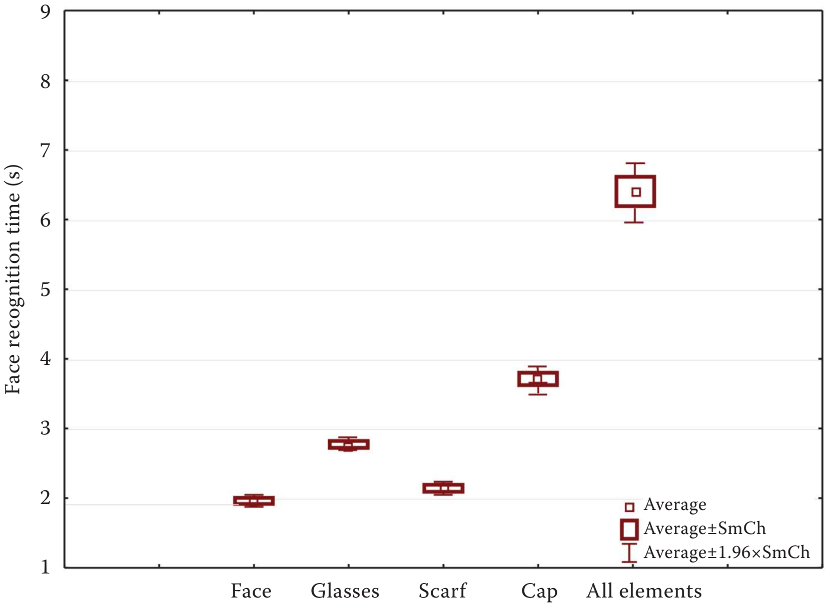

Figure 3. Results of the average recognition time by the HIKVISION DS-2DE7232IW-AE(S5)

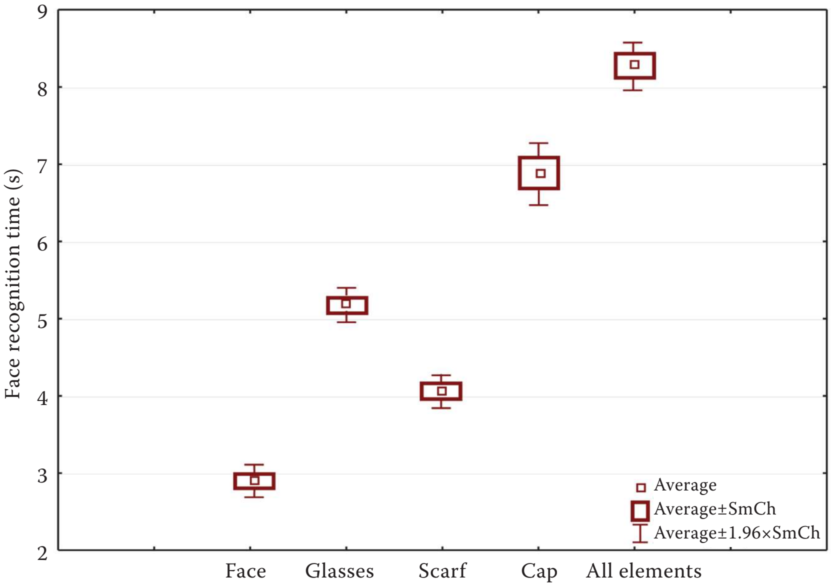

Figure 4. Results of the average recognition time by the HIKVISION DS-2CD2H45FWD-IZS (2.8–12 mm) (B)

On the basis of these unpaired *t*-tests, we cannot rule out the possibility that different devices with various face coverage practices may yield measurements with a comparable measurement duration. Intriguingly, the Glasses vs. Scarf test type produced the highest equality of the applied

Table 2. Results of the applied *t*-tests

Type of cameratype of test (group 1 vs. 2)	Type of test	Averagetime of group 1	Averagetime of group 2	*t* value	*P* value
C vs. B	all elements vs all elements	6.147	6.713	–1.3817	0.215471
B vs. A	all elements vs hat	6.319	7.341	–1.8945	0.055509
C vs. B	glasses vs scarf	2.072	2.097	–0.0499	0.914754
B vs. A	glasses vs face	2.841	2.578	1.7410	0.068313

A – HIKVISION DS-2CD2H45FWD-IZS (2.8-12 mm) (B); B – HIKVISION DS-2DE7232IW-AE(S5); C – HIKVISION iDS- 2CD8426G0/F-I (B)

Table 3. Applied Friedman's test and Kendall's conformity test for the uncovered face

Type of test and camera system	Average rank	Sum order	Average	Standard deviation
Uncovered face A	2.842113	191.000	2.632541	0.056482
Uncovered face B	2.216789	164.000	1.896264	0.395681
Uncovered face C	1.000000	67.000	0.798456	0.156127

Table 4. Applied Friedman's test and Kendall's conformity test for all the elements

Type of test and camera system	Average rank	Sum order	Average	Standard deviation
Uncovered face A	2.333333	14.0000	8.174426	0.934714
Uncovered face B	1.933333	11.5000	6.148732	1.455272
Uncovered face C	1.833333	11.0000	7.247148	1.754353

t-tests for the HIKVISION iDS-2CD8426G0/F-I vs. the HIKVISION DS-2DE7232IW-AE(S5).

In the applied unpaired testing with different devices, but the same face-covering concept, the main finding is that we consistently reject the hypothesis, with one notable exception. This exception reflects the device HIKVISION iDS-2CD8426G0/F-I vs. HIKVISION DS-2DE7232IW-AE in testing faces covered by all the elements (S5). In this instance, it is impossible to reject the hypothesis. In this application, both devices show comparable results, however, with other applications, they drastically diverge. The assessment of conformity for the individual measurement results on the exposed face was definitively determined using the statistical tests of Friedman and Kendall in the Statistica software (Table 3).

Based on typical recognition times, the device that is most suited is the HIKVISION iDS-2CD8426G0/F-I, which has a rating of 1. According to these tests, the second suitable device is the HIKVISION DS-2DE7232IW-AE(S5), which received an average rating of 2.216789. HIK VISION DS-2CD2H45FWD-IZS (2.8–12 mm) (B) obtained indisputably the lowest ranking with a rating of 2.842113. In the subsequent graph, you can observe the concluding mean figures from Friedman's assessment and Kendall's verification test (Figure 5).

The assessment of conformity for each element in the additional results statistics was explicitly outlined in the individual measurement results for the Friedman test and Kendall's conformity test used in Statistica software. (Table 4).

It is unclear which gadget would be best given the typical recognition times. In this instance of identification, the HIKVISION DS-2DE7232IW-AE(S5) and iDS-2CD8426G0/F-I are nearly on par. With a rating of 2.842113, the HIKVISION DS-2CD2H45FWD-IZS (2.8–12 mm) (B) unquestionably received the bottom spot. The following graph illustrates the final average values of Friedman's test and Kendall's conformity test (Figure 6).

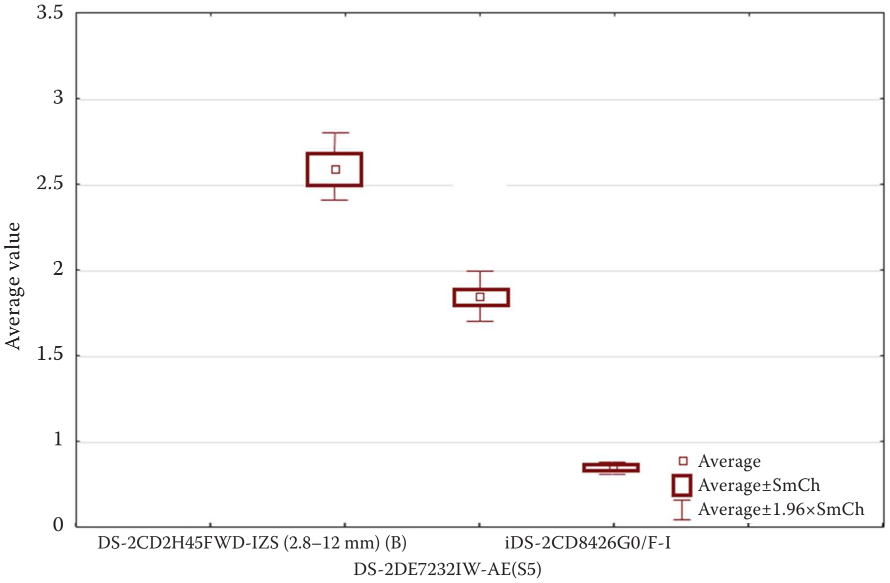

Figure 5. Average results from Friedman's test and Kendall's concordance test

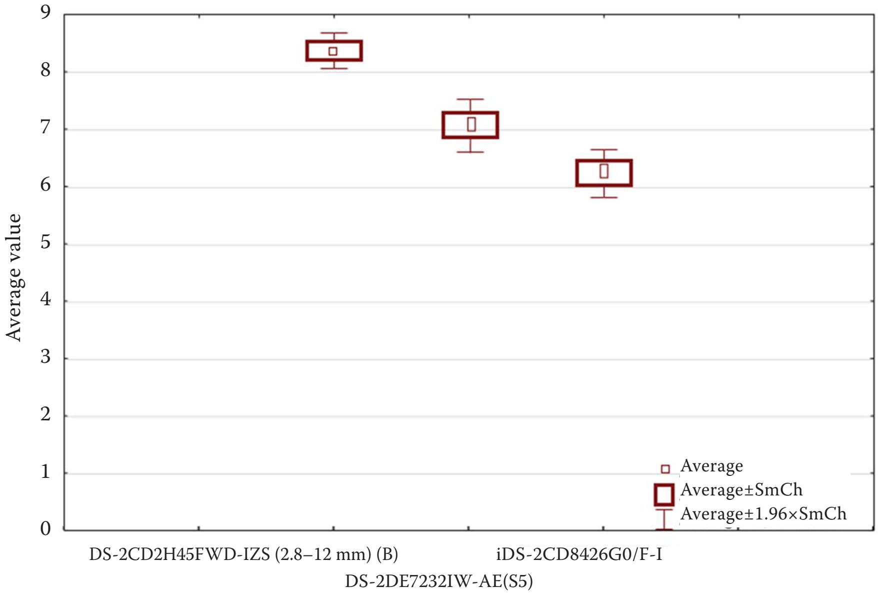

Figure 6 Average values of Friedman's test and Kendall's conformity test

According to the latest research findings, the systems capacity to identify an individual is significantly diminished by the progressive masking of facial features during identification. In the article "Deep face recognition imperfect facial data", this has previously been discussed. Such studies address facial detection and a person's identification in great detail. It also contains a portion of the facial covering and the software's partial disposal of it. This study suggests that in order to enhance the general system recognition qualities, an uncovered face should be used without any items (Elmahmudi & Ugail 2019).

This paper shows the results where facial masking significantly slows down the identification and also reduces the accuracy of recognising a person. A similar problem is addressed by the study "Efficient Fine-tuning Strategies for Enhancing Face Recognition Performance in Challenging Scenarios", which proposes the DPEFT method (Data-Parameter-Efficient Fine-Tuning), which allows for the effective adaptation of facial recognition models even when the face is masked. Unlike our study, which focused on the performance of specific cameras, DPEFT focuses on optimising artificial intelligence algorithms. Here, the authors use DPEFT to demonstrate that the appropriate tuning of models can improve the camera performance in less-than-ideal conditions. This suggests that, in addition to high-quality hardware, advanced software also plays a very important role, which could lead to improved security systems (Lin et al. 2025)

CONCLUSION

Among the tested devices, the HIKVISION iDS-2CD8426G0/F-I camera identification system demonstrated the highest effectiveness for identification purposes. In contrast, the performance of the other detectors was significantly lower, making them unsuitable for preventing unauthorised access into the agri-food facilities.

Among the three facial recognition camera systems that were tested, the HIKVISION iDS-2CD8426G0/F-I system demonstrated the fastest and most consistent identification performance across all the scenarios. It achieved the shortest average recognition times, even under varying conditions such as wearing glasses, scarves, or baseball caps.

The HIKVISION DS-2DE7232IW-AE(S5) system showed mediocre performance, with recognition times increasing slightly under face-covering conditions, but still remaining within an acceptable range.

The HIKVISION DS-2CD2H45FWD-IZS (2.8 to 12 mm) (B) system recorded the slowest recognition times in all the tests, especially when multiple facial obstructions were combined, indicating a limited effectiveness in challenging identification scenarios.

We reject the null hypothesis and accept the alternative hypothesis, confirming that facial obstructions, such as masks or hats, can significantly delay recognition processes and reduce the accuracy of camera-based identification systems. The measured data show that when the face

https://doi.org/10.17221/35/2025-RAE

is disguised, the device's processing time increases and negatively impacts the process of accurately identifying a person.

Consequently, it is advised, in agri-food complexes, based on the findings of this assessment, that one should avoid the use of face coverings, as doing so precludes the unmistakable identification of the person by distinctive facial characteristics. Eliminating this step from the identification process will undoubtedly enhance and raise the bar for protection against unwanted access.

REFERENCES

Al-Obaydy W.N.I., Suandi S.A. (2019): Automatic pose normalization for open-set single-sample face recognition in video surveillance. Multimedia Tools and Applications, 79: 2897–2915.

Beltrán M., Calvo M. (2023): A privacy threat model for identity verification based on facial recognition. Computers & Security, 132: 103324.

Benjamin J., Biggs H., Berger A., Rukanskaitė J., Heidt M.B., Merrill N., Pierce J., Lindley J. (2023): The entoptic field camera as metaphor-driven research-through-design with AI technologies. CHI '23, 178: 1–19.

Elmahmudi A., Ugail H. (2019):. Deep face recognition using imperfect facial data. Future Generation Computer Systems, 99: 213–225.

Hartová V., Hart J. (2017): Comparison of reliability of false rejection rate by monocriterial and multi-criteria of biometric identification systems. Agronomy Research, 15: 999–1005.

Hartová V., Hart J., Prikner P. (2018): Influence of face lighting on the reliability of biometric facial readers. Agronomy Research, 16: 1025–1031.

Hasan M.R., Guest R., Deravi F. (2023): Presentation-level, privacy protection techniques for automated face recognition – A survey. ACM Computing Surveys, 55: 1–27.

Jasserand C. (2022): Research, the GDPR, and mega biometric training datasets: Opening the Pandora Box 1. In: Proc. 21th Int. Conf. Biometrics Special Interest Group (BIOSIG 2022), Darmstadt, Sept 14–19, 2022: 193–204.

Jiang X., Liu M., Kot A.C. (2006): Fingerprint Retrieval for Identification. IEEE Transactions on Information Forensics and Security, 1: 532–542.

Karu K., Jain A.K. (1996): Fingerprint classification. Pattern Recognition, 29: 389–404.

Li S., Deng W. (2020): Deep facial expression recognition: A survey. IEEE Transactions on Affective Computing, 11: 1–17.

Lin Y., Wu Z., Huang Q., Liu X., Yin B., Hu J. (2025): Efficient fine-tuning strategies for enhancing face recognition performance in challenging scenarios. In: Proc. 2025 IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP), Hyderabad, Apr 6–11, 2025: 1–5.

Mahdi F.P., Habib M., Ahad A.R., Mckeever S., Moslehuddin A.S.M., Vasant P., Watada J. (2017): Face recognition-based real-time system for surveillance. Intelligent Decision Technologies, 11: 79–92.

Nagano K., Luo H., Wang Z., Seo J., Xing J., Hu L., Wei L., L, H. (2019): Deep face normalization. ACM Transactions on Graphics, 38, 1–16.

Pramerdorfer C., Kampel M. (2016): Facial expression recognition using convolutional neural networks: State of the art. arXiv preprint, arXiv: 1612.02903.

Rouast P.V., Adam M.T.P., Chiong R. (2019): Deep learning for human affect recognition: Insights and new developments. IEEE Transactions on Affective Computing, 10: 530–543.

Smith M., Miller S. (2022): The ethical application of biometric facial recognition technology. AI & Society, 37: 167–175.

Tan J., Niu L., Adams J.K., Boominathan V., Robinson J.T., Beraniuk R.G., Veeraraghavan A. (2019): Face detection and verification using lensless cameras. IEEE Transactions on Computational Imaging, 5: 180–194.

Vojkovic G., Milenkovic M. (2018): GDPR in access control and time and attendance systems using biometric data. In: Proc. 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), May 21–25, 2018: 1138–1142.

Vošahlík J., Hart J. (2020): Reliability of camera systems to recognize facial features for access to specialized production areas. Agronomy Research, 18: 1082–1089.

Wang H., Wang Y., Zhou Z., Ji X., Gong D., Zhou J., Liu W. (2018): CosFace: Large margin cosine loss for deep face recognition. In: Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), 2018: 5265–5274.

Yang Y., Yang Q., Su Z., Wu W. (2024): Employee fingerprint identification management system based on bidirectional ResNext network with triplet loss. In: Proc. 8th Int. Conf. on Management Engineering, Software Engineering and Service Sciences (ICMSS), Wuhan, 2024: 48–52.

Received: March 27, 2025
Accepted: May 5, 2025
Published online: June 6, 2025