Actual Problems of Mathematical Modeling and Information Technologies (APMMIT-2025)

# A Comprehensive Review of Face Anti-Spoofing Methods with Emphasis on Image Distortion Analysis

AIPCP25-CF-APMMIT2025-00110 | Article

PDF auto-generated using **ReView** from

RIVER VALLEY TECHNOLOGIES

# A Comprehensive Review of Face Anti-Spoofing Methods with Emphasis on Image Distortion Analysis

Shukrullo Kakharov[1, 2, a)], Abdugofur Rakhimov[2, b)], Dilnoza Bekmurotova[2, c)]

[1]*Oriental University, Tashkent, Uzbekistan,*
[2]*Digital technologies and artificial intelligence development research institute, Tashkent, Uzbekistan*

[a)] *Corresponding author: sh.kaxarov93@gmail.com*
[b)] *abdugofurrakhimov6@gmail.com*
[c)] *dilnozabekmurotova@gmail.com*

**Abstract.** In order to circumvent biometric identification systems, the attack is often using images printed on paper, replay able video recordings, specially made three-dimensional masks, as well as artificial data created using deep fake technology, which has been increasingly developed in recent times. To address such risks, various approaches to the detection of falsified biometric data or Presentation Attack Detection (PAD) are proposed in the scientific literature published by various industry experts. In this article modern research on falsification of biometric data (on the example of facial images) is considered on the basis of a deep critical analysis of the types of various attacks, hand-crafted and deep learning-based methods of feature extraction and recognition, classification approaches, benchmark datasets for effectiveness evaluation and systematic analysis of evaluation criteria was implemented. Previous similar research studies has been largely focused on deep learning-based architectures, and the feasibility of developing image quality-based approaches from classical textural analysis and motion-based methods which is discussed in detail in the example of the Image Distortion Analysis (IDA) method. Each category of methods has been deeply analyzed in detail with the latest highly cited major papers on the field, the results of the experimental studies also carried out, with their limitations and implementation complexities. In addition, this study also provides a description of problems that are currently not sufficiently studied by researchers, including factors such as difficulties in increasing the ability to generalize across different data sets, the variability of the environment, bias, and the rapid emergence of deepfake attacks. In this study has been identified a number of promising areas for future research development, including generalization-oriented training, the development of lightweight and strong models, and the use or improvement of standardized assessment criteria. This work is intended to serve as a detailed resource for researchers and practitioners in creating and constructing secure and reliable systems against future biometric data falsification.

## INTRODUCTION

To this day, no unified solution has been proposed, face recognition systems are one of the most common biometric authentication technologies. They are also used in mobile devices, access control systems, border control, surveillance systems, as well as in online financial services. Compared to other biometric modalities such as fingerprint or iris recognition, face recognition offers several advantages, including user convenience, contactless acquisition, and the ability to operate using low-cost, consumer-grade RGB cameras.

Despite these advantages, face recognition systems suffer from a fundamental security weakness: their susceptibility to presentation attacks. A presentation attack occurs when an adversary presents an artificial facial artifact, such as a printed photograph, a digital display showing a video, or a three-dimensional mask to the sensor in order to impersonate a legitimate user. Because early face recognition systems were designed primarily for identity matching rather than liveness verification, they often fail to distinguish between genuine (bona fide) facial presentations and spoofed ones.

Several studies have demonstrated the severity of this problem. Galbally et al. reported that commercial off-the-shelf face recognition systems can incorrectly accept a substantial portion of spoofed samples under uncontrolled

conditions, particularly when high-quality print or replay media are used [1, 2]. This system is considered directly vulnerable in applications that are important for security and pose a risk, the reason being that in the case of unauthorized access it can lead to financial losses, a violation of privacy or damage from other circumstances. In an effort to reduce these risks, researchers have proposed various methods for detecting Face spoofing or presentation attacks (PAD – Presentation Attack Detection). Early approaches had relied more on hand-made text descriptors, such as Local Binary Patterns (LBP), to identify micro-text differences between real skin and artificial media [3-5]. Although these research methods have shown good results in controlled datasets, they are often considered weak in terms of generalization in other datasets and devices. Subsequent research has led to the introduction of motion-based methods, such as blinking and head movements, as well as internal system disorders caused by falsified media retrieval, which include image quality-based approaches that analyze in depth [6,7].

In recent years, however, in-depth learning methods, namely Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Generative Adversarial Networks (GAN), have taken over the field, enabling automatic study of spatial and temporal expressions [8-11]. While these models have achieved high accuracy in the dataset, their unseen environments, various devices, and attack types are still an open problem. Several articles on face forgery have been published in recent years. At the same time, many existing works often focus on in-depth learning architectures and less on critical analysis of traditional methods as well as image quality-based techniques. In a similar way, the limitations of generalization, evaluation on different databases, and practical implementation have not yet been sufficiently studied.

Our article aims to complement the following ventricles:

Classification of types of attacks and their features in face falsification.

Analysis of key categories of face falsification methods, such as motion-based, Surface Pattern, Image Quality-based, and multi-source (multi-cue) approaches.

A thorough discussion of the Image Distortion Analysis (IDA) method as an image quality-based approach, looking at the possibility of generalization in its various datasets.

Analysis of open datasets and evaluation protocols used in the literature.

Identifying key problems and setting future research directions, specifically in the context of deep fake attacks and real-world deployment.

## FACE SPOOFING ATTACK TAXONOMY

Face spoofing attacks are broadly classified according to the physical or digital medium used. This process is very important, the reason is that the effectiveness of anti-face falsification methods is considered inextricably linked with the state of attack. In the literature, face-fake attacks are mainly divided into three types: these, attacks through published photos (print attacks), attacks through re-played videos (replay attacks), and attacks through masks (mask attacks).

*A. Print Attacks*

Through published photos, the attack is considered one of the oldest and simplest forms of face falsification. In this case, the attacker provides the system with a high-quality printed photo of the real user. The photo can be printed on a variety of materials, including plain paper, colored photo paper, or surface patterned surfaces. Early studies using NUAA photography Imposter Dataset have shown that published photographs do not contain certain features of live human skin, namely a thin surface pattern, diffusing light from the lower layers, and natural reflection patterns [3,4]. To find these differences, researchers have proposed surface pattern-based descriptors such as LBP, WLD, and HOG. But further research has found some limitations. High-resolution printers and surface patterned paper can partially recreate their skin-like patterns, a condition that only reduces the separation power of surface pattern-based features. In addition, lighting changes and differences in camera quality significantly affect surface pattern descriptors, a situation that leads to poor generalization in different data sets. In addition, detecting attacks with published photos will not be enough for real-world systems with only a surface pattern, even if the ratio to others is easy.

*B. Replay Attacks*

Attacks with repeated videos are considered complex and dangerous compared to published photos. In these attacks, attackers present previously recorded video or digital images to a face recognition system via smartphone, tablet, or laptop screens. The main advantage of Replay attacks is that they can partially mimic facial movements, expressions and some physiological signals, unlike simple images. Research work by Zhang et al has shown that facial movement in replay attacks is partially consistent with actual face-image, with ephemeral and photometric artifacts resulting from the screen and rewriting process. Optical flow - based approach systems were developed primarily to

detect these artifacts [6,7]. Researchers has achieved a 1.25% HTER result in the Idiap REPLAY-ATTACK dataset, indicating that action-based methods are highly effective against replay attacks. Besides, subsequent studies have also identified the limitations of these approaches. High-quality OLED or AMOLED screens, high refresh frequency and high resolution significantly reduce movement inconsistencies in replay attacks. Also, background motion or lighting changes in the environment can cause false positives or false negatives by creating noise during the optical flow calculation process. These cases pose serious problems in the stable operation of action-based methods in real-world settings. The main important aspect is that replay attacks are often seen as an "intermediate stage" between Published photo attacks and deep fake-based attacks. Therefore, effective defense mechanisms against this type of attack are considered important in the design of more complex attack-resistant systems in the future.

*C. Mask Attacks*

Attacks with mask is considered one of the complex and dangerous types of face faking. These attacks use three-dimensional (3D) face masks made of special elastic materials. Such masks can study not only the structure of the face, but also the geometric structure such as the nose, cheeks, chin and eyelids. Research by Kim et al shows that mask attacks are very difficult to detect with facial patterns and motion-based methods, the reason being that 3D masks maintain depth and spatial contours. Effective detection therefore often relies on specialized sensor devices, including Depth camera, structured light sensors, or infrared (IR) imaging technologies [12,13].

Proposed approaches to mask-based attacks rely on three types of signals:

1. Discontinuities in depth.
2. Differences in material reflection.
3. Thermal or infrared response properties.

These methods can provide high accuracy against mask attacks, but significantly increase the cost of the system and limit their use in consumer devices. As a result, in real world conditions, mask attacks remain one of the most important problems in the field of face forgery [14].

## FACE ANTI-SPOOFING METHODS: DETAILED REVIEW

### Motion-Based Methods

Action-based face falsification techniques are based on natural facial movement analysis. These visual movements mainly include eyes blinking, dizziness, and facial muscle movements. The basis of this approaches is that it is almost impossible to reproduce such actions artificially perfectly. Traditional action-based methods rely on rule-based strategies. However, such approaches are vulnerable to replay attacks, with the possibility that natural wink patterns of pre-recorded videos are also present. In-depth learning-based action approaches, hybrid models, CNN-RNN and 3D CNN architectures demonstrate significant advances in the study of temporal consistency patterns [7,10,15]. The main limitations of these models are considered to be due to the high computational cost and the lack of sufficient optimization for real-time operation.

### Texture-Based Methods

Texture-based methods are among the earliest and most widely studied approaches in face anti-spoofing. They aim to detect micro-texture differences between genuine and spoofed facial surfaces using handcrafted features extracted from facial images.

Wen et al. proposed LBP-based approaches, which achieved effective results in detecting print attacks. Subsequent studies enhanced discriminative power by incorporating descriptors such as WLD, HOG, and DoG, often combined with classifiers like SVM or Ada Boost [3,4,16]. However, experiments have shown that texture-based methods are highly sensitive to illumination variations, camera quality, and resolution differences, with performance dropping significantly on cross-device datasets such as CASIA-FASD and MSU-MFSD.

Texture-based method offers speed and simplicity, making them attractive for low-cost or real-time applications, but their limited generalization, weakness to complicated attacks, and inability to detect deep fake or mask attacks restrict their use as offline solutions. To improve robustness, modern systems often combine texture features with motion-based cues, image quality metrics, or deep learning architectures, resulting in hybrid approaches that balance efficiency and accuracy [5].

## Image Quality-Based Methods

Thus far, research has shown that, image quality-based approaches have been developing as an important focus in anti-face falsification research. Other methods that directly analyze biometric facial features, these techniques focus on internal distortions that occur in the process of falsification, i.e., image acquisition and retrieval. The type and extent of these breakdowns will depend on the forgery tool (printers, screens, or camera sensors) and the information retrieval process. These artifacts are not usually present in real facial images, so they are a reliable indicator in detecting falsification.

Galbally et al. [1] with image Quality assessment (Image Quality Assessment, IQA), it has been proven that real and falsified images can be effectively distinguished. They showed this by analyzing characteristics such as dullness (blurriness), noise level, color accuracy and bright reflections. The main advantage of image quality-based methods is that they function independently of identification, that is, they can detect falsification artifacts that do not depend on the personality of the subject. Subsequent research has further developed these approaches, introducing feature analysis using different color spaces (HSV, YCbCr), spectral domains, and statistical descriptors. These improvements generally lead to higher efficiency in different datasets compared to traditional methods.

## Image Distortion Analysis (IDA): A Representative Approach

Image distortion analysis (Image Distortion Analysis, IDA) Wen et al. [17] the Image Distortion Analysis (IDA) proposed by is one of the most cited approaches to face falsification based on image quality. The main idea of the IDA is that distortions that occur during falsification attacks are considered difficult to reproduce in real facial images.

*IDA distinguishes the following main groups:*

1. *Specular Reflection Features.* Published photos and screens reflect a different light from human skin. IDA calculates the proportion of bright pixels, their intensity distribution, and statistical measurements to identify artificial surfaces.
2. *Blurriness Features.* Dullness caused by camera focus shift and movement is common in replay attacks. These properties analyze the reduction of high-frequency components in the image.
3. *Chromatic Moment Features.* HSV is the mean, dispersion values for each channel in color space, helping to determine color inconsistencies. Screen and printer devices cannot fully reproduce the skin-specific reflection effects.
4. *Color Diversity Features.* Spatial and statistically high color diversity can be observed on real faces. The IDA quantifies this variability.

These properties are combined into a 121-dimensional feature vector and classified using an SVM-based classifier. For video data, however, a multi-frame merge is used.

## Multi-Cue Methods

Multi-cue methods offer a comprehensive approach to the face anti-spoofing problem by integrating multiple sources of information, such as RGB images, depth data, infrared signals, or audio cues. The basic assumption is that if one cue is compromised, the remaining cues can still contribute to reliable spoofing detection.

Multi-cue methods provide exhaustive approach to face anti-spoofing by integrating multiple information sources, such as RGB images, depth data, infrared signals, or audio cues [12,13,18-23]. The underlying idea is that if one cue is compromised, other cues can still detect spoofing attempts.

## Deep Learning Approaches

In recent years, in-depth study has developed as key approaches in research against face falsification. Because they allow you to automatically study distinguishing features from raw facial data. Researchers have researched a wide range of architectures, ranging from traditional CNN (Convolutional Neural Networks) models to 3D CNN and Gans, each focused on solving key problems in falsification detection.

CNNs (Convolutional Neural Networks) are very effective in detecting spatial surface patterns and color artifacts in facial images. Such as, LBP-CNN hybrid models show improved detection of published photo attacks by combining micro-texture features with deep spatial representation. Standard 2D CNNs, such as Res Net or VGG variants, have been successfully applied in RGB color frames derived from datasets such as CASIA-FASD, providing high intra-dataset accuracy [19].

3D CNNs, on the other hand, allow the capabilities of CNNs to model temporal continuity across sequential video frames. Architectures such as, C3D or i3d are effective in distinguishing real facial movements from replay attacks by studying spatiotemporal features. For example, optical flow sequences combined with 3D CNNs have demonstrated superior performance on the Idiap REPLAY-ATTACK dataset, capturing subtle temporal inconsistencies that traditional 2D CNNs fail to detect [9,20].

GANs (Generative Adversarial Networks) have been leveraged for two main purposes. Data augmentation, where synthetic variations of facial images help to mitigate limited dataset sizes, and simulating deep fake or high-quality spoofing attacks [20,21]. Works such as Face Bag Net and Deep Fake Detection Challenge submissions use GAN-generated videos to improve model robustness against adversarial spoofing scenarios.

Deep networks may learn dataset-specific artefacts rather than generalizable spoofing cues. For instance, models trained on intra-database protocols often exhibit dramatic performance drops in cross-database evaluation, highlighting poor generalization [7,16].

Overall, deep learning approaches offer unmatched discriminative power and flexibility for detecting sophisticated spoofing attacks. However, their practical deployment requires careful design choices to balance accuracy, generalization, and computational efficiency, making hybrid and lightweight architectures increasingly popular in contemporary research.

The following table presents the advantages, disadvantages, and general critical discussions of each of the current modern methods.

**TABLE 1.** Summary of Advantages and Disadvantages of the Compared Methods

| Method Type | Typical Advantages | Typical Disadvantages | Overall Critical Discussion |
|---|---|---|---|
| **Motion-Based** | Effective against replay attacks; Physiologically interpretable. | Sensitive to illumination and background motion; high computational cost | Effective for repeated attacks, but sensitive to environmental conditions and expensive to calculate. |
| **Texture-Based** | Fast; Low computational cost; Real-time capable. | Poor cross-database generalization; vulnerable to high-quality print/replay/mask attacks | Fast and simple, but ineffective against limited generalization and complex attacks. |
| **Image Quality-Based** | Identity-independent; Robust cross-database. | Sensitive to high-quality spoofing media; single-cue limitations | Improve the consistency of the transverse base using independent distortion tips; However, high quality spoofing media can reduce efficiency. |
| **Image Distortion Analysis (IDA)** | Strong cross-database generalization; Identity-independent cues. | Sensitive to high-quality displays/printers; may require DL integration | Improve the consistency of the transverse base using independent distortion tips; However, high quality spoofing media can reduce efficiency. |
| **Multi-Cue** | High robustness; Mask high-quality replay detection; Mitigates single-cue failure | Requires extra hardware; higher computational cost; less practical for consumer/mobile devices | Offer the most comprehensive protection by combining several methods and achieving high strength against masks and high-quality repeated attacks, but requires additional hardware and computing resources. |
| **Deep Learning** | High accuracy; automatic feature learning; robust to complex attacks. | Requires large annotated datasets; risk of overfitting; high computational cost; latency issues. | It is considered unparalleled for detecting complex fraud attacks, including spatio -temporal and generative properties. Lightweight and hybrid architectures increase real-world capabilities in addressing datasets and computational constraints. |

## Face Anti-Spoofing Methods and Benchmark Dataset Performance

Face anti-spoofing researches use a benchmark dataset to evaluate and compare algorithms. The most commonly used public data sets include NUAA, Idiap REPLAY-attack, CASIA-FASD, and MSU-MFSD. Evaluation protocols have a significant impact on the reported performance. Evaluation within a database usually shows high accuracy, but does not reflect actual generalization. Only, cross-database evaluation often reveals a significant decrease in performance and highlights the problems of positioning these methods in an unrestricted environment.

The following table summarizes major face anti-spoofing approaches and their performance across benchmark datasets:

**TABLE 2.** Comparative Performance of Face Anti-Spoofing Methods Across Benchmark Datasets

| Method Type | Key Features / Architecture | Dataset(s) | Attack Types | Performance / Accuracy | Notes |
|---|---|---|---|---|---|
| Motion-Based [5,8] | Eye blinking, micro-expressions, subtle head/face motions; optical flow; CNN-RNN / 3D CNN | Idiap REPLAY-ATTACK | Replay videos | HTER = 1.25% (Optical flow), TPR ~92% (multi-frame) | Performance decreases in cross-database tests; challenging for real-time mobile deployment |
| Texture-Based [2,3,7,12] | Handcrafted features: LBP, WLD, HOG, DoG; SVM / AdaBoost | CASIA-FASD | Printed photo, Replay | 80–90% (intra-database) | Performance drops in cross-database evaluation |
| Image Quality-Based [1] | Blurriness, noise, color consistency, specular reflection | MSU- MFSD | Printed photo, Replay | TPR = 75.5% (IDA) | Works better when combined with multiple cues |
| Image Distortion Analysis (IDA) [13] | Specular reflection, blurriness, chromatic moments, color diversity; 121-dimensional SVM classifier | Idiap REPLAY-ATTACK, MSU- MFSD | Replay, Printed photo | TPR = 92.2% (Idiap), 75.5% (MSU) | Multi-frame fusion for videos; robust to dataset-specific artifacts |
| Multi-Cue [5,9,10] | Fusion of RGB, depth, infrared, audio cues | CASIA-FASD | Replay, Mask | Depth/RGB / IR+RGB: TPR ~95% (intra-database) | Most effective for real-world deployment; resource-intensive |
| Deep Learning [7,8,15,16] | CNN, 3D CNN, LBP-CNN, GAN, CNN-RNN hybrids; Space-time modeling | CASIA-FASD, NUAA, MSU- MFSD, Idiap REPLAY-ATTACK | Replay, Mask, Deepfake | Intra-database: 90–98%; Cross-database may drop | Lightweight and hybrid architectures improve deployment feasibility |

## Challenges and Future Research Directions

*Face anti-spoofing research continues to face several critical problems:*

– *Attack variability.* Spoofing attacks are very diverse in type and quality, they include published photos, replayed videos, 3D masks, and content created through deep fake. This variety of attack tools makes it difficult to effectively generalize methods based on a single character (single-cue) or tailored to a particular dataset.

- *Environmental sensitivity*. Many of the available approaches are considered highly sensitive to changes in lighting conditions, background motion, camera quality, and device-specific features. Such environmental factors can significantly reduce detection accuracy under real conditions.
- *Demographic bias*. Current datasets often lack sufficient diversity in terms of age, gender, and ethnicity, which can lead to models showing inaccurate or uneven results across different demographics [21].
- *Data scarcity*. In particular, deep learning models require large amounts of annotated datasets for the training process. The limited size and diversity of publicly available datasets, however, limits the generalization capacity of the models and increases the risk of overfitting (over-matching).
- *Deep fake-based attacks*. The emergence is difficulty deep fake videos and artificial facial manipulations are bringing to the surface high level of realistic falsification scenarios where traditional structure-based, action-based, or image quality-based methods are difficult to detect.
- *Future research directions should focus on:*
- *Domain generalization.* Development of models with stable performance in unseen datasets and different attack types
- *Physiological signal analysis.* Applying subtle physiological signs such as pulses or micro-expressions to increase resistance to complex attacks.
- *Fairness-aware learning.* Eliminate demographic bias to ensure fair identification results across diverse population groups.
- *Standardized evaluation protocols.* To facilitate fair comparison of algorithms, the creation of constant criteria on different databases and devices.

By solving these problems, future anti-face falsification studies can develop towards more generalized, durable and practical life-appropriate systems that can detect both conventional and emerging attacks.

## CONCLUSION

This article provides a complete and in-depth analysis of the technologies used against falsification of facial data, which has an important importance among biometric data. Studies have shown that texture-based and action-based methods may show effective results under controllable conditions, but they have been shown to show limited generalization capability across unexplored environments and types of attack. The opposite direction to this has been shown to be those approaches based on image quality analysis, particularly in the case of IDA, can significantly increase cross-database durability by using non-personality distortion markers. It has also demonstrated that multi-cue-based and deep learning-based approaches can deliver good results with their ability to provide high resilience to attacks with a high level of sophistication, including high-quality replay and masked attacks, as well as emerging deep fake threats. Unfortunately, such methods often have a number of limitations in terms of high computational complexities, strong reliance on large data sets, and the fact that additional sensors or expensive hardware require modules. Future research on the field is intended to focus on the development of hybrid solutions that combine classical signal and light deep learning architectures. These approaches offer the ability to increase cross-domain model generalization, enable real-time implementation, and provide high resiliency across a variety of environments and demographics. By addressing these challenges, next-generation anti-facial identity anti-spoofing systems can deliver reliable results in real-world approbation conditions and serve to effectively mitigate the emerging counterfeiting threats to traditional and biometric systems.

## REFERENCES

1. J. Galbally, S. Marcel, and J. Fierrez, “Image quality assessment for fake biometric detection: Application to face recognition,” IEEE Transactions on Image Processing, vol. 23, no. 2, pp. 710–724, 2014. doi: 10.1109/TIP.2013.2292332
2. Fazilov, S. K., & Yusupov, O. R. (2021, September). Improvement of the daugman method for nonreference assessment of image quality in iris biometric technology. In 2021 IEEE East-West Design & Test Symposium (EWDTS) (pp. 1-4). IEEE.
3. T. de Freitas Pereira, “LBP-based face anti-spoofing for countermeasure against photo attacks,” in Proc. ICB, 2013. doi: 10.1109/ICB.2013.6613002
4. I. Chingovska, “On the effectiveness of LBP in face anti-spoofing,” in Proc. BIOSIG, 2012. doi: 10.1109/BIOSIG.2012.6312726

5. Fazilov, S. K., & Yusupov, O. R. (2019, September). Algorithm for Extraction of the Iris Region in an Eye Image. In 2019 IEEE East-West Design & Test Symposium (EWDTS) (pp. 1-5). IEEE.
6. Z. Zhang, “A face anti-spoofing database with diverse attacks,” in Proc. Int. Conf. Biometrics (ICB), 2012, pp. 26–31. doi: 10.1109/ICB.2012.6199849
7. T. de Freitas Pereira, “Can face anti-spoofing countermeasures work in a real-world scenario?” in Proc. ICB, 2014. doi: 10.1109/ICB.2014.6996241
8. Narzillo, M., Bakhtiyor, A., Shukrullo, K., Bakhodirjon, O., Gulbahor, A., “Peculiarities of face detection and recognition”, In International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities, ICISCT 2021.
9. D. Menotti, “Deep representations for spoofing detection,” IEEE TIFS, vol. 10, no. 4, pp. 864–879, 2015. doi: 10.1109/TIFS.2015.2398817
10. A. George and S. Marcel, “Deep pixel-wise supervision for PAD,” in CVPRW, 2019. doi: 10.1109/CVPRW.2019.00036
11. Fazilov, S. K., & Yusupov, O. R. (2019, September). Algorithm for Extraction of the Iris Region in an Eye Image. In 2019 IEEE East-West Design & Test Symposium (EWDTS) (pp. 1-5). IEEE.
12. Y. Kim, J. Na, and S. Yoon, “Face anti-spoofing based on depth and infrared information,” Sensors, vol. 17, no. 5, 2017. doi: 10.3390/s17051015
13. Y. Atoum, “Face anti-spoofing using patch and depth-based CNNs,” in IJCB, 2017. doi: 10.1109/IJCB.2017.8272676
14. Yusupov, R., Eshonqulov, E., Qodirov, A., Shukurov, E., & Malikov, Z. (2025, October). Remote sensing image segmentation: Methods and evaluation metrics. In AIP Conference Proceedings (Vol. 3377, No. 1, p. 060020). AIP Publishing LLC.
15. Fazilov, S.K., Kakharov, S. S., Rashidov, K. S., Khandamov, Y., “Formation of an integrated system of descriptors of recognized objects in images”, *AIP Conf. Proc.* 3244, 030072 (2024)https://doi.org/10.1063/5.0241600
16. Z. Boulkenafet, “Face anti-spoofing based on color texture analysis,” IEEE TIFS, vol. 11, no. 8, pp. 1818–1830, 2016. doi: 10.1109/TIFS.2016.2555282
17. Z. Wen, H. Han, and A. K. Jain, “Face spoof detection with image distortion analysis,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 746–761, 2015. doi: 10.1109/TIFS.2015.2398810
18. J. Komulainen, “Context based face anti-spoofing,” in BTAS, 2013. doi: 10.1109/BTAS.2013.6712721.
19. Yusupov, O., Eshonqulov, E., Yusupov, R., & Sattarov, K. (2024, May). Analysis of superpixel segmentation approaches in remote sensing images. In AIP Conference Proceedings (Vol. 3147, No. 1, p. 040026). AIP Publishing LLC.
20. Z. Yu, “Searching central difference CNNs for face anti-spoofing,” in CVPR, 2020. doi: 10.1109/CVPR42600.2020.00533
21. Y. Li, “Face anti-spoofing via adversarial cross-modality adaptation,” IEEE TIFS, vol. 15, pp. 3381–3396, 2020. doi: 10.1109/TIFS.2020.3002689
22. J. Yang, “Face liveness detection with component dependent descriptor,” in Proc. ICB, 2012. doi: 10.1109/ICB.2012.6199846
23. Nuritdinov, J., Kakharov, S., Tashxodjayev, A., “Application of Minkowski operator in artificial intelligence tasks”, In AIP Conference Proceedings (Vol. 3244, No. 1). AIP Publishing, November, 2024. https://doi.org/10.1063/5.0241599