Торайғыров университетінің хабаршысы
ҒЫЛЫМИ ЖУРНАЛЫ

НАУЧНЫЙ ЖУРНАЛ
Вестник Торайгыров университета

Торайғыров университетінің ХАБАРШЫСЫ

Энергетикалық сериясы
1997 жылдан бастап шығады

ВЕСТНИК Торайгыров университета

Энергетическая серия
Издается с 1997 года

ISSN 2710-3420

№ 1 (2025)

ПАВЛОДАР

НАУЧНЫЙ ЖУРНАЛ
Вестник Торайгыров университета

Энергетическая серия
выходит 4 раза в год

СВИДЕТЕЛЬСТВО
о постановке на переучет периодического печатного издания,
информационного агентства и сетевого издания
№ 14310-Ж
выдано
Министерство информации и общественного развития
Республики Казахстан

Тематическая направленность
публикация материалов в области электроэнергетики,
электротехнологии, автоматизации, автоматизированных и
информационных систем, электромеханики и теплоэнергетики

Подписной индекс – 76136

---

https://doi.org/10.48081/PXLE1275

МРНТИ 28.23.37

https://doi.org/10.48081/CBEO3003

***Ж. А. Икрам[1], Б. С. Омаров[2], Н. К. Смайлов[3]**

[1]КазНУ имени Аль-Фараби, Республика Казахстан, г. Алматы

[2]Международный университет информационных технологий, Республика Казахстан, г. Алматы

[3]Казахский национальный исследовательский технический университет имени К. И. Сатпаева, Республика Казахстан, г. Алматы

[1]ORCID: https://orcid.org/0009-0001-8059-6590

[2]ORCID: https://orcid.org/0000-0002-8341-7113

[3]ORCID: https://orcid.org/0000-0002-7264-2390

*e-mail: zhanserikz@gmail.com

ДВУХДОМЕННЫЙ ПОДХОД К ОБНАРУЖЕНИЮ ПОДДЕЛЬНЫХ ЛИЦ

В данной работе рассматривается новый двухдоменный подход к обнаружению поддельных лиц, ориентированный на повышение надежности и точности современных биометрических систем. Предлагаемая методология основана на уникальном сочетании анализа в пространственной области и детальном исследовании частотных характеристик, что достигается благодаря специально разработанной двухветвевой архитектуре. Первая ветвь обрабатывает аугментированные изображения, выявляя ключевые признаки в виде текстурных и цветовых аномалий, которые часто сопровождают попытки спуфинга. Вторая ветвь одновременно анализирует фурье-преобразования тех же изображений, позволяя обнаруживать повторяющиеся паттерны и другие высокочастотные искажения, не всегда заметные при классическом пространственном анализе. Для проверки эффективности модели использовался набор данных OULU-NPU, известный своей сложностью и разнообразием типов атак, включая распечатанные изображения, демонстрацию видео на экранах и использование 3D-масок. Результаты экспериментов подтвердили высокую точность классификации, свидетельствуя о способности модели надежно дифференцировать подлинные лица от сфабрикованных. Кроме того, достигнутые показатели близки к лучшим современным результатам, что указывает на высокую практическую ценность данного решения.

Таким образом, предложенный двухдоменный анализ, совмещающий пространственные и частотные признаки, открывает перспективы дальнейшего совершенствования механизмов защиты, в особенности для систем, критичных к ошибкам аутентификации и уязвимых к все более изощренным методам подделки.

Ключевые слова: биометрия, компьютерное зрение, определение живости, нейронные сети, Фурье преобразование.

Введение

Технологии защиты от подделки лиц имеют критическое значение в современных биометрических системах безопасности. С распространением систем распознавания лиц в повседневной жизни – от разблокировки смартфонов до систем контроля в аэропортах – растет и изощренность атак злоумышленников, что требует создания более совершенных защитных механизмов [1;2;3;4;5].

Исторически сложилось, что методы противодействия спуфингу лиц фокусировались преимущественно на анализе признаков в пространственной области. Исследователи разрабатывали алгоритмы для выявления аномалий в текстурах, цветовых распределениях и движениях, характерных при использовании фотографий, видеозаписей или масок [6;7;8]. Несмотря на определенную эффективность, эти методы значительно уступают перед высококачественными подделками, имитирующими естественные характеристики живого лица.

Развитие исследований в области частотного анализа открыло новые перспективы. Применение преобразований Фурье и вейвлет-анализа позволило выявлять частотные аномалии, незаметные при пространственном анализе [9;10;11;12;13] – отсутствие микротекстуры кожи или наличие характерных муаровых паттернов при атаках с использованием цифровых экранов.

Однако применение только одного из этих подходов имеет принципиальные ограничения. Пространственный анализ может не обнаруживать тонкие аномалии в продвинутых атаках, а частотные методы могут упускать визуальные артефакты, очевидные в пространственном представлении [14].

Материалы и методы

Точное разграничение подлинных изображений лиц и сложных спуфинг-атак представляет значительную проблему в области защиты систем распознавания лиц. Современные методы обмана, использующие высококачественные фотографии, видео воспроизведение, трехмерные маски и другие технологии, обладают уникальными характеристиками,

требующими тонких механизмов обнаружения [15;16;17]. Эффективная система защиты должна умело анализировать и интерпретировать сложные визуальные признаки для разграничения этих атак от законных попыток доступа.

Суть проблемы можно сформулировать следующим образом: при получении видеопотока необходимо точно определить, соответствует ли представленное изображение лица реальному, живому человеку (подлинная попытка), или это попытка обмана с использованием фотографий, видео на экране или высококачественных масок.

Для решения этой задачи наша модель использует стратегию двойной оптимизации, основанную на интеграции функций потерь бинарной кросс-энтропии (1) и среднеквадратической ошибки (2). Этот подход повышает точность обнаружения путем эффективного использования признаков из пространственной и частотной областей при минимизации указанных функций.

Функция потерь бинарной кросс-энтропии играет ключевую роль в ветви модели, отвечающей за анализ пространственной области, и направлена на улучшение способности системы точно классифицировать видеопоследовательности.

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2 \quad (1)$$

N – общее количество пикселей

y*i* – настоящие пиксельные значения

– предсказанные пиксельные значения

Минимизация функции потерь бинарной кросс энтропии позволяет модели оттачивать свои предсказания, становясь более умелой в выявлении несоответствий, сигнализирующих о попытке обмана.

$$BCELoss = -\frac{1}{N}\sum_{i=1}^{N}(y_i * log(\hat{y}_i) + (1 - y_i) * log(1 - \hat{y}_i)) \quad (2)$$

N – общее количество сэмплов

y*i* – разметка

Ŷi – предсказанная вероятность

В ветви анализа частотной области среднеквадратичная ошибка (MSE) измеряет расхождение между фактическими и предсказанными частотными представлениями изображений. Оптимизация по MSE позволяет модели выявлять тонкие нерегулярности в частотных структурах – часто явные признаки спуфинг-атаки.

При оптимизации этих целевых функций мы сталкиваемся с несколькими ключевыми проблемами:

1 Разнообразие и качество данных

Значительную сложность представляет вариативность качества данных и многообразие типов спуфинг-атак. Видеоматериалы могут существенно различаться по разрешению, условиям освещения и фоновым помехам, что влияет на способность модели к обобщению. Более того, сложность современных атак – от простых фотографий до сложных 3D-масок и дипфейков – требует от модели обучения широкому спектру признаков для точной классификации.

2 Переобучение и обобщение

Высокая размерность видеоданных и сложность двухдоменного подхода создают риск переобучения на тренировочном наборе. Критически важно обеспечить хорошее обобщение модели на новые видео, особенно с применением неизвестных ранее техник спуфинга или снятые в нестандартных условиях. Для снижения риска переобучения мы применяем регуляризацию, аугментацию данных и кросс-валидацию.

3 Балансировка функций потерь

Оптимизация комбинированной целевой функции, включающей потери BCE и MSE, требует тщательной балансировки. Относительные веса этих функций могут значительно влиять на производительность модели, определяя соотношение между анализом в пространственной и частотной областях. Поиск оптимального баланса – нетривиальная задача, требующая обширного экспериментирования.

4 Вычислительная сложность

Двухдоменный подход по своей природе увеличивает вычислительную сложность. Обработка видео в обеих областях и оптимизация комбинированной функции требуют существенных вычислительных ресурсов. Для управления этой сложностью необходимы эффективная реализация и использование аппаратных ускорителей, таких как GPU.

Архитектура

Наш подход к обнаружению поддельных лиц базируется на двухветвевой архитектуре (Рисунок 1), использующей признаки как из пространственной, так и из частотной областей. Процесс включает предобработку входных изображений, извлечение признаков и их обработку через две специализированные ветви модели.

Для предварительной обработки мы используем каскадные сверточные сети MTCNN [18], которые изменяют размер, обрезают и выравнивают каждое лицо до единого разрешения 512×512 пикселя. Такая стандартизация создает оптимальные условия для последующего извлечения признаков.

В качестве основы для извлечения признаков мы выбрали архитектуру EfficientNet-V2S [19], предварительно обученную на наборе данных ImageNet. Этот выбор представляет собой оптимальный компромисс между вычислительной эффективностью и точностью извлечения характеристик, что важно для анализа в обеих доменных областях.

Ветвь анализа пространственной области

Для повышения устойчивости к различным типам атак применяется серия аугментаций изображений. После этого изображения обрабатываются сетью EfficientNet-V2S. Полученные логиты, отражающие вероятность подлинности изображений, используются для расчета потерь BCE. Этот механизм фокусируется на пространственных характеристиках, указывающих на возможную подделку.

Ветвь анализа частотной области

Вторая ветвь исследует особенности в частотной области. Карты признаков, полученные после третьего блока сети EfficientNet-V2S, обрабатываются специализированной CNN, разработанной для частотного анализа. Эта CNN включает шесть сверточных слоев с ядрами 3×3 или 1×1, каждый из которых сопровождается пакетной нормализацией и функцией активации ReLU. После третьего сверточного слоя используется механизм отсева с вероятностью 0.3 для предотвращения переобучения. Архитектура завершается пятым сверточным слоем, формирующим одноканальную карту, эффективно сжимающую признаки для точного анализа.

Рисунок 1 – Архитектура разработанной модели

Целевым выходом для этой ветви является FFT-изображение лица, полученное из предобработанного изображения 512×512. Вычисляя среднеквадратичную ошибку между выходом CNN и FFT-изображением, модель оценивает свою способность выявлять аномалии в частотной области.

Набор данных

В исследовании использовался набор данных OULU-NPU [20] как показано на Рисунке 2, содержащий около 5000 видео от более 50 субъектов для оценки возможностей обнаружения «живости» лица. Из каждого видео было выбрано 10 кадров с интервалом от начала до 200-го кадра, что в сумме дало около 50000 изображений. Этот набор включает кадры, снятые на шести различных устройствах в трех различных условиях освещения, что имитирует разнообразие реальных условий.

OULU-NPU оценивает производительность модели по 4 протоколам:

Протокол I проверяет адаптивность к новым условиям освещения и фона

Протокол II оценивает устойчивость к новым типам атак

Протокол III исследует влияние вариативности камер

Протокол IV тестирует генерализацию при комбинации новых условий, типов атак и источников камер

Для оценки эффективности системы используются следующие метрики:

Attack Presentation Classification Error Rate – частота неправильной классификации поддельных изображений как подлинных

Bonafide Presentation Classification Error Rate – частота неправильной классификации подлинных изображений как поддельных

Average Classification Error Rate – среднее значение между APCER и BPCER, представляющее общую производительность системы

Эксперименты проводились на системе с графической картой RTX 4070, Обучение выполнялось с размером батча 16, оптимизатором Adam (вес распада 3e-5), начальной скоростью обучения 0.001 и 20 эпохами. Применялись различные аугментации: горизонтальное отражение, регулировка контраста/гаммы/яркости, эластичные и оптические искажения, сдвиг, масштабирование и вращение для обогащения вариативности данных.

Рисунок 2 – Лицо, атака с распечатанной бумагой и атака с помощью видео

Результаты и обсуждение

Результаты экспериментов в Таблице 1, выполненных по четырем протоколам, демонстрируют различия в значениях APCER, BPCER и ACER в зависимости от условий проверки.

Таблица 1 - Результаты модели

Protocol	APCER (%)	BPCER (%)	ACER (%)
1	1.4	3.2	2.3
2	2	2.8	2.4
3	3.0±3.1	4.4±2.6	3.7±3.5
4	5.3±4.2	4.7±3.6	5.0±4.0

При проведении испытаний в условиях стабильного освещения и фона (Протокол I) достигнуты значения APCER равное 1,4 %, BPCER – 3,2 % и средний показатель ACER – 2,3 %. Испытания на устойчивость к новым типам атак (Протокол II) дали значения APCER 2,0 %, BPCER 2,8 % и ACER 2,4 %. Более сложные сценарии, учитывающие вариативность камер, изменения освещения и комбинированные атаки, характеризуются увеличением ошибок: для Протокола III показатели составляют APCER 3,0 ± 3,1 %, BPCER 4,4 ± 2,6 % и ACER 3,7 ± 3,5 %, а для Протокола IV – APCER 5,3 ± 4,2 %, BPCER 4,7 ± 3,6 % и ACER 5,0 ± 4,0 %. Результаты подтверждает высокую эффективность модели в условиях, характеризующихся относительной однородностью данных, что отражается в минимальных значениях ошибок для Протокола I. Умеренное увеличение APCER и BPCER в Протоколе II свидетельствует о способности системы корректно распознавать новые

типы атак без существенного смещения в сторону ложноположительных или ложноотрицательных срабатываний. Значительный рост показателей ошибок в Протоколах III и IV указывает на сложность задач, возникающих при работе с разнообразными условиями эксплуатации, и подчеркивает актуальность дальнейшей оптимизации модели. Наблюдаемые стандартные отклонения демонстрируют влияние факторов внешней изменчивости, что требует дополнительных исследований, направленных на усиление обобщающих возможностей системы в динамичных и непредсказуемых условиях.

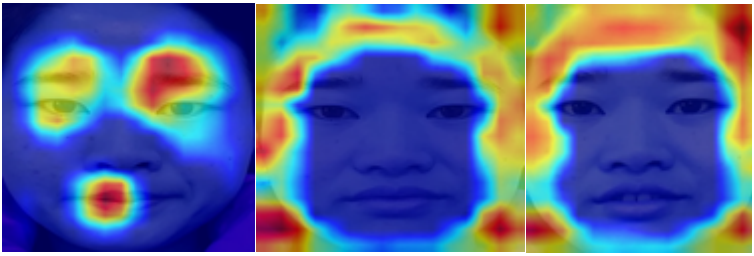

Рисунок 3 – Результаты интерпретации модели с помощью GRAD-Cam. Живое лицо, распечатанное лицо и видео воспроизведение

Визуализация на Рисунке 3, полученная с помощью Grad-CAM, демонстрирует заметное различие в распределении внимания модели для живого лица, распечатанного изображения и видео воспроизведения. Для реального лица наблюдается более равномерная концентрация активаций в областях глаз, носа и рта, что соответствует характерным признакам подлинной живости. При анализе распечатанного лица акцент смещается на текстурные и цветовые несоответствия, возникающие из-за отражений и особенностей бумажной поверхности. В случае видео воспроизведения обнаруживается повышенная реакция на артефакты, вызванные электронным экраном, такими как муаровые узоры и неестественные световые переходы. Разница в тепловых картах подтверждает способность разработанной архитектуры эффективно выявлять уникальные аномалии для каждого типа спуфинга, обеспечивая высокую точность дифференциации подлинных и поддельных изображений.

Выводы

Результаты проведенного исследования демонстрируют высокий потенциал предлагаемого двухдоменного подхода к обнаружению поддельных лиц. Предложенная методология, основанная на интеграции анализа в пространственной и частотной областях, обеспечивает надежное различие между реальными и фальсифицированными изображениями.

Экспериментальные данные подтверждают, что объединение глубоких признаков из аугментированных изображений с детализированным анализом их фурье-преобразований приводит к значительному снижению ошибок классификации. Полученные показатели свидетельствуют о практической применимости разработанной модели для защиты биометрических систем в условиях сложных и динамичных атак. Перспективы дальнейших исследований включают оптимизацию вычислительной эффективности, расширение обучающих выборок и адаптацию архитектуры для выявления новых типов спуфинг-атак, что позволит повысить общую устойчивость систем распознавания лиц в реальных сценариях эксплуатации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 **Li, H., Li W., Cao, H., Wang, S., Huang, F., Kot, A. C.** Unsupervised Domain Adaptation for Face Anti-Spoofing // IEEE Transactions on Information Forensics and Security. – 2018. – Vol. 13, No. 7, P. 1794–1809. – DOI: 10.1109/TIFS.2018.2801312.

2 **Kollreider, K., Fronthaler, H., Bigun, J.** Non-intrusive liveness detection by face images // Image and Vision Computing. – 2009. – Vol. 27, Issue 3, pp. 233–244. – DOI: 10.1016/j.imavis.2007.05.004.

3 **Zhang, S., Liu, A., Wan, J., Liang, Y., Guo, G., Escalera, S.,** Escalante, H. J., Li, S. Z. CASIA-SURF: A Large-Scale Multi-Modal Benchmark for Face Anti-Spoofing // IEEE Transactions on Biometrics, Behavior, and Identity Science. – 2020. – Vol. 2, No. 2, pp. 182–193. – DOI: 10.1109/TBIOM.2020.2973001.

4 **Lei, Li,** Zhaoqiang, Xia, Xiaoyue, Jiang, Fabio, Roli, Xiaoyi, Feng. CompactNet: learning a compact space for face presentation attack detection // Neurocomputing. – 2020. – Vol. 409, P. 191–207. – DOI: 10.1016/j.neucom.2020.05.017.

5 **Wang, Z., Yu, Z., Wang, X., Qin, Y., Li, J., Zhao, C., Liu, X., Lei, Z.** Consistency Regularization for Deep Face Anti-Spoofing // IEEE Transactions on Information Forensics and Security. – 2023. – Vol. 18, P. 1127–1140. – DOI: 10.1109/TIFS.2023.3235581.

6 **Feng, L., Po, L.-M., Li, Y., Xu, X., Yuan, F., Cheung, T. C.-H., Cheung, K.-W.** Integration of image quality and motion cues for face anti-spoofing: A neural network approach // Journal of Visual Communication and Image Representation. – 2016. – Vol. 38, pp. 451–460. – DOI: 10.1016/j.jvcir.2016.03.019.\

7 **Wang, C., Zhou, J.** An adaptive index smoothing loss for face anti-spoofing // Pattern Recognition Letters. – 2022. – Vol. 153, P. 168–175. – DOI: 10.1016/j.patrec.2021.12.006.

8 **Liu, M., Mu, J., Yu, Z., Ruan, K., Shu, B., Yang, J.** Adversarial learning and decomposition-based domain generalization for face anti-spoofing // Pattern Recognition Letters. – 2022. – Vol. 155, P. 171–177. – DOI: 10.1016/j.patrec.2021.10.014.

9 **Guangcheng, Wang, Zhongyuan, Wang, Kui, Jiang, Baojin, Huang, Zheng, He, Ruimin, Hu.** Silicone mask face anti-spoofing detection based on visual saliency and facial motion // Neurocomputing. – 2021. – Vol. 458, P. 416–427. – DOI: 10.1016/j.neucom.2021.06.033.

10 **Chang, H.-H., Yeh, C.-H.** Face anti-spoofing detection based on multi-scale image quality assessment // Image and Vision Computing. – 2022. – Vol. 121, Article 104428. – DOI: 10.1016/j.imavis.2022.104428.

11 **Jia, S., Hu, C., Li, X., Xu, Z.** Face spoofing detection under super-realistic 3D wax face attacks // Pattern Recognition. – 2021. – DOI: 10.1016/j.patrec.2021.01.021.

11 **Bonomi, M., Pasquini, C., Boato, G.** Dynamic texture analysis for detecting fake faces in video sequences // Journal of Visual Communication and Image Representation. – 2021. – Vol. 79, Article 103239. – DOI: 10.1016/j.jvcir.2021.103239.

12 **Ur Rehman, Y. A., Po, L.-M., Liu, M.** SLNet: Stereo face liveness detection via dynamic disparity-maps and convolutional neural network // Expert Systems with Applications. – 2020. – Vol. 142, Article 113002. – DOI: 10.1016/j.eswa.2019.113002.

13 **Chettri, B., Kinnunen, T., Benetos, E.** Deep generative variational autoencoding for replay spoof detection in automatic speaker verification // Computer Speech & Language. – 2020. – Article 101092. – DOI: 10.1016/j.csl.2020.101092.

14 **Monteiro, J., Alam, J., Falk, T. H.** Generalized end-to-end detection of spoofing attacks to automatic speaker recognizers // Computer Speech & Language. – 2020. – Article 101096. – DOI: 10.1016/j.csl.2020.101096.

15 **Peng, F., Qin, L., Long, M.** Face presentation attack detection based on chromatic co-occurrence of local binary pattern and ensemble learning // Journal of Visual Communication and Image Representation. – 2019. – Article 102746. – DOI: 10.1016/j.jvcir.2019.102746.

16 **Liu, Y., Liu, X.** Spoof Trace Disentanglement for Generic Face Anti-Spoofing // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2023. – Vol. 45, No. 3, pp. 3813–3830. – DOI: 10.1109/TPAMI.2022.3176387.

17 **Zhang, K., Zhang, Z., Li, Z., Qiao, Y.** Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks. – 2016.

18 **Tan, M., Le, Q. V.** EfficientNetV2: Smaller Models and Faster Training // arXiv preprint. – 2021. – arXiv: 2104.00298.

19 **Boulkenafet, Z., Komulainen, J., Li, L., Feng, X., Hadid, A.** OULU-NPU: A Mobile Face Presentation Attack Database with Real-World Variations // 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), Washington, DC, USA. – 2017. – 30 May–03 June. – DOI: 10.1109/FG.2017.77.

Поступило в редакцию 04.03.25
Поступило с исправлениями 04.03.25
Принято в печать 10.03.25

**Ж. А. Икрам[1], Б. С. Омаров[2], Н. К. Смайлов[3]*
[1]Әл-Фараби атындағы ҚазҰУ, Қазақстан Республикасы, Алматы қ.
[2]Халықаралық ақпараттық технологиялар университеті, Қазақстан Республикасы, Алматы қ.
[3]Қ. И. Сатпаев атындағы ҚазҰТЗУ, Қазақстан Республикасы, Алматы қ.
04.03.25 ж. баспаға түсті.
04.03.25 ж. түзетулерімен түсті.
10.03.25 ж. басып шығаруға қабылданды.

ЕКІ ДОМЕНДІ ЖАЛҒАН БЕТТЕРДІ АНЫҚТАУҒА АРНАЛҒАН ТӘСІЛ

Бұл жұмыста заманауи биометриялық жүйелердің сенімділігі мен дәлдігін арттыруға бағытталған жалған бет-бейнелерді анықтаудың жаңа екі домендік тәсілі қарастырылады. Ұсынылып отырған әдістеме кеңістіктік талдау мен жиілік сипаттамаларын терең зерттеуді біріктіретін арнайы әзірленген екі тармақты архитектураға негізделеді. Бірінші тармақ өңделген кескіндерді талдап, спуфинг әрекеттерімен жиі байланысты болатын текстуралық және түстік ауытқулар сияқты негізгі белгілерді айқындайды. Екінші тармақ сол кескіндердің Фурье түрлендірулерін бір мезгілде зерттеп, дәстүрлі кеңістіктік талдауда әрдайым анықталмайтын қайталанатын үлгілер мен басқа да жоғары жиілікті бұрмалануларды анықтауға мүмкіндік береді. Модельдің тиімділігін бағалау үшін түрлі шабуыл түрлерінің күрделілігімен және әртүрлілігімен танымал OULU-NPU деректер жинағы пайдаланылды, онда қағазға басылған кескіндер, экрандарда бейнені көрсету және 3D маскаларды қолдану сияқты алуан түрлі әдістер қамтылған. Эксперименттік нәтижелер модельдің жалған бет-бейнелерді шынайыларынан сенімді ажырата алатындығын

дәлелдеп, жіктеу дәлдігінің жоғары екенін көрсетті. Сонымен қатар, алынған көрсеткіштер ең үздік заманауи нәтижелерге жақын, бұл шешімнің тәжірибелік маңыздылығының жоғары екенін білдіреді. Осылайша, кеңістіктік және жиіліктік белгілерді біріктіретін ұсынылған екідомендік талдау аутентификация қателеріне сезімтал және барған сайын күрделіленіп келе жатқан спуфинг әдістеріне осал жүйелерді қорғау механизмдерін одан әрі жетілдіруге едәуір мүмкіндік береді.

Кілтті сөздер: Биометрия, компьютерлік көру, тіршілік анықтау, нейрондық желілер, Фурье түрлендіру.

**Zh. A. Ikram[1], B. S. Omarov[2], N. K. Smailov[3]*
[1]Al-Farabi Kazakh National University, Republic of Kazakhstan, Almaty
[2]International Information Technology University,
Republic of Kazakhstan, Almaty
[3]Satbayev University, Republic of Kazakhstan, Almaty
Received 04.03.25
Received in revised form 04.03.25
Accepted for publication 10.03.25

TWO-DOMAIN APPROACH TO DETECTING FAKE FACES

In this paper, we present a novel two-domain approach for detecting fake faces aimed at improving the reliability and accuracy of modern biometric systems. Our proposed methodology is based on a unique combination of spatial domain analysis and a detailed investigation of frequency characteristics, achieved through a specially developed two-branch architecture. The first branch processes augmented images, identifying key features such as textural and color anomalies that often accompany spoofing attempts. The second branch simultaneously analyzes the Fourier transforms of these images, enabling the detection of repeating patterns and other high-frequency distortions not always noticeable through traditional spatial analysis. To evaluate the model's effectiveness, we employed the OULU-NPU dataset, recognized for its complexity and variety of attack types, including printed images, on-screen video demonstrations, and the use of 3D masks. The experimental results confirmed high classification accuracy, demonstrating the model's ability to reliably distinguish genuine faces from fabricated ones. Moreover, the achieved metrics are close to state-of-the-art results, indicating the strong

practical value of this solution. Consequently, the proposed two-domain analysis, which combines spatial and frequency features, offers significant prospects for further enhancing protective mechanisms, particularly for systems that are highly sensitive to authentication errors and vulnerable to increasingly sophisticated spoofing methods.

Keywords: Biometrics, computer vision, liveness detection, neural networks, Fourier transform.

Теруге 10.03.2025 ж. жіберілді. Басуға 28.03.2025 ж. қол қойылды.
Электронды баспа
29.9 Mb RAM
Шартты баспа табағы 22,2. Таралымы 300 дана. Бағасы келісім бойынша.
Компьютерде беттеген: А. К. Мыржикова
Корректор: А. Р. Омарова, Д. А.Кожас
Тапсырыс №4358

Сдано в набор 10.03.2025 г. Подписано в печать 28.03.2025 г.
Электронное издание
29.9 Mb RAM
Усл. печ. л. 22,2. Тираж 300 экз. Цена договорная.
Компьютерная верстка: А. К. Мыржикова
Корректор: А. Р. Омарова, Д. А. Кожас
Заказ № 4358

«Toraighyrov University» баспасынан басылып шығарылған
Торайғыров университеті
140008, Павлодар қ., Ломов к., 64, 137 каб.

«Toraighyrov University» баспасы
Торайғыров университеті
140008, Павлодар қ., Ломов к., 64, 137 каб.
67-36-69
E-mail: kereku@tou.edu.kz
www.vestnik-energy.tou.edu.kz