Научная статья/Scientific article
УДК 004.056
https://dx.doi.org/10.26583/bit.2026.1.04
https://elibrary.ru/uiebwz

МЕТОД ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ПАТЧА НА ИЗОБРАЖЕНИИ С ИСПОЛЬЗОВАНИЕМ МАТЕМАТИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

Дмитрий А. Есипов[1]✉, Алёна Д. Клетенкова[2], Илья Ю. Попов[3]
[1,3]Национальный исследовательский университет ИТМО, Кронверкский пр., 49, лит. А, Санкт-Петербург, 197101, Россия
[2]АО «Позитив Текнолоджиз», ул. Итальянская, 17, Санкт-Петербург, 191186, Россия
✉*some1else.d.ma@gmail.com*

Аннотация. Активное внедрение технологий искусственного интеллекта связано с их эффективностью при выполнении прикладных задач, включая обработку изображений. Однако вместе с этим возрастает и количество уязвимостей информационных систем, эксплуатируемых посредством модификации входных изображений, что формирует основные угрозы их безопасности. Разработанные методы защиты нередко привязаны к набору данных или архитектуре модели, а также ориентированы исключительно на обнаружение атаки. Метод устранения искажений, встраиваемых пиксельными атаками, с использованием математических преобразований позволяет реализовывать противодействие атакам искажения входных данных, оптимизированным по L_0, однако уязвим к внесению сосредоточенных искажений (состязательного патча). Целью текущей работы является расширение области применения указанного метода путем уменьшения влияния описанного недостатка. Предложен метод обнаружения вредоносного патча на изображении с использованием математических преобразований, позволяющий классифицировать внесенное искажение как сосредоточенное или распределенное. Классификация, как и дальнейшее восстановление, предполагает предварительное обнаружение внесенного искажения. Вычисляется значение средних координат искаженных пикселей и среднее расстояние от искаженных пикселей до указанных средних координат. Если расстояние превышает некоторый порог отсечения, искажение считается распределенным, иначе – сосредоточенным. Также метод позволяет обнаруживать границы прямоугольного патча для дальнейшего исследования атаки. Апробация метода выполнена на наборе данных CIFAR-10. Метод продемонстрировал высокое качество классификации и обнаружения границ искаженной области. Предложенный метод дополняет разработанный ранее метод устранения искажений, встраиваемых пиксельными атаками, снижая влияние его ограничения на противодействие сосредоточенным искажениям. Метод потенциально независим от набора данных и параметров нейронной сети.

Ключевые слова: *искусственная нейронная сеть, обработка изображений, состязательная атака, вредоносное возмущение, вредоносный патч, атака по карте значимости на основе Якобиана*

Для цитирования: Есипов, Д., Клетенкова, А., Попов, И. (2026). Метод обнаружения вредоносного патча на изображении с использованием математических преобразований. *Безопасность информационных технологий,* 33(1), 40-48. doi: http://dx.doi.org/10.26583/bit.2026.1.04

ADVERSARIAL PATCH DETECTION METHOD VIA MATHEMATICAL TRANSFORMATIONS

Dmitry A. Yesipov[1]✉, Alyona D. Kletenkova[2], Ilya Yu. Popov[3]
[1,3]ITMO University, Kronverkskiy Pr., 49, Unit A, St. Petersburg, 197101, Russia
[2]Positive Technologies, Italyanskaya St., 17, St. Petersburg, 191186, Russia
✉*some1else.d.ma@gmail.com*

Abstract. The widespread deployment of artificial intelligence technologies is motivated by their demonstrated effectiveness in applied domains, notably in image processing. Concurrently, such integration introduces additional vulnerabilities in information systems, with adversarial manipulation of input images representing a primary threat vector. Existing defense mechanisms are frequently constrained by dataset dependency, model-specific assumptions, and a predominant focus on attack detection rather than

counteraction. A method of eliminating malicious perturbations embedded by L_0-optimized attacks via mathematical transformations has proven effective against pixel-level adversarial perturbations, yet exhibits a notable limitation in countering concentrated disturbances, particularly patch attacks. The present study addresses this limitation by extending the scope of the method through a novel adversarial patch detection method via mathematical transformations. The method classifies perturbations into concentrated or distributed categories following preliminary perturbed pixel detection, achieved by computing the centroid of perturbed pixels and the mean distance of perturbation pixels to this centroid. Perturbations exceeding a threshold are identified as distributed; otherwise, they are designated as concentrated. Furthermore, the method provides the ability to delineate rectangular patch boundaries, facilitating subsequent attack analysis. Empirical evaluation on the CIFAR-10 dataset demonstrates high accuracy in both perturbation classification and boundary detection. The proposed method augments a method of eliminating malicious perturbations embedded by L_0-optimized attacks by mitigating their limitation to concentrated adversarial perturbations counteraction. The developed method is potentially independent from both dataset and neural network architecture.

Keywords: *artificial neural network, image processing, adversarial attack, malicious perturbation, Adversarial patch, Jacobian Saliency Map Attack*

For citation: Yesipov, D., Kletenkova, A., Popov, I. (2026). Adversarial patch detection method via mathematical transformations. *IT Security (Russia),* 33(1), 40-48. doi: http://dx.doi.org/10.26583/bit.2026.1.04

Введение

В настоящее время развитие технологий искусственного интеллекта сопровождается их активным внедрением в различные сферы благодаря высокой эффективности, гибкости и способности обрабатывать разнородные данные лучше традиционных алгоритмов [1–4]. Системы искусственного интеллекта находят широкое применение в различных прикладных областях [5–12], в том числе в критической информационной инфраструктуре [5–9].

Однако широкое распространение искусственного интеллекта сопровождается увеличением поверхности атаки систем, использующих указанные технологии[1,2]. Наиболее опасными считаются атаки, направленные на обход или искажение целевой модели. Особенно значительные последствия подобные угрозы имеют в сфере обработки изображений и видео, где подмена данных способна нарушить работу систем безопасности и критически важных объектов инфраструктуры.

Обход и нарушение целостности нейронной сети, например, встраивание бэкдора, могут быть реализованы посредством наложения вредоносного патча на изображение [10–12]. Такой атакой является наложение локализованного и видимого вредоносного шума (Localized and Visible Adversarial Noise, LaVAN) [10]. Указанная атака предполагает искажение области изображения, внутри которой все пиксели модифицированы. В случае рассмотренного алгоритма патч имеет форму прямоугольника, стороны и положение которого задаются при адресации атаки.

Ограничением метода восстановления изображений, предложенного в [4], является противодействие концентрированным искажениям, таким как вредоносный патч. Тогда для эффективного применения разработанного решения необходима классификация искажения как концентрированного или распределенного. В текущей работе предложен метод обнаружения вредоносного патча на изображении с использованием математических преобразований, позволяющий в том числе отличать сгруппированное и распределенное искажения.

[1]ФСТЭК. Банк данных угроз безопасности информации. URL: https://bdu.fstec.ru/threat (дата обращения: 02.10.2025).

[2]MITRE. Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS). URL: https://atlas.mitre.org/ (дата обращения: 02.10.2025).

1. Разработанный метод обнаружения вредоносного патча

Предлагаемый метод предполагает обнаружение атак и искажений, оптимизированных по L_0 [2, 3], и использование алгоритмов определения типа искажения и его границ.

Алгоритм предобработки. Применяемый алгоритм предобработки [2] основан на предположении, что искаженные элементы одновременно выступают как локальные, так и глобальные выбросы. Для идентификации локальных выбросов вычисляется величина локального отклонения n

$$n = \sum_{i=1}^{c} \frac{x_i - \sum_{j=1}^{k} \frac{y_{i,j}}{k}}{255},$$

где n – оценка локального отклонения, i – индекс цветовой компоненты, c – число цветовых компонент, x – оцениваемый пиксель, x_i – значение i-ой цветовой компоненты исследуемого пикселя, k – число соседних пикселей, $y_{i,j}$ – значение i-ой компоненты j-го соседа.

Для определения глобальных выбросов используется расстояние Махаланобиса [13] $m = \sqrt{(\mathbf{x}-\boldsymbol{\mu})^T \mathbf{S}^{-1} (\mathbf{x}-\boldsymbol{\mu})}$, где $\mathbf{x}$ – оцениваемый пиксель, $\boldsymbol{\mu}$ – среднее значение пикселей изображения, $\mathbf{S}$ – ковариационная матрица пикселей изображения.

Итоговая оценка аномальности s определяется как произведение полученных оценок $s = m * n$.

Метод обнаружения атаки. Если оценка аномальности некоторого пикселя превышает заданный порог отсечения, изображение классифицируется как подвергшееся атаке. При этом все пиксели, значения оценок аномальности которых также превышают (возможно, иной) порог, рассматриваются как искаженные.

Кроме того, для обнаружения атаки может быть использован метод, предполагающий использование машинного обучения [3]. Ограничениями указанного метода являются невозможность определения координат искаженных элементов изображения, а также сложность применения к обучающей выборке.

Алгоритм определения патча. В случае патча атакованные пиксели сгруппированы. Иными словами, они отклоняются от координат некоторого центрального пикселя не больше, чем на некоторую величину. В случае атаки по Якобиану пиксели распределены по всему изображению.

Алгоритм обнаружения (различения) вредоносного патча основан на идее поиска среднего показателя координат всех потенциально атакованных пикселей с последующим расчетом расстояний от каждого искаженного пикселя до вычисленных координат. Тогда если среднее расстояние будет меньше некоторого значения, то пиксели сгруппированы и пиксельная атака искажения (модификации) входных данных реализована посредством наложения вредоносного патча. Среди рассмотренных атак [10–12] имеет место искажение прямоугольной [10, 11] и круглой области [12].

Рассмотрим искажение круглой области. Общее число искаженных пикселей примерно равно площади круга $N_p \approx S = \pi R^2$. Пиксели, отклоняющиеся от среднего показателя координат на одинаковые расстояния, лежат в концентрических кольцах на расстоянии $r \in [0, R]$ от центра круга. Площадь кольца между r и dr равна $dS = 2\pi r * dr$. Тогда вклад каждого кольца в среднее распределение равен $r * \frac{dS}{\pi R^2} = \frac{2r^2}{R^2} * dr$. Следовательно, среднее расстояние можно вычислить как интеграл по всем указанным кольцам: $\bar{r} = \int_0^R \frac{2r^2}{R^2} = \frac{2}{R^2} * \int_0^R r^2 dr = \frac{2}{R^2} * \frac{R^3}{3} = \frac{2}{3} R$.

Рассмотрим искажение прямоугольной области $R = \{(x, y): -a \le x \le a, -b \le y \le b\}$, где R – искаженная прямоугольная область. Диагональ указанного прямоугольника $d = \sqrt{(2a)^2 + (2b)^2} = 2\sqrt{a^2 + b^2}$. Центр прямоугольника соответствует точке пересечения его диагоналей. Тогда среднее расстояние от произвольной точки внутри рассматриваемой области до центра прямоугольника $\bar{r} = \frac{1}{4ab}\int_{-a}^{a}\int_{-b}^{b}\sqrt{x^2 + y^2} * dx * dy$. Прямоугольник характеризуется осевой симметрией относительно его центра по обеим осям координат, следовательно, при смещении точки отсчета в центр прямоугольника оси разделят его на 4 равные части. Тогда $\bar{r} = \frac{4}{4ab}\int_{0}^{a}\int_{0}^{b}\sqrt{x^2 + y^2} * dx * dy = \frac{1}{ab}\int_{0}^{a}\int_{0}^{b}\sqrt{x^2 + y^2} * dx * dy$. Пусть прямоугольники увеличиваются пропорционально, диагональ каждого равна $d_k = 2k\sqrt{a_k^2 + b_k^2}$, среднее расстояние $\bar{r_k} = k * C$, где C – некоторая константа (ввиду линейности интеграла при масштабировании). Тогда $\frac{\bar{r_k}}{d_k} = \frac{kC}{2k\sqrt{a_k^2 + b_k^2}} = \frac{C}{2\sqrt{a_k^2 + b_k^2}}$ – то есть среднее расстояние линейно зависит от размеров прямоугольника и линейно масштабируется. Отношение $\frac{\bar{r_k}}{d_k}$ стремится к некоторой константе, зависящей только от размеров и соотношения сторон прямоугольника.

Рассмотрим частный случай прямоугольной области: квадрат со стороной 2, то есть $a = b = 1$. Для этого случая известно, что среднее расстояние $\bar{r} = \frac{4+\sqrt{2}+\ln(1+\sqrt{2})}{6} \approx 0{,}765$, а диагональ $d = 2\sqrt{2} = 2\sqrt{a^2 + b^2} \approx 2{,}828$. Четверть диагонали примерно равна $0{,}707$, то есть $\bar{r} \approx \frac{d}{4} + \varepsilon$. При увеличении соотношения сторон $\bar{r} \to \frac{d}{4}$. Иными словами, $\lim_{k\to\infty}\frac{\bar{r_k}}{d_k} \approx \frac{1}{4}$.

При предобработке изображения и обнаружении искаженных элементов возможно вычислить их количество $N \approx S$. В случае прямоугольной области искажения наибольшее среднее расстояние достигается при минимальном соотношении сторон. Тогда для предполагаемой квадратной области $N = S = a^2$, тогда $a = \sqrt{N}$, $d = a\sqrt{2}$. Максимальное расстояние от точки в искаженной области до ее центра равно половине диагонали, то есть $r_{max} = \sqrt{\frac{N}{2}}$. Среднее расстояние $\bar{r} < \sqrt{\frac{N}{2}}$. Аналогично в случае круглой области $N = S = \pi R^2$, $r_{max} = R = \sqrt{\frac{N}{\pi}}$ и $\bar{r} < \sqrt{\frac{N}{\pi}}$. С учетом погрешности обнаружения искаженных элементов имеет смысл выбрать порог отсечения $\bar{r} < \sqrt{\frac{N}{2}}$. Блок-схема описанного алгоритма классификации искажения представлена на рис. 1.

Алгоритм определения границ искаженной области. Для определения цели атаки необходимо определение не только факта атаки, но и искаженной области изображения. Чаще всего патч имеет прямоугольную форму [10, 11], тогда его границы могут быть обнаружены посредством анализа по строкам и столбцам матрицы показателей аномальности пикселей. Определение искаженной области заключается в последовательном проходе по строкам и столбцам указанной матрицы и рассмотрение суммы значений всех элементов строки или столбца. В случае превышения суммой некоторого значения строка или столбец считается началом искаженной области (рис. 2).

Таким образом, возможно определение координат четырех углов, определяющих атакованную область прямоугольного патча с различными длинами сторон. Для иной формы патча необходима модификация алгоритма.

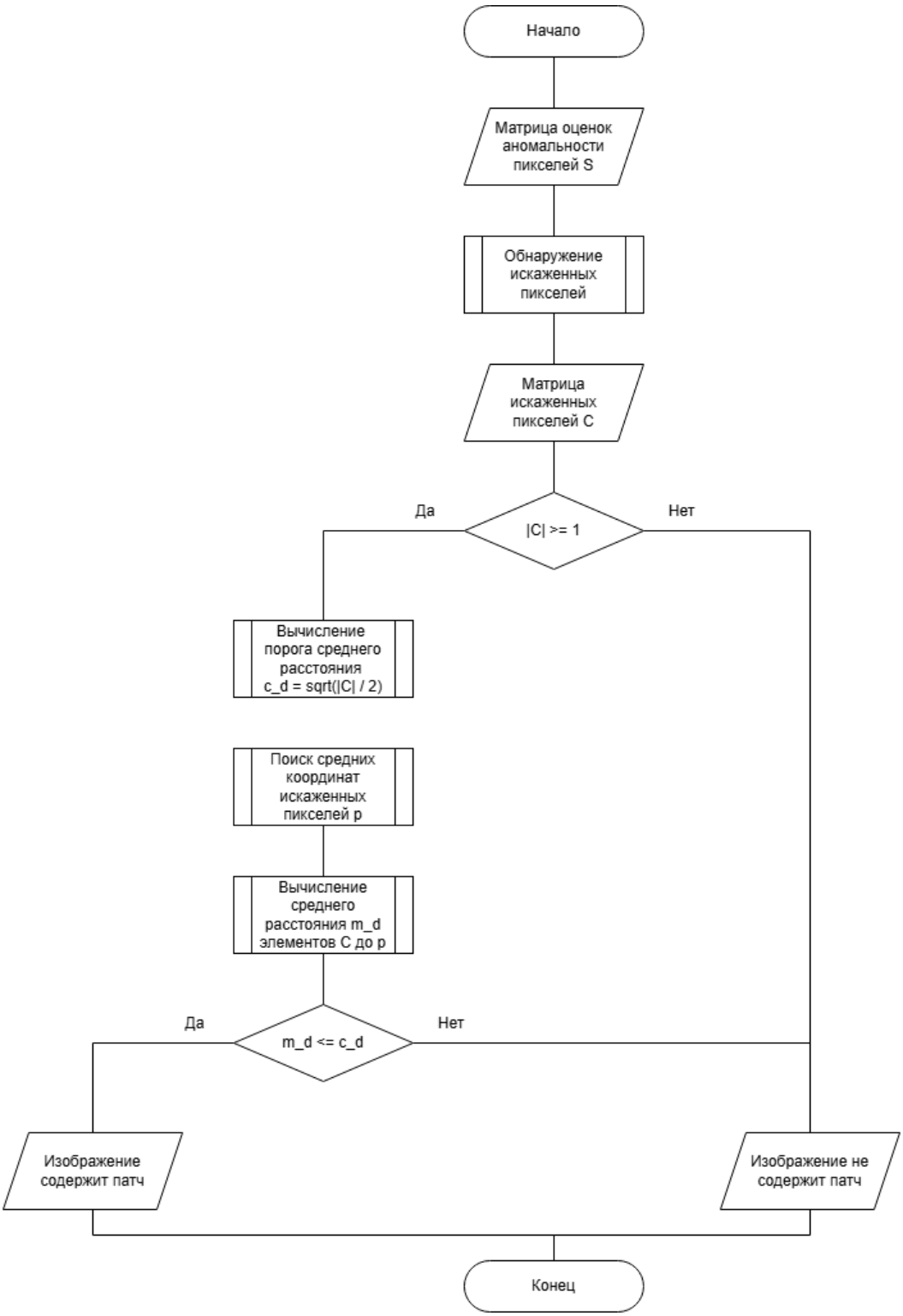

Рис. 1. Блок-схема алгоритма классификации искажения

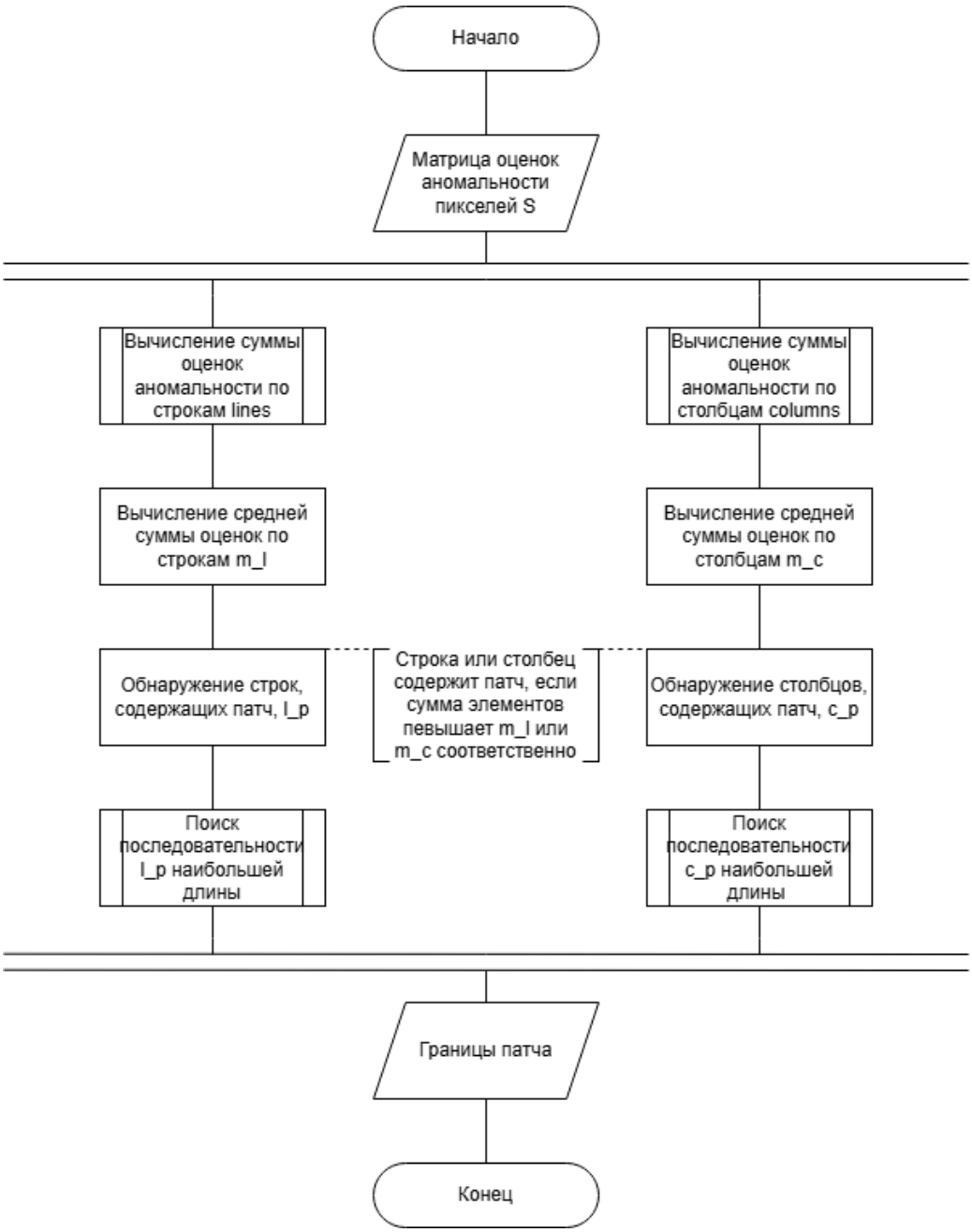

Рис. 2. Блок-схема алгоритма обнаружения границ патча

2. Планирование эксперимента

Алгоритмы атаки. В качестве атак были выбраны два алгоритма: LaVAN [2, 10] и JSMA [2, 14].

Наборы данных. Использованы наборы искаженных данных, полученные в [2][3] (табл. 1).

Таблица 1. Характеристики используемых наборов данных

Набор данных	Алгоритм атаки		Количество элементов
	Название	γ (gamma), %	
CIFAR-10	LaVAN	-	60 000
	JSMA	1	17 098
		3	38 991
		5	48 709

[3]GitHub. iNDm3802. L0-optimized_attack_detection. URL: https://github.com/iNDm3802/L0-optimized_attack_detection (дата обращения: 31.08.2025).

Метрика качества классификации искажения. F_1-мера использована как целевая метрика качества для обнаружения атаки. Также рассчитаны и другие метрики качества: корректность (accuracy), точность (precision) и полнота (recall).

Метрика качества обнаружения границ искаженной области. F_1-мера использована как целевая метрика качества для обнаружения атаки. Также рассчитаны точность (precision) и полнота (recall).

3. Результаты и их анализ

Тестирование алгоритма классификации искажения. Разработанный алгоритм классификации протестирован на искаженном атаками LaVAN [10] (концентрированное искажение) и JSMA [14] (распределенное искажение) наборе данных CIFAR-10. Полученные значения показателей качества приведены в табл. 2.

Таблица 2. Показатели качества классификации искажения

Порог отсечения	Корректность, %	Точность, %	Полнота, %	F_1-мера, %
$\frac{\sqrt{N}}{\sqrt{2}}$	98,70	97,66	98,80	98,23

Согласно табл. 2, разработанный алгоритм достигает корректности классификации в 98,70% и F_1-меры в 98,23%, тем самым демонстрируя высокое качество различения концентрированных и распределенных искажений.

Тестирование алгоритма обнаружения границ искаженной области. Разработанный алгоритм протестирован на искаженном атакой LaVAN [10] наборе данных CIFAR-10. В качестве порога отсечения рассмотрены: абсолютная величина; множитель среднего значения сумм строк и столбцов соответственно; множитель стандартных отклонений от среднего значения сумм строк и столбцов соответственно (рис. 3).

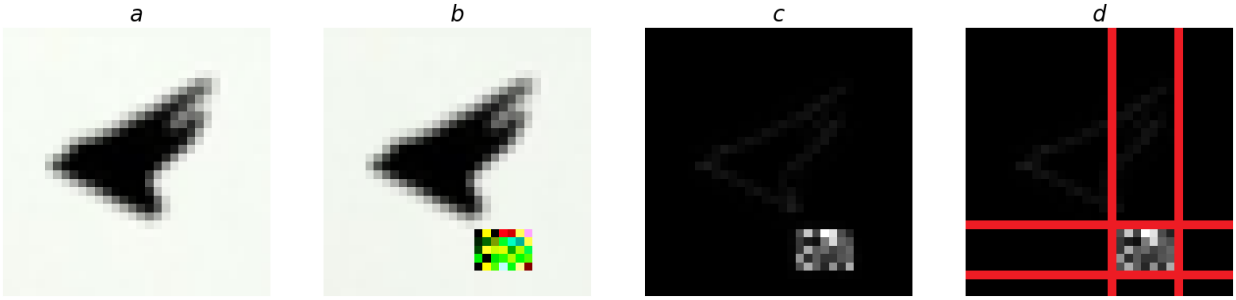

Рис. 3. Пример работы алгоритма: a – оригинальное изображение, b – искаженное изображение, c – матрица оценок аномальности пикселей, d – обнаруженные границы

Показатели качества обнаружения области и границ концентрированного искажения приведены в табл. 3.

Таблица 3. Показатели качества обнаружения области и границ искажения

Порог отсечения	Точность, %	Полнота, %	F_1-мера, %
1,2	94,80	94,02	94,41
$2{,}5 * \mu$	96,90	97,39	97,14
$\mu + \sigma$	96,89	97,41	97,15

Согласно табл.3, разработанный алгоритм достигает F_1-меры в 97,15%, тем самым демонстрируя высокое качество обнаружения области и границ концентрированного искажения.

Программная реализация изложенных в статье алгоритмов размещена в открытом доступе[4].

4. Обсуждение результатов

Хотя разработанный метод демонстрирует высокое качество, алгоритм обнаружения границ искаженной области позволяет определять границы только прямоугольной области [10, 11], тогда как имеют место патчи других форм, в том числе круглой [12]. Определение границ таких искажений является ограничением разработанного решения.

Возможно устранение указанного ограничения путем модификации или замены алгоритма обнаружения границ искаженной области.

Заключение

Разработанный метод дополняет ранее предложенный метод устранения пиксельных искажений. Совместное последовательное применение указанных методов расширяет область применения метода устранения искажений за счет снижения влияния его ограничений.

СПИСОК ЛИТЕРАТУРЫ/REFERENCES:

1. Есипов Д.А., Бучаев А.Я., Керимбай А., Пузикова Я.В., Сайдумаров С.К., Сулименко Н.С., Попов И.Ю., Кармановский Н.С. Атаки на основе вредоносных возмущений на системы обработки изображений и методы защиты от них. Научно-технический вестник информационных технологий, механики и оптики. 2023, т. 23, № 4, с. 720-733. DOI: https://doi.org/10.17586/2226-1494-2023-23-4-720-733.
   Esipov D.A., Buchaev A.Y., Kerimbay A., Puzikova Y.V., Saidumarov S.K., Sulimenko N.S., Popov I.Yu., Karmanovskiy N.S. Attacks based on malicious perturbations on image processing systems and defense methods against them. Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2023, v. 23, no. 4, pp. 720-733. DOI: https://doi.org/10.17586/2226-1494-2023-23-4-720-733 (in Russian).
2. Esipov D.A. An approach to detecting L0-optimized attacks on image processing neural networks via means of mathematical statistics. Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2024, v. 24, no. 3, pp. 490-499. DOI: https://doi.org/10.17586/2226-1494-2024-24-3-490-499.
3. Есипов Д.А. Басов М.И. Клетенкова А.Д. Обнаружение неконвенциональных пиксельных атак посредством статистического анализа распределения оценок аномальности. Научно-технический вестник информационных технологий, механики и оптики. 2025, т. 25, № 1, с. 128-139 (на англ. яз.). DOI: https://doi.org/10.17586/2226-1494-2025-25-1-128-139.
   Esipov D.A., Basov M.I., Kletenkova A.D. Detection of L0-optimized attacks via anomaly scores distribution analysis. Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2025, v. 25, no. 1, pp. 128-139. DOI: https://doi.org/10.17586/2226-1494-2025-25-1-128-139.
4. Есипов, Дмитрий А.; Сулименко, Никита С.; Попов, Илья Ю. Метод устранения искажений, встраиваемых пиксельными атаками, [S.l.], т. 32, № 3, с. 13–25, 2025. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2025.3.02.
   Yesipov, Dmitry A.; Sulimenko, Nikita S.; Popov, Ilya Yu. A method of eliminating malicious perturbations embedded by L0-optimized attacks. IT Security (Russia), [S.l.], v. 32, no. 3, pp. 13-25, 2025. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2025.3.02 (in Russian).
5. Severino A., Curto S., Barberi S., Arena F., Pau G. Autonomous vehicles: an analysis both on their distinctiveness and the potential impact on urban transport systems. Applied Sciences. 2021, v. 11, no. 8, p. 3604. DOI: https://doi.org/10.3390/app11083604.
6. Wang L., Fan X., Chen J., Cheng J., Tan J., Ma X. 3D object detection based on sparse convolution neural network and feature fusion for autonomous driving in smart cities. Sustainable Cities and Society. 2020, v. 54, p. 102002. DOI: https://doi.org/10.1016/j.scs.2019.102002.
7. Chen L., Lin S., Lu X., Cao D., Wu H., Guo C., Liu C. Wang F.Y. Deep neural network based vehicle and pedestrian detection for autonomous driving: A survey. IEEE Transactions on Intelligent Transportation Systems. 2021, v. 22. no. 6, pp. 3234-3246. DOI: https://doi.org/10.1109/TITS.2020.2993926.
8. Sarvamangala D. R., Kulkarni R. V. Convolutional neural networks in medical image understanding: a survey. Evolutionary intelligence. 2022, v. 15, no. 1. pp. 1-22. DOI: https://doi.org/10.1007/s12065-020-00540-3.

[4]GitHub. iNDm3802. Adversarial patch detection method. URL: https://github.com/iNDm3802/Adversarial-patch-detection-method (дата обращения: 18.09.2025).

9. Zhang Y., Shi D., Zhan X., Cao D., Zhu K., Li Z. Slim-ResCNN: A deep residual convolutional neural network for fingerprint liveness detection. IEEE Access. 2019, v. 7, pp. 91476-91487. DOI: https://doi.org/10.1109/ACCESS.2019.2927357.
10. Karmon D., Zoran D., Goldberg Y. Lavan: Localized and visible adversarial noise. International Conference on Machine Learning. 2018, pp. 2507-2515. DOI: https://doi.org/10.48550/arXiv.1801.02608.
11. Liu, X., Yang, H., Liu, Z., Song, L., Li, H., Chen, Y. Dpatch: An adversarial patch attack on object detectors. arXiv preprint arXiv:1806.02299, 2018. DOI: https://doi.org/10.48550/arXiv.1806.02299.
12. Liu, A., Wang, J., Liu, X., Cao, B., Zhang, C., Yu, H. Bias-based universal adversarial patch attack for automatic check-out. Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part XIII 16. 2020, pp. 395-410. DOI: https:// doi.org/10.1007/978-3-030-58601-0 24.
13. McLachlan G.J. Mahalanobis distance. Resonance. 1999, v. 4, no. 6, pp. 20-26. DOI: https://doi.org/10.1007/bf02834632.
14. Papernot N., McDaniel P., Jha S., Fredrikson M., Celik Z. B., Swami A. The limitations of deep learning in adversarial settings. 2016 IEEE European symposium on security and privacy (EuroS&P). 2016, pp. 372-387. DOI: https://doi.org/10.1109/EuroSP.2016.36.

Конфликт интересов. *Авторы заявляют об отсутствии конфликта интересов.*
Conflict of interest. *The authors declare no conflict of interest.*

ИНФОРМАЦИЯ ОБ АВТОРАХ:

Дмитрий Андреевич Есипов, *к.т.н.; ассистент, Национальный исследовательский университет ИТМО.*
e-mail: some1else.d.ma@gmail.com,
https://orcid.org/0000-0003-4467-5117.

Алёна Дмитриевна Клетенкова, *младший аналитик, АО «Позитив Текнолоджиз».*
e-mail: alyonka8855@mail.ru,
https://orcid.org/0009-0001-8148-6764.

Илья Юрьевич Попов, *к.т.н., доцент; Национальный исследовательский университет ИТМО.*
e-mail: ilyapopov27@gmail.com,
https://orcid.org/0000-0002-6407-7934.

INFORMATION ABOUT THE AUTHORS:

Dmitry Andreevich Yesipov, *Ph.D.; Assistant Professor, ITMO University.*
e-mail: some1else.d.ma@gmail.com,
https://orcid.org/0000-0003-4467-5117.

Alyona Dmitrievna Kletenkova, *Junior Analyst, Positive Technologies.*
e-mail: alyonka8855@mail.ru,
https://orcid.org/0009-0001-8148-6764.

Ilya Yuryevich Popov, *Ph.D., Associate Professor; ITMO University.*
e-mail: ilyapopov27@gmail.com,
https://orcid.org/0000-0002-6407-7934.

Статья поступила в редакцию 17.09.2025; одобрена после рецензирования 20.12.2025; принята к публикации 20.01.2026
The article was submitted 17.09.2025; approved after reviewing 20.12.2025; accepted for publication 20.01.2026