

УДК 004.056

doi: 10.15622/rcai.2025.088

СНИЖЕНИЕ СЛОЖНОСТИ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ НА ОСНОВЕ МЕТОДА АВТОМАТИЧЕСКОЙ ЛОКАЛИЗАЦИИ АНОМАЛИЙ В МНОГОМЕРНЫХ ПРОСТРАНСТВАХ

А.Я. Бучаев (*abdulhamid0055@yandex.ru*)

И.И. Комаров (*i_krov@mail.ru*)

Университет ИТМО, Санкт-Петербург

В работе представлен способ снижения сложности интеллектуального анализа, основанный на автоматической локализации и группировке однородных и аномальных объектов в многомерных пространствах. Предложенный метод направлен на динамическую работу в условиях изменяющейся входной выборки, такой результат достигается использованием статистического анализа и формального метода принятия решения, что также позволяет легко интерпретировать результаты группировки и локализации. Таким образом, интеллектуальный анализ фокусируется на статистически неустойчивых объектах выборки и отделяет их друг от друга, что обеспечивает снижение риска атаки уклонения с использованием видимых вредоносных вставок. В качестве примера практического применения полученных результатов рассматривается динамическая маска матрицы внимания визуального трансформера. Применение предложенного решения позволяет исключить квадратичную сложность механизма внимания без предварительного регулирования маски и в режиме реального времени.

Ключевые слова: кибербезопасность, определение порога аномальности, вектор признаков, статистическая устойчивость, интеллектуальный анализ данных, механизм принятия решений, визуальный трансформер.

Введение

При интеллектуальном анализе среди множества обрабатываемых объектов и их признаков встречаются однородные выборки объектов, представленные в различных видах от скользящих окон при анализе временных рядов до фрагментов изображений. При этом существующие меха-

низмы, предназначенные для сопоставления фактов и выделения информации для дальнейшего интеллектуального анализа, используют всю подаваемую на вход информацию, описывающую объект выборки.

Побочным эффектом такого подхода являются повышение вычислительной сложности процесса выделения ключевой информации, снижение фокусировки интеллектуального анализа, а также возникновение потенциального риска атаки уклонения на модель интеллектуального анализа.

Предполагается, что обобщение однородных объектов позволит снизить вычислительную сложность при обработке входных данных интеллектуальной моделью. Такой подход позволяет обратить внимание на статистически нерегулярные объекты, которые несут в себе больше информации, и проводить их интеллектуальный анализ независимо.

Процесс предобработки входной выборки объектов для интеллектуального анализа должен сопровождаться выделением области интересов, основанным на формализованных, доказуемых и главное – интерпретируемых методах предобработки и принятия решения. Таким образом, прикладная система интеллектуального анализа снизит время обработки данных и потребляемые ресурсы, улучшит фокусировку на нетривиальных объектах и разграничит объекты анализа, сохраняя интерпретируемость выходных результатов, так как степень декомпозиции и возможность качественной интерпретации результатов влияют на конечное восприятие и уровень доверия пользователя в отношении используемой системы.

В работе предлагается способ снижения сложности интеллектуального анализа данных за счет автоматической локализации аномалий в многомерных пространствах на основе формального метода определения порога принятия решения.

Целью данной работы является снижение ресурсоемкости при интеллектуальной обработке данных и обеспечение безопасности путем локализации объектов и аномалий в многомерном пространстве.

Объект исследования – процесс интеллектуального анализа данных, представленных набором объектов.

Предмет исследования – формальные методы определения порога принятия решения в задачах кластеризации.

1. Научно-методический аппарат

Одним из актуальных механизмов интеллектуального анализа является механизм внимания, определяющий взаимную «важность» между входными объектами. Существенным ограничением механизма внимания является квадратичная сложность. Для решения этой проблемы авторы работы [Sun et al., 2025] предлагают ряд подходов, включая различные типы масок механизма внимания, сведение самовнимания к линейной сложности, в том числе гибридные вариации моделей, комбинирующие линейные

слои и слои с полным вниманием, подчеркивая, что снижение вычислительных затрат является важным этапом для будущих исследований долгосрочных последовательностей, мультимодальности и сложного (многоэтапного) мышления.

Фиксированные маски для матрицы внимания выполняют разделение связей объектов друг с другом на две группы: связь объектов есть; нулевая связь, но такой разделение не являются универсальным решением, необходимо подбирать предложенные маски в соответствии с предполагаемым графом связей объектов друг с другом. Такой подход не учитывает физическую сущность и динамику процессов, поэтому необходимо проводить разделение связей объектов друг с другом на основе формального и динамического метода определения порога разделения или принятия решения.

Методы определения порога принятия решения разделяются на две большие группы: формальные и эвристические, в рамках данной работы необходимым требованием является автономность модуля принятия решения, то есть рассматривается полностью автоматическое решение. Исходя из этого, интересующей группой являются формальные методы определения порога, которые подразделяются на:

- статистические методы на основе Монте-Карло, которые учитывают ретроспективную статистику. Такие методы являются статичными и требуют периодичного обновления информации для соответствия актуальным объектам информационной системы [Shen et al., 2021], [Xu et al., 2022];
- методы с применением теории игр используют экспертную аналитику для оценки влияния тех или иных факторов на отклик целевой функции. В дальнейшем полученные оценки входят в основу математической модели [Ni et al., 2024], [Li et al., 2021];
- методы математического программирования (методы оптимизации) применяются, когда задача механизма принятия решения описывается, например, системой линейных уравнений, решаемых методами линейного программирования. В случаях, когда зависимости механизма принятия решения не сводятся к линейным, применяют методы нелинейного программирования, которые в общем случае решают задачу поиска локальных оптимумов.

Задачу разделения совокупности элементов на типичные и нетипичные (аномальные) элементы можно рассматривать как задачу разделения совокупности объектов на несколько групп, то есть поиск границ или порогов разделения совокупности. В таком случае, имея минимум два класса – типичные и нетипичные элементы, можно использовать метод бинаризации Оцу [Otsu et al., 1979], который основан на принципе минимизации внутриклассовой дисперсии, влекущей максимизацию межклассовой дисперсии. Данный метод имеет вычислительную сложность $O(n)$, где

n – число возможных значений. Изначально метод использовался для би-наризации изображений градаций серого, однако Авторы работы [Liao et al., 2001] представили метод разделения совокупности элементов на множество классов по тому же принципу максимизации межклассовой дисперсии Оцу. Рассмотренные методы сегментации изображений применимы и в другой области определения – вещественных числах. Главным компонентом при использовании методов разделения выборки на классы на основе подхода Оцу является гистограмма значений, формируемая из области определения объектов выборки.

В качестве исходной выборки объектов будет использоваться совокупность фрагментов размером 100 на 100 пикселей изображения (рис. 1.а), обработка которого в рамках задачи выявления нетипичных объектов выполняется в соответствии с предыдущей научной работой [Бучаев и др., 2024]. Разделение изображения на фрагменты является одним из этапов обработки данных визуальным трансформером в части кодировщика. Масштабируемость используемых и предложенных методов позволяет обрабатывать входные совокупности различной природы, например, в работе [Ляховенко и др., 2024] Авторы описывают модель построения многомерного пространства автономных транспортных средств. Однако для простоты визуализации и обработки данная работа сосредоточена на обработке изображений визуальным трансформером.

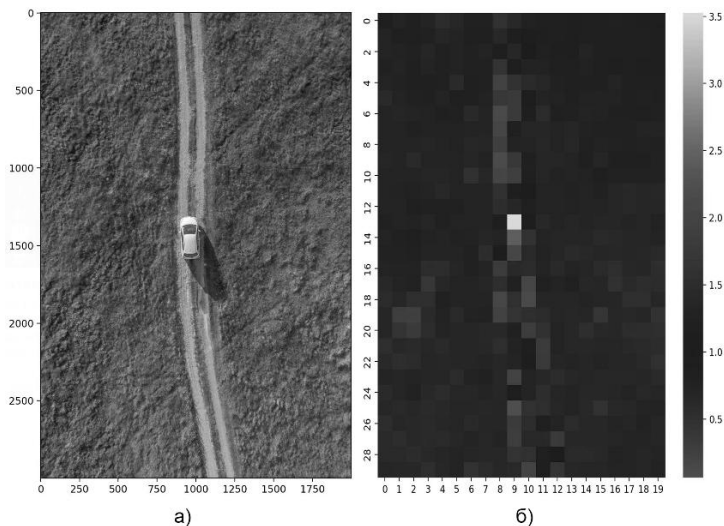


Рис. 1. а) исходное изображение; б) тепловая карта в соответствии с показателем отклонения дисперсии

В таком случае разделяемой на классы совокупностью будет являться набор показателей отклонений дисперсии фрагментов изображения (рис. 2). При использовании классического метода Оцу было получено следующее разделение на группы типичных (значения меньше порога) и нетипичных (значения больше порога) фрагментов изображения, порог принятия решения в данном случае равен 1,127.

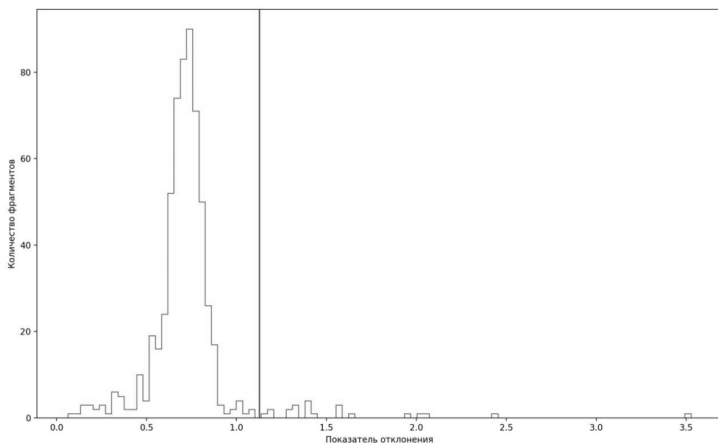


Рис. 2. Гистограмма плотности распределения значений показателя отклонения дисперсии фрагментов изображения с разделением на классы

2. Определение строгости порога аномальности относительно степени однородности изображения

Определение порога аномальности необходимо проводить с учётом динамики информационной системы, в том числе – физической сущности и динамики процессов. Предполагается, что для однородной выборки автоматическое вычисление порога должно быть более строгим, чем вычисление порога в разнородной выборке, где в рамках общей статистики выбросом является однородный фрагмент, то есть деление на классы происходит наоборот. Следовательно, в случае однородной выборки степень допустимого отклонения дисперсии текущего фрагмента от общей дисперсии выборки должна быть меньше.

Гипотеза А: абсолютная разница среднего и медианы объекта, имеющего равномерное распределение вероятностей значений каждого компонента вектора описателя объекта по отдельности и представляющего однородную структуру (количественное преимущество имеет только одно значение среди наборов значений по каждой компоненте, то есть низкая энтропия), стремится к нулю.

Обоснование А (для изображения): в случае, когда структура отдельной компоненты фрагмента Х представлена преимущественно одним значением , и распределение вероятностей значений структуры отдельной компоненты фрагмента стремится к равномерному, , следовательно, .

Согласно Гипотезе А, чем меньше абсолютная разница среднего и медианы структуры отдельной компоненты фрагмента, тем более однородное и равномерное распределение значений компоненты он имеет. Для вычисления «степени» однородности [Arafeh et al., 2022] предполагается использовать расстояние Хеллингера, которое оценивает степень разности двух дискретных распределений вероятности и [Kumari et. al., 2017] (2.1).

$$= \frac{1}{k} \sum_{k=1}^k \left| \frac{p_k}{k} - \frac{q_k}{k} \right| \tag{2.1}$$

где k – количество значений дискретного распределения; – вероятность k-го элемента.

Предлагается сравнивать распределение вероятностей текущего фрагмента и распределение вероятностей сгенерированного набора значений (для изображений от 0 до 255), имеющего распределение близкое к равномерному. Результаты, полученные в ходе проверки гипотезы, показаны на рис. 3.

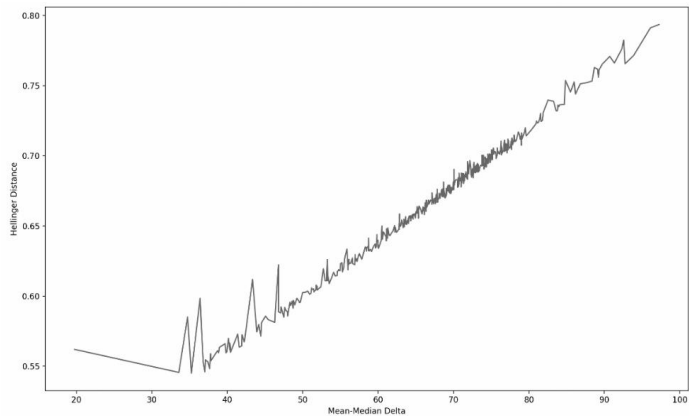


Рис. 3. Усредненная по трем компонентам изображения зависимость расстояния Хеллингера от разности среднего и медианы

Предложенная гипотеза о разности среднего и медианы имеет ряд ограничений, связанных со случаями, когда фрагмент данных содержит в себе перетекающие градиенты. В таком случае , однако структура отдельной компоненты фрагмента не имеет равномерного рас-

пределения вероятностей и однородности в совокупности значений компоненты. Подобные случаи можно наблюдать в первом, третьем и пятом наблюдениях графика, исходные части которых изображены на рис. 4.

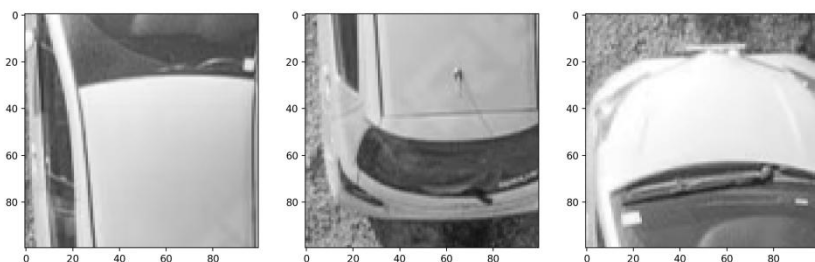


Рис. 4. Фрагменты изображения, не соответствующие предложенной гипотезе о разнице среднего и медианы

3. Результат работы и преимущества автоматической локализации

На исходном изображении (рис. 1,а) можно наблюдать 2 однородные среды – зеленое поле и элементы дороги (включая боковые насыпи). Используя модификацию метода Оцу для многоклассового разделения, были получены результаты, представленные на рис. 5,а. Для данного случая были получены два значения, разделяющие совокупность на три среды – 0,543 и 1,161.

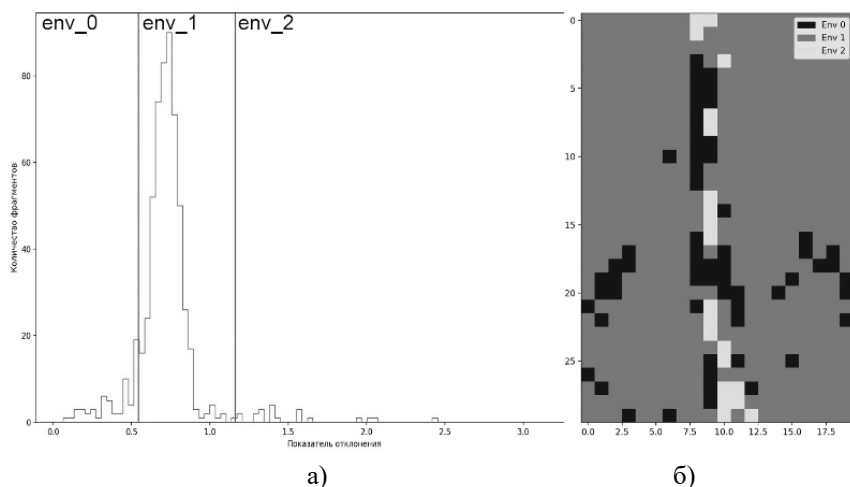


Рис. 5. а) разделение совокупности значений показателя отклонения дисперсии фрагментов на три класса; б) группировка однородных фрагментов изображения

Определяя строгость порога аномальности в соответствии с абсолютной разницей медианы и среднего, были получены результаты сегментирования исходного изображения на три класса. На рис. 5,б можно наблюдать разделение фрагментов на классы в соответствии со средами, определяемым формальными статистическими методами.

Результат работы предложенного метода позволяет сгруппировать однородные фрагменты изображения, динамически формируя маску для механизма внимания, то есть при векторизации похожие фрагменты изображения будут иметь большую связь в матрице внимания, а объекты, принадлежащие разным группам (кластерам), будут иметь слабую связь. Таким образом, динамически формируется маска для матрицы внимания с учетом физической сущности обрабатываемой выборки.

Заключение

В работе представлен способ снижения сложности интеллектуального анализа данных, основанный на методе автоматической локализации и группировки однородных объектов и аномальных объектов входной совокупности обрабатываемых данных. Предложенный метод масштабируется на пространства большей размерности, является интерпретируемым и динамическим, что соответствует требованиям технологий, в которых предполагается его применение. Вместе с этим осуществляется снижение риска атаки уклонения, так как группировка объектов разграничивает объекты, содержащие вредоносные вставки, от легитимных объектов из-за нарушения статистической устойчивости.

В дальнейшей планируется проведение экспериментов по преобразовке входных данных и последующей обработке визуальным трансформером с использованием динамической маски матрицы внимания.

Список литературы

- [Бучаев и др., 2024] Бучаев А.Я., Бегаев А.Н., Комаров И.И. Метод автоматического обнаружения аномалий в пространстве событий информационной безопасности // Промышленные АСУ и контроллеры. – 2024. – № 2. – С. 31-41.
- [Ляховенко и др., 2024] Ляховенко Ю.А., Мухамеджанов С., Комаров И.И. Метод Построения Модели Пространства Автономных Транспортных Средств // International Journal of Open Information Technologies. – 2024. – Т. 12, № 7. – С. 38-42.
- [Arafteh et al., 2022] Arafteh, Mohamad & Hammoud, Ahmad & Otrok, Hadi & Mourad, Azzam & Talhi, Chamseddine & Dziong, Zbigniew. Independent and Identically Distributed (IID) Data Assessment in Federated Learning. – 2022. – P. 293-298. – 10.1109/GLOBECOM48099.2022.10001718.
- [Kumari et al., 2017] A. Kumari and U. Thakar, "Hellinger distance based over-sampling method to solve multi-class imbalance problem," 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), Nagpur, India, 2017. – P. 137-141. – doi: 10.1109/CSNT.2017.8418525.

- [Li et al., 2021] Li Y, Fan Z. and Zhao X. Game Decision of a Closed-loop Supply Chain with components remanufacturing // 2021 IEEE International Conference on Recent Advances in Systems Science and Engineering (RASSE), Shanghai, China, 2021. – P. 1-6. – doi: 10.1109/RASSE53195.2021.9686926.
- [Liao et al., 2001] Liao, Ping-Sung, Tse-Sheng Chen and P. C. Chung. A Fast Algorithm for Multilevel Thresholding // J. Inf. Sci. Eng. – 2001. – 17. – P. 713-727.
- [Ni et al., 2024] Ni W. and Zhang Y. Threshold Detection of Cloud Computing System with Impatient Users Based on Game Theory // 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Tianjin, China, 2024. – P. 3128-3133. – doi: 10.1109/CSCWD61410.2024.10580422.
- [Otsu et al., 1979] Otsu N. A threshold selection method from gray-level histogram // IEEE Transactions on System Man Cybernetics. – 1979. – Vol. SMC-9, No. 1. – P. 62-66.
- [Shen et al., 2021] Shen L. and Wang S. Monte Carlo Tree Search for Network Planning for Next Generation Mobile Communication Networks // 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 2021. – P. 1-6. – doi: 10.1109/GLOBECOM46510.2021.9685526.
- [Sun et. al., 2025] Sun W., Hu J., Zhou Y. et. al. Speed always wins: A survey on efficient architectures for large language models [Электронный ресурс] // arXiv. – 2025. – Режим доступа: <https://arxiv.org/abs/2508.09834> (дата обращения: 16.08.2025).
- [Xu et. al., 2022] Xu L., Hurtado-Gruoso J., Jeurissen D., Liebana D.P. and Dockhorn A. Elastic Monte Carlo Tree Search with State Abstraction for Strategy Game Playing // 2022 IEEE Conference on Games (CoG), Beijing, China, 2022. – P. 369-376. – doi: 10.1109/CoG51982.2022.9893587.