Национальная безопасность / nota bene
Правильная ссылка на статью:
Горохова Р.И., Никитин П.В. Алгоритмы обнаружения дублирующего контента в изображениях критической информационной инфраструктуры с использованием методов машинного обучения // Национальная безопасность / nota bene. 2024. № 6. DOI: 10.7256/2454-0668.2024.6.71885 EDN: SMNUAJ URL: https://nbpublish.com/library_read_article.php?id=71885

Алгоритмы обнаружения дублирующего контента в изображениях критической информационной инфраструктуры с использованием методов машинного обучения

Горохова Римма Ивановна

ORCID: 0000-0001-7818-8013

кандидат педагогических наук

ведущий научный сотрудник; институт цифровых технологий; Финансовый университет при Правительстве РФ

125993, Россия, г. Москва, Ленинградский пр-т, 49

RIGorokhova@fa.ru

Никитин Петр Владимирович

ORCID: 0000-0001-8866-5610

кандидат педагогических наук

доцент; кафедра искусственного интеллекта; Финансовый университет при Правительстве РФ

125167, Россия, г. Москва, Ленинградский пр-т, 49

pvnikitin@fa.ru

Статья из рубрики "Научно-техническое обеспечение национальной безопасности"

DOI:

10.7256/2454-0668.2024.6.71885

EDN:

SMNUAJ

Дата направления статьи в редакцию:

04-10-2024

Дата публикации:

04-12-2024

Аннотация: В статье рассматривается метод выявления аномалий в визуальном контенте критической информационной инфраструктуры. Этот метод основывается на сравнении хэш-строк, получаемых из визуальных данных, для обнаружения потенциальных отклонений или дублирующего контента, который может указывать на нарушения авторских прав, распространение неправомерного контента или другие угрозы безопасности. Предметом исследования является процесс выявления аномалий в изображениях критической информационной инфраструктуры (КИИ) с использованием технологии хэширования. Актуальность исследования обусловлена растущей угрозой нарушений авторских прав и распространения нелегального контента. С учетом усложнения методов кибератак и увеличения объема визуального контента, анализ и мониторинг изображений становятся особенно важными. Критическая информационная структура, включая системы государственного управления, науки, экономики и энергетики, напрямую зависят от защиты своей информации. Поэтому выявление аномалий в изображениях и их оперативное реагирование играют ключевую роль в сохранении целостности и конфиденциальности данных. Целью являются разработка алгоритма для идентификации дублирования контента и создание эффективного инструмента для мониторинга изображений. В работе применяется интеграция методов компьютерного зрения и алгоритмов машинного обучения. Разработка включает использование хэш-строк для прецизионного сравнения изображений. Научная новизна данного исследования заключается в разработке и внедрении нового подхода к выявлению аномалий в изображениях критической информационной инфраструктуры с использованием технологии хэширования. Применение технологии обеспечивает уникальные идентификаторы для визуальных данных и позволяет эффективно сравнивать и анализировать изображения. Такой подход значительно увеличивает скорости обработки данных и точность выявления дублирования контента и аномалий в изображениях. Классификация изображений на основе хэширования обеспечивает более высокую степень чувствительности к аномалиям и позволяет отсеивать ложные срабатывания, что является критически важным для организаций с высоким уровнем защищенности информации. Результаты показывают высокую эффективность предложенного метода, достигнута значительная степень точности в выявлении аномалий, что подтверждено экспериментами на реальных данных. Представленные алгоритмы продемонстрировали улучшение по сравнению с существующими решениями.

Ключевые слова:

критическая информационная инфраструктура, визуальный контент, аномалии, угрозы, компьютерное зрение, похожие изображения, дублирующий контент, хэш-строки, перцептивное хэширование, машинное обучение

Введение. В визуальном контенте критической информационной инфраструктуры (КИИ) могут встречаться различные виды аномалий, которые представляют потенциальные угрозы информационной безопасности. Аномалии могут быть представлены в виде вредоносных изображений, содержащих вредоносный код или скрипты (например, XSS-атаки, встроенные эксплойты) или намеренно искаженных для обхода систем фильтрации и обнаружения; фальсифицированных изображений, представляющих собой поддельные или сфабрикованные изображения, используемые для дезинформации и манипулирования или подвергшиеся манипуляциям для сокрытия или искажения информации; изображения-индикаторы компрометации, содержащие признаки

вторжения, таргетированных атак или действий злоумышленников; нетипичные или подозрительные изображения, не соответствующие "нормальному" визуальному контенту, характерному для данной КИИ, демонстрирующие аномальные характеристики, отклоняющиеся от установленных шаблонов или политик безопасности или связанные с нетипичными событиями в функционировании КИИ. Следует отметить, что вопросы обеспечения безопасности исследуются очень активно в настоящее время.

Информационная безопасность является важной составляющей самых различных сфер. Специфика угроз рассматривается в исследовании Ромашковой О. Н. и Каптерева А. И. [1], выявление и классификация угроз, которые могут возникать для различных объектов, включая как информационные системы, так и физические активы приведено в работе Турянской К. А.[2], актуальные угрозы, связанные с использованием облачных вычислений приведены в статье Боярчука Д. А., Фролова К. А. и Склярука В. Л.[3], ключевые аспекты, связанные с охраной информации в условиях цифровизации, включая уязвимости новых технологий, способов реагирования на инциденты и важность разработки стратегий управления рисками исследованы в работе Мустафаева А. Г., Кобзаренко Д. Н., Бучаева А. Я.[4], Емельянов А. А. анализирует риски и уязвимости, которые могут возникнуть при использовании гипервизоров, и их влияние на защиту виртуализированных сред [5].

Различные подходы предлагаются к моделированию угроз с помощью разработки сценариев для выявления уязвимостей и предсказания возможных атаки на информационные ресурсы [6]. Комплексный подход к управлению рисками и необходимость постоянного мониторинга угроз предлагается в работе Гриня В.С. [7]. Автор представляет рекомендации по предотвращению утечек информации, включая методы контроля доступа, аудит систем и обучение персонала.

В статье Бекмухан А. и Усатовой О.[8] исследуются подходы к повышению уровня безопасности мультисерверных веб-приложений и систем. В работе рассматриваются методы управления рисками, включая идентификацию угроз, оценку уязвимостей, а также применение технологий для обеспечения защиты данных.

Вопросы верификации информации в условиях современного информационного потока подробно рассмотрены в работе Шестеркиной Л.П., Красавиной А.В. и Хакимовой Е.М. [9]. Авторы охватывают различные аспекты процесса проверки фактов, включая методы оценки достоверности источников информации, использование эффективных инструментов и технологий, а также признаки недостоверных данных.

Вопросам обработки изображений в последнее время занимается все большее количество исследователей. В статье Алпатова А. Н.[10] проведен анализ современных подходов и методов анализа видеопотока с целью выявления аномальных событий, имеющих глубокий генезис. Автор подчеркивает важность своевременного обнаружения аномалий для повышения безопасности и эффективности различных систем, таких как видеонаблюдение, охрана и мониторинг. В работе обосновываются основные характеристики глубокого генезиса аномалий, а также анализируются алгоритмы и технологии, используемые для их выявления. Ключевым аспектом исследования является применение методов машинного обучения и искусственного интеллекта для автоматизации процесса анализа и повышения точности обнаружения. В работе [11] проведено исследование применения нейронных сетей в контексте изучения

визуального контента с точки зрения информационной безопасности, а в статье [12] показаны возможности различных технологий ИИ, такие как машинное обучение, анализ больших данных и нейронные сети, и их влияние на диагностику, лечение и профилактику заболеваний на основе анализа имеющихся изображений.

Программно-техническое решение, включающее алгоритмы машинного обучения и методы анализа данных, которые позволяют эффективно идентифицировать потенциально опасные мультимедийные объекты приведены в статье Пилькевича С. В. и др. [13]. Кроме того, акцентируется внимание на значимости исследования в контексте повышения кибербезопасности и защиты пользователей от вредоносного контента.

Механизмы, с помощью которых злоумышленники могут манипулировать изображениями, создавая искаженные данные, что может привести к ошибкам в их интерпретации рассмотрены в исследовании [14]. рассматриваются современные угрозы, связанные с воздействием вредоносных возмущений на системы компьютерного зрения. Авторы анализируют различные типы атак, сценарии их реализации и последствия для надежности и безопасности систем обработки изображений.

В качестве ответа на эти угрозы авторы обсуждают существующие методы защиты и разработки, направленные на повышение устойчивости систем к вредоносным воздействиям. Рассматриваются подходы, основанные на использовании различных алгоритмов фильтрации и регуляризации, а также применение методов обучения, способных улучшить обобщающую способность моделей.

В статье [15] предложен инновационный подход к выявлению вредоносного ПО. Авторы предлагают метод, в котором бинарный код программ преобразуется в изображения, что позволяет использовать уже существующие алгоритмы машинного обучения для анализа и распознавания угроз. Статья описывает процесс преобразования бинарных файлов в двумерные изображения и обосновывает выбор данной техники как средства борьбы с вредоносным ПО. В работе [16] на основе применения сверточных нейронных сетей показана возможность статического анализа приложений, представленных в виде последовательности байтов и дальнейшего перевода полученных данных в формат изображения для обнаружения вредоносных программ.

Следует отметить, что многие работы были сосредоточены на преобразовании бинарных исполняемых файлов в изображения. Например, в работе [17] авторы группируют двоичные последовательности исполняемых файлов по 8-битным векторам. Преобразованные 8-битные векторы затем преобразуются в черно-белые изображения. После процесса преобразования авторы непосредственно применяют алгоритм random forest для классификации вредоносных программ, используя значения пикселей в качестве объектов. В исследованиях [18, 19] авторы извлекают визуальные признаки с помощью классических экстракторов объектов компьютерного зрения.

Вопросы обнаружения вредоносных изображений и связанная с этим проблема кибербезопасности представлены в работах [20, 21]. Авторы подчеркивает, что файлы изображений могут использоваться для распространения вредоносного ПО, обходя традиционные механизмы фильтрации. Как отмечается в [22], для классификации легитимных и вредоносных файлов использовались следующие признаки: размер файла, максимальный размер маркеров, количество маркеров, количество байтов после конца файла. Для классификации легитимных и вредоносных JPEG-файлов были использованы следующие методы машинного обучения: деревья решений и ансамбли деревьев

решений: случайный лес и стохастический градиентный бустинг [23].

В статье [24] авторы объясняют, что перцептивное хеширование позволяет создавать хеши изображений, которые учитывают их визуальные характеристики, а не просто битовые представления. Такой подход обеспечивает более устойчивую идентификацию, даже если изображения подвергались изменениям, таким как изменение размеров, сжатие или незначительные перемены в цветах. Авторы [25] подчеркивают, что эффективное сравнение изображений имеет ключевое значение для приложений в области компьютерного зрения, таких как управление мультимедийным контентом, цифровая фотография и системы мониторинга.

В работе [26] рассматриваются различные метрики расстояния, применяемые для анализа и сравнения растровых изображений. Кроме того, авторы обсуждают влияние выбора метрики на качество распознавания и сопоставления изображений, приводят примеры сценариев, в которых различные метрики могут показывать значительные различия в продуктивности.

Выявление таких аномалий в визуальном контенте критической информационной инфраструктуры является важной задачей для обеспечения ее информационной безопасности и устойчивости к киберугрозам. Применение методов глубокого обучения позволяет создавать эффективные системы обнаружения и реагирования на данные виды аномалий.

Актуальность обусловлена необходимостью решения проблем, связанных управлением большим объёмом цифрового контента, выявлением дублирующегося контента, защитой авторских прав и борьбой с мошенничеством.

Модели должны быть способны выявлять аномалии в визуальном контенте, которые могут указывать на наличие вредоносного ПО, фишинговых атак или других угроз информационной безопасности.

Разработать подход, основанный на применении трансферного обучения и методов активного обучения, для адаптации моделей глубокого обучения к особенностям визуального контента критической информационной инфраструктуры. Цель - повысить точность и эффективность обнаружения аномалий в изображениях, загружаемых в КИИ и повышение контроля над использованием изображений за счет разработки алгоритма поиска одинаковых и похожих изображений в базе данных с использованием перцептивных хэш-строк.

Методы исследования

Поиск одинаковых и похожих изображений в базе данных – это важная задача в области компьютерного зрения, обработки изображений и систем управления данными. Различные подходы и методы позволяют эффективно решать эту задачу.

Хеширование изображений основано на создании уникального представления (хеша) для каждого изображения. Существует несколько методов хеширования:

- перцептивное хеширование (pHash), которое использует преобразования (например, дискретное косинусное преобразование) для создания компактного представления изображений и чем больше похожи два изображения, тем ближе их хеши в значении,

- классификационное хеширование (dHash и aHash), применяющее простые алгоритмы,

такие как вычисление разности между соседними пикселями (dHash) или создание среднего значения (aHash). Они также создают уникальные хеши, которые позволяют быстро определять схожесть.

Следующим методом является вычисление хешей, позволяющее сравнивать изображения. Для сравнения наиболее часто применяются методы:

- расстояние Хэмминга, позволяющее проводить быстрое сравнение битовых последовательностей хешей, определяя количество различий между ними,

- косинусное сходство, которое измеряет угол между векторами, представляющими изображения, и позволяет выявлять схожесть изображений по направлению их векторов.

Также одним из методов являются особенности извлечения для более точного поиска признаков, которые представляют изображение в виде высокоуровневых характеристик:

- сверточные нейронные сети (CNN) используются для извлечения глубоких признаков изображения, таких как текстуры, формы и цвета, и они представляют собой векторы, которые могут быть сравнены с помощью методов поиска, таких как kNN (k-Nearest Neighbors),

- методы извлечения ключевых точек, таких алгоритмов, как SIFT (Scale-Invariant Feature Transform) и SURF (Speeded-Up Robust Features), извлекают ключевые точки и описания изображений.

Анализ возможностей нескольких существующих систем поиска похожих изображений, таких как Яндекс Картинки, Google Images, Duplicate Photo Finder, VisiPics, их области применения и алгоритмов, на которых они основаны, представлены в таблице 1.

Существующие решения Google Images и Яндекс Картинки имеют ограничения API, скорости и пополняемости базы данных картинок. Duplicate Photo Finder и VisiPics имеют низкую устойчивость к модификациям. Таким образом, подходящего открытого решения для поставленной задачи нет.

Таблица 1–Сравнение существующих решений

Критерий Сервис	Яндекс Картинки	Google Images	Duplicate Photo Finder	VisiPics
Качество поиска дубликатов	Высокое	Высокое	Высокое	Высокое
Устойчивость к модификациям	Высокая	Высокая	Низкая	Низкая
Источник исследуемых изображений	Веб-страницы	Веб-страницы	Локальные файлы	Локальные файлы
Поиск для конкретного изображения	Да	Да	Нет	Нет
Доступность API	Ограничена	Ограничена	–	–
Скорость ответа	Низкая	Низкая	Высокая	Высокая
Полнота базы	Неполная	Неполная	–	–

данных	Неполная	Неполная		

Проведённый анализ позволил сделать вывод, что разработка метода поиска похожих изображений актуальна, поскольку существующие решения не обладают всей полнотой удовлетворения выбранным критериям. Сервисы, совершающие поиск изображений в локальных файлах не устойчивы к модификациям изображения, а способны выявлять только полные дубликаты. Также в них не предусмотрен поиск для конкретного изображения, доступен только полный обход директорий и выявление всех найденных пар дубликатов.

Существует несколько подходов к выявлению похожих изображений основными среди них можно выделить сравнение пикселей как последовательное сравнение значений пикселей изображений на одинаковых позициях, гистограммы изображений в виде анализа распределения яркости или цветовых характеристик изображения и формирования соответствующих гистограмм, использование свёрточных нейронных сетей, перцептивные хэши основанные на вычислении хэш-суммы изображения, которая учитывает его содержание. Сравнение методов представлено в таблице 2.

Таблица 2–Сравнение существующих методов

Критерий Метод	Сравнение пикселей	Сравнение гистограмм	Нейронные сети	Перцептивные хэш-алгоритмы
Устойчивость к модификациям	Низкая	Низкая	Высокая	Высокая
Сложность вычислений	Низкая	Низкая	Высокая	Низкая
Скорость вычислений	Высокая	Высокая	Низкая	Высокая
Требования к памяти	Низкие	Низкие	Высокие	Низкие
Сложность реализации	Низкая	Средняя	Высокая	Низкая

Метод на основе перцептивных хэш-функций прост в реализации, но при этом показывает высокую скорость и точность выявления дубликатов и похожих изображений, не требует больших вычислительных ресурсов.

Сравнительный анализ существующих перцептивных хэш-алгоритмов представлен в таблице 3.

Таблица 3 – Сравнительный анализ перцептивных хэш-алгоритмов

Критерий Алгоритм	Хэш по среднему	Хэш на основе ДКП*	Хэш на основе разности
Точность работы алгоритма: устойчивость к изменению размера, яркости и геометрическим модификациям	Низкая	**Высокая**	Низкая
Скорость вычисления хэша	Высокая	Средняя	Высокая

Сложность вычислений	Низкая	Средняя	Низкая
Объем памяти, занимаемой хэшем	Низкий	Средний	Низкий
Объем предварительной обработки изображения	Низкий	Высокий	Средний

В результате сравнения выбран алгоритм хэширования на основе дискретного косинусного преобразования (ДКП), так как он является самым точным и устойчивым к модификациям изображений.

Алгоритм работы выполняется по следующему алгоритму: к обработанному изображению применяется ДКП, которое позволяет разделить изображение на частоты, далее работа идет только с низкочастотными компонентами, а высокочастотные шумы и мелкие детали игнорируются, далее выполняется бинаризация, результатом которой является цепочка битов, на основе которой идет построение хэша.

Бинаризация выполняется в соответствие с формулой (1). В соответствие с формулой каждый коэффициент ДКП сравнивается со средним значением всей матрицы коэффициентов, если значение больше или равно среднему, то в цепочку битов записывается значение 1, иначе – 0. На выходе получаем хэш длиной 64 бита.

$$X[k] = \sum_{n=0}^{N-1} x[n] * cos\left(\frac{(2n+1) * k\pi}{2N}\right), k = \overline{0, N-1,} \qquad (1)$$

где $x[n]$ – последовательность точек сигнала, N – размер изображения, $X[k]$ – ДКП.

Для оценки надежности и дискриминационных характеристик хэширования изображений требуются метрики расстояния или сходства расстояние Хэмминга, нормализованное расстояние Хэмминга, коэффициент битовых ошибок, позволяющие определить различия между двумя схожими медиа-объектами. Исходя из этих данных, можно сделать вывод о том, являются ли изображения идентичными или совершенно различными, то есть два хэша должны отражать уровень их «визуального различия. Анализ метрик сходства по критериям скорость вычисления, сложность вычислений, объем памяти, точность вычислений, чувствительность к небольшим изменениям изображения показало эффективность работы метрики расстояние Хэмминга.

В качестве метрики сходства перцептивных хэшей выбрано Расстояние Хэмминга, так как метрика проста и быстра в вычислении, подходит для работы с хэшами одинаковой длины и дает прямое представление о количестве различий.

Она рассчитывается как количество позиций, в которых соответствующие символы двух битовых строк различны и *d* вычисляется по формуле (2):

$$d = \sum_{i=1}^{L} |x_i - y_i|, \qquad (2)$$

где *xi* и *yi* – значения битов хэш-функций *x* и *y*, *L* – длина хэша.

Основные этапы предлагаемого метода включают в себя (рисунок 1):

– предварительную обработку изображений;

– подготовку базы данных;

– генерацию хэша изображения;

– поиск схожих изображений на основе оценки сходства.

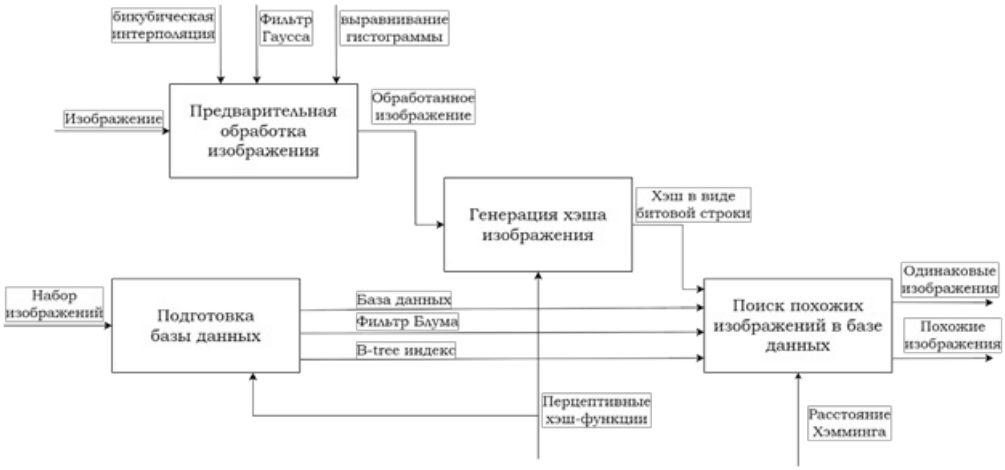

Рисунок 1 – Основные этапы метода

Этапы предварительной обработки изображения включают в себя последовательное выполнение операций:

– изменение размера: бикубическая интерполяция уменьшает объём данных для обработки, устраняет высокие частоты и детализацию изображения, изображение приводятся к размеру 32x32.

Бикубическая интерполяция вычисляется по формуле (3).

$$I_{new}(x,y) = (1-\alpha)*(1-\beta)*I(x_1,y_1) + \alpha*(1-\beta)*I(x_2,y_1) + (1-\alpha)*\beta*I(x_1,y_2) + \alpha*\beta*I(x_2,y_2), \quad (3)$$

где $I_{new}(x,y)$ – новое значение пикселя в x,y,

$I(x_1,y_1)$ – значение ближайшего пикселя,

$\alpha*\beta$ – дробные части координат x и y соответственно.

– нормализация цвета: применяется метод выравнивания гистограмм для повышения устойчивости к изменениям яркости и цветовой гаммы. Выравнивание гистограммы производится в соответствие с формулой (4).

$$I_{new}(x,y) = \frac{L-1}{M*N}\sum_{i=0}^{L-1} H(i), \quad (4)$$

где $I_{new}(x,y)$ – новое значение пикселя в x,y,

L – количество уровней яркости (256),

$M,$ – ширина и длина изображения,

$H(i)$ – гистограмма изображения.

– размытие: фильтр Гаусса применяется для уменьшения шума, сглаживания текстуры и уменьшения детализации изображений. Фильтр Гаусса вычисляется по формуле (5).

$$G(x,y) = \frac{1}{2\pi\sigma^2} e^{\frac{-(x^2+y^2)}{2\sigma^2}}, \quad (5)$$

где $G(x,y)$ – функция Гаусса в x, y,

σ – стандартное отклонение.

– сокращение цветов: путем вычисления среднего значения каналов RGB изображение преобразуется в оттенки серого для уменьшения объёма данных. Среднее значение каналов определяется по формуле (6).

$$I_{new}(x,y) = \frac{R+G+B}{3}, \quad (6)$$

где $I_{new}(x,y)$ – новое значение пикселя в x, y,

R, G, B – значение красного, зеленого и синего канала.

После выполнения всех операций предварительной обработки будет получена маленькая и размытая версия изображения в оттенках серого.

При стандартной реализации алгоритма поиск похожих изображений осуществляется путем расчета расстояния Хэмминга между хэшом искомого изображения и каждым изображением в базе данных, что является ресурсозатратным.

Для оптимизации в исследовании рассмотрено пороговое расстояние Хэмминга $k = 4$, тогда согласно фактору сегментации хэш можно разделить на 3 подстроки. Каждая подстрока будет храниться в отдельной таблице.

Фактор сегментации означает, что если разбить хэш на r частей, то найдется хотя бы $q = r - \left[\frac{k}{2}\right]$ подстрок, для которых расстояние Хэмминга будет не более единицы.

$$r = \left[\frac{k}{2}\right] + 1, \quad (7)$$

где r – фактор сегментации,

k – пороговое значение расстояния Хэмминга.

Тогда у похожих изображений каждая из подстрок либо полностью совпадёт, либо будет отличаться не более, чем на один бит.

Подготовка базы данных выполняется по следующему алгоритму:

- предварительная обработка полученного набора изображений,

- формирование хэша в виде битовых строк для каждого обработанного изображения,

- деление битовой строки на подстроки и получение набора подстрок изображения,

- создание таблиц для каждой подстроки,

- создание индексов и фильтра Блума для таблиц подстрок.

Таким образом, поиск изображений выполняется по алгоритму на рисунке 2. Хэш для

искомого изображения делится на 3 подстроки. Для выявления похожих изображений достаточно сгенерировать набор комбинаций подстрок, отличающихся максимум на один бит и далее проверять их наличие в базе данных.

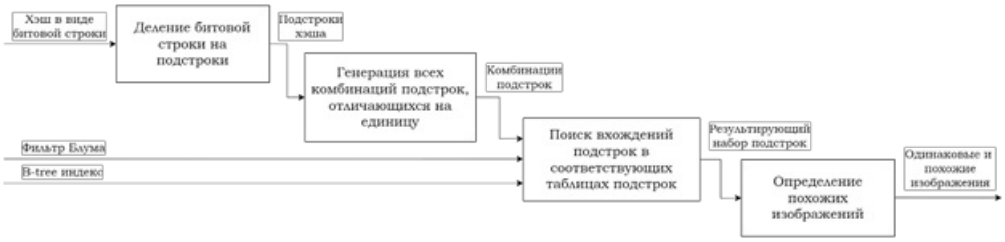

Рисунок 2 – Алгоритм поиска похожих изображений в базе данных

Для увеличения скорости поиска используются B-tree индексы и фильтр Блума. Фильтр Блума это вероятностная структура данных, которая может однозначно определить, что элемент отсутствует в наборе данных, таким образом уменьшая объем искомых подстрок в таблицах.

Для оценки времени работы алгоритма использовался набор данных из 1200 различных изображений со средним размером 3,2 Мб, поиск каждого изображения осуществлялся 5 раз, замерялось время поиска и считался средний результат. Было проведено сравнение времени работы алгоритмов поиска изображений для стандартного алгоритма, алгоритмов с делением хэш-строк и надстройками сервера, также с добавлением индексов и фильтром Блума и предложенным методом с делением хэш-строк, надстройками сервера, добавлением индексов и фильтром Блума. Итог показал, что разработанный алгоритм с делением хэша на подстроки, настройками сервера, индексами и фильтром Блума работает в 3 раза быстрее стандартной реализации.

Проводилась оценка устойчивости представленного алгоритма к модификациям изображений. Результаты проверки устойчивости разных хэш-алгоритмов к модификациям изображений показаны в таблице 4, где Ah - Хэш по среднему, Dh - Хэш на основе разности, Ph - Хэш на основе ДКП.

Таблица 4 – Устойчивость алгоритма к модификациям изображений

№	Тип модификации	Ah	Dh	Ph
1	Исходное изображение	0	0	0
2	Увеличение яркости	8	4	0
3	Уменьшение яркости	0	0	0
4	Увеличение контрастности	6	1	0
5	Уменьшение контрастности	4	3	0
6	Перевод в оттенки серого	0	0	0
7	Гамма-коррекция	2	1	0
8	Гауссова фильтрация	3	0	0
9	Добавление шума соли и перца	0	0	0
10	Добавление гауссова шума	2	1	0
11	Добавление водяного			

11	Добавление водяного знака	1	1	0
12	Добавление текста	1	1	0
13	Добавление объекта	6	1	1
14	Изменение размера	0	0	0
15	Обрезка на 10%	19	15	3
16	Обрезка на 40%	22	19	5
17	Поворот на 7°	16	13	3
18	Поворот на 90°, 180°	0	0	0
19	Зеркальное отражение	32	16	2
20	Изменение цвета	8	7	0

Результаты сравнения хэш-алгоритмов продемонстрировали, что алгоритм на основе ДКП обеспечил наивысшую устойчивость к различным типам модификаций, сохранив стабильность в 15 из 20 случаев. В то же время, хэш-алгоритм по среднему показал устойчивость только в 6 случаях, а хэш на основе разности — в 7 случаях. Эти результаты свидетельствуют о том, что хэш-алгоритм на основе ДКП является наиболее эффективным инструментом для задач поиска дубликатов изображений благодаря своей высокой стойкости к модификациям. Таким образом, предлагаемый подход поиска одинаковых и похожих изображений является эффективным.

Заключение

В ходе проведенного исследования была проанализирована эффективность алгоритмов поиска изображений с использованием перцептивного хэширования. Результаты оценки времени работы алгоритмов подтвердили высокую производительность разработанного оптимизированного метода, который включает разделение хэша на подстроки, настройку серверных параметров, использование индексов и фильтра Блума. Этот подход продемонстрировал ускорение процесса поиска в три раза по сравнению с традиционным алгоритмом, основанным на вычислении расстояния Хэмминга.

Кроме того, разработанный алгоритм показал хорошие результаты в отношении устойчивости к изменениям изображений. Это позволяет надежно идентифицировать дубликаты, основываясь на сравнении расстояния Хэмминга не больше трех.

Важно отметить, что гипотеза о применении данного метода для поиска похожих изображений была успешно протестирована на примере аудиосигналов. Разработанный алгоритм продемонстрировал свою эффективность в выявлении дубликатов аудиозаписей и продемонстрировал устойчивость к множеству модификаций данных.

Таким образом, результаты исследования подтверждают возможность применения предложенных алгоритмов в задачах, связанных как с обработкой изображений, так и с анализом аудиосигналов, что открывает новые перспективы для более широкого использования технологий перцептивного хэширования в различных областях.

Библиография

1. Ромашкова О. Н., Каптерев А. И. Анализ угроз и рисков информационной безопасности в вузе // Вестник Московского городского педагогического университета. Серия: Информатика и информатизация образования. 2023. №. 1 (63). С. 37-47.
2. Турянская К. А. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса // Международный журнал гуманитарных и естественных наук. 2024. №. 2-

2 (89). С. 151-155.
3. Боярчук Д. А., Фролов К. А., Склярук В. Л. Угрозы информационной безопасности облачных технологий // Современные проблемы радиоэлектроники и телекоммуникаций. 2022. №. 5. С. 207.
4. Мустафаев А. Г., Кобзаренко Д. Н., Бучаев А. Я. Цифровая трансформация экономики: угрозы информационной безопасности // Beneficium. 2021. №. 2 (39). С. 21-26.
5. Емельянов А. А. Обеспечение информационной безопасности при использовании средств виртуализации на базе гипервизоров / /Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская. 2022. С. 232.
6. Барыбина А. З. Моделирование угроз информационной безопасности сценарным подходом // Естественно-гуманитарные исследования. 2022. №. 42 (4). С. 35-44.
7. Гринь В. С. Анализ угроз информационной безопасности и каналов утечки информации // StudNet. 2021. Т. 4. №.8. С. 1616-1620.
8. Бекмухан А., Усатова О. Оптимизация безопасности в мультисерверных веб-системах: эффективное управление рисками // Вестник КазАТК. 2024. Т. 133. №. 4. С. 296-307.
9. Фактчекинг и верификация: учебное пособие / Л.П. Шестеркина, А.В. Красавина, Е.М. Хакимова. Челябинск: Издательский центр ЮУрГУ, 2021. 64 с.
10. Алпатов А. Н. Особенности обнаружения аномалий глубокого генезиса в видеопотоке // Системная трансформация–основа устойчивого инновационного развития. 2023. С. 19.
11. Применение нейронных сетей для распознавания образов / Е. М. Павлов, А. В. Рыжов, К. С. Баланев, И. М. Крепков // Бюллетень науки и практики. 2023. Т. 9. № 12. С. 52-58. DOI 10.33619/2414-2948/97/06. EDN UURLEA.
12. Лазарев, Е. А. Применение компьютерного зрения и обработки изображений с помощью нейронных сетей / Е. А. Лазарев // Вестник науки. 2023. Т. 5. № 12-1(69). С. 412-415. EDN BVXPYI.
13. Пилькевич С. В. и др. Демонстратор программно-технического средства автоматизированного распознавания вредоносных мультимедийных объектов в сети интернет (итоги исследования) // Вестник Российского нового университета. Серия: Сложные системы: Модели, анализ и управление. Учредители: Российский новый университет. 2023. №. 2. С. 157-175.
14. Есипов Д. А. и др. 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.
15. Панчехин Н. И., Десятов А. Г., Сидоркин А. Д. Система распознавания вредоносных программ на основе представления бинарного файла в виде изображения с применением машинного обучения. 2023. Политехнический молодежный журнал. 2023. № 04, 1-10. DOI: 10.18698/2541-8009-2023-4-886.
16. Басараб М.А., Коннова Н.С. Интеллектуальные технологии на основе искусственных нейронных сетей. Москва, МГТУ им. Н.Э. Баумана, 2017, 56 с.
17. Random Forest for Malware Classification. URL: https://arxiv.org/abs/1609.07770 (accessed 20.11.2024).
18. Xu L., Zhang D., Jayasena N., Cavazos J. HADM: Hybrid Analysis for Detection of Malware. Proceedings of SAI Intelligent Systems Conference, 2018. http://doi.org/10.1007/978-3-319-56991-8_51.
19. Towards Building an Intelligent Anti-Malware System: A Deep Learning Approach using Support Vector Machine (SVM) for Malware Classification. URL: https://arxiv.org/abs/1801.00318 (accessed November 20, 2024).
20. Machine LearningBased Solution fortheDetectionof MaliciousJPEGImages [Электронный ресурс]. 2020. Режим доступа: https://ieeexplore.ieee.org/document/8967109/metrics#metrics. Дата доступа: 11.11.2024.

21. Петифорова Д. Е., Штепа К. А. Анализ использования перцептивного хеширования в процессе идентификации изображений // Информационно-телекоммуникационные технологии и математическое моделирование высокотехнологичных систем. 2021. С. 274-277.
22. Мягких П. А., Ядута А. З. Сравнение изображений с использованием перцептивных хешей // Фундаментальные и прикладные исследования в науке и образовании. 2023. С. 72-76.
23. Валишин А. А., Запривода А. В., Цухло С. С. Моделирование и сравнительный анализ эффективности перцептивных хеш-функций для поиска сегментированных изображений // Математическое моделирование и численные методы. 2024. №. 2 (42). С. 46-67.
24. Никифоров М. Б., Тарасова В. Ю. Алгоритм обнаружения визуального сходства изображений // Цифровая обработка сигналов. 2022. №. 3. С. 53-57.
25. Детков А. А. и др. Сравнительный анализ метрик векторного расстояния растровых изображений // Вестник кибернетики. 2024. Т. 23. №. 3. С. 22-30.
26. Трефилов П. А. Хранение и поиск схожих изображений в темпоральных базах данных с использованием перцептивных хэш-строк // Труды Международного симпозиума «Надежность и качество». 2020. Т. 1. С. 192-196.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в рецензируемой статье выступают алгоритмы обнаружение дублирующего контента в изображениях критической информационной инфраструктуры с использованием методов машинного обучения.
Методология исследования базируется на обобщении сведений из научных публикаций по рассматриваемой теме, применении различных методов хеширования изображений (перцептивного и классификационного хеширования), вычисление хешей с применением методов расстояния Хэмминга и косинусного сходства.
Актуальность работы авторы связывают с необходимостью противостоять потенциальным угрозам информационной безопасности в виде вредоносных изображений, содержащих вредоносный код или скрипты, фальсифицированных изображений информации и др. Для этого предлагается использовать программно-технические решения, включающие алгоритмы машинного обучения и методы анализа данных, для эффективной идентификации потенциально опасных мультимедийных объектов.
Научная новизна рецензируемого исследования, по мнению рецензента, состоит в подтверждении возможности применения предложенных алгоритмов в задачах, связанных как с обработкой изображений, так и с анализом аудиосигналов, для более широкого использования технологий перцептивного хэширования в различных областях.
Структурно в тексте выделены следующие разделы: Введение, Методы исследования, Заключение и Библиография.
В публикации проведен анализ возможностей нескольких существующих систем поиска похожих изображений, таких как Яндекс Картинки, Google Images, Duplicate Photo Finder, VisiPics, их области применения и алгоритмов.
Проведено сравнение существующих подходов к выявлению похожих изображений: сравнение значений пикселей изображений на одинаковых позициях, гистограммы изображений в виде анализа распределения яркости или цветовых характеристик изображения и формирования соответствующих гистограмм, использование свёрточных нейронных сетей, перцептивные хэши основанные на вычислении хэш-суммы

изображения, которая учитывает его содержание. В результате сравнения перцептивных хэш-алгоритмов отмечен алгоритм хэширования на основе дискретного косинусного преобразования как самый точный и устойчивый к модификациям изображений. Разработанный алгоритм продемонстрировал свою эффективность и в выявлении дубликатов аудиозаписей.

Библиографический список включает 26 источников – публикации отечественных и зарубежных ученых по теме статьи на русском и иностранном языках, а также интернет-ресурсы. На источники в тексте имеются адресные ссылки, подтверждающие наличие апелляции к оппонентам.

Из резервов улучшения публикации надо отметить, что вводная часть публикации выглядит чрезмерно объемной – авторам предлагается рассмотреть возможность выделения из Введения самостоятельного раздела в виде Обзора литературы, а также озаглавить Основную часть статьи или сформировать разделы Результаты исследования и Осуждение результатов.

Статья отражает результаты проведенного авторами исследования, соответствует направлению журнала «Национальная безопасность / nota bene», содержит элементы научной новизны и практической значимости, может вызвать интерес у читателей, рекомендуется к опубликованию после улучшения структурирования текста.