АНАЛИЗ ТЕКУЩЕГО СОСТОЯНИЯ НАУЧНЫХ ИССЛЕДОВАНИЙ В ОБЛАСТИ РОБАСТНОГО ХЭШИРОВАНИЯ ИЗОБРАЖЕНИЙ

А.В. Козачок[1], С.А. Копылов[1], Р.В. Мещеряков[2], О.О. Евсютин[2]
[1] Академия Федеральной службы охраны России, Орёл, Россия,
[2] Томский государственный университет систем управления и радиоэлектроники, Томск, Россия

Аннотация

Развитие концепции интернета вещей привело к существенному росту объемов обрабатываемой информации. Значительную часть данных, циркулирующих в глобальной сети, при этом составляет мультимедиаконтент. Зачастую эта информация содержит персональные данные конкретного пользователя или является объектом интеллектуальной собственности и авторского права. Задача по защите авторских прав владельцев цифровых изображений на протяжении последних десятилетий не теряет актуальности. Классические средства защиты информации не обеспечивают требуемый уровень защищенности данных изображений от возможных угроз ввиду специфичности формата их представления. В работе произведен сравнительный анализ существующих исследований в области робастного хэширования изображений как одного из возможных механизмов защиты авторского права для цифровых изображений. Приведена классификация методов робастного хэширования изображений, определены их достоинства и недостатки, выявлены общие особенности, присущие классам. Определены направления дальнейших исследований.

Ключевые слова: обработка изображений, целостность данных, защита авторского права, робастное хэширование, дискретное косинусное преобразование, дискретное вейвлет-преобразование, преобразование Фурье, моменты Цернике.

Цитирование: **Козачок, А.В.** Анализ текущего состояния научных исследований в области робастного хэширования изображений / А.В. Козачок, С.А. Копылов, Р.В. Мещеряков, О.О. Евсютин // Компьютерная оптика. – 2017. – Т. 41, № 5. – С. 743-755. – DOI: 10.18287/2412-6179-2017-41-5-743-755.

Введение

С каждым годом в современных информационно-вычислительных сетях в геометрической прогрессии увеличиваются объемы обрабатываемой информации. Появление интернета вещей привело к лавинообразному росту устройств, имеющих доступ к глобальной сети [1]. С ростом объемов данных и степени разнородности устройств в значительной степени возросло и количество инцидентов информационной безопасности, связанных с утечкой информации. Так, по данным аналитического центра InfoWatch, за 2016 год зарегистрировано 1556 случаев утечек конфиденциальной информации, что на 3,4 % больше, чем в 2015 году. В результате данных утечек скомпрометировано 3,1 миллиарда записей персональных данных [2]. Одним из типов данных, подвергшихся компрометации, являются изображения, содержащие конфиденциальную информацию их владельцев.

В настоящее время в системах защиты информации активно применяется криптографическое хэширование для обеспечения конфиденциальности, целостности и защиты авторских прав владельцев информации [3, 4]. Однако изображения относятся к типу данных, который допускает внесение незначительных изменений, которые не влияют на их визуальное восприятие. Данная особенность не позволяет использовать средства криптографического хэширования для решения задачи обеспечения целостности и защиты авторских прав владельцев изображений.

Одним из возможных способов решения задачи по обеспечению целостности и защиты авторских прав владельцев изображений является применение технологии робастного хэширования.

1. Назначение и особенности робастного хэширования

Процесс криптографического хэширования, или вычисления криптографической хэш-функции (collision-resistant hash-function), представляет собой функцию отображения строки бит в строку бит фиксированной длины, удовлетворяющую следующим свойствам [5]:

1) по значению функции сложно вычислить исходные данные, отображаемые в это значение;

2) для заданных исходных данных сложно вычислить другие исходные данные, отображаемые в то же значение функции;

3) сложно вычислить какую-либо пару исходных данных, отображаемых в одно и то же значение.

Современные методы криптографического хэширования разработаны для хэширования неизменяемых типов данных. В таких данных результат хэширования чувствителен к изменению хотя бы одного бита. В связи с этим незначительные изменения приводят к изменениям хэш-кода. Однако существуют типы данных, в которых небольшие изменения являются неизбежными и допустимыми. Так, например, к цифровым изображениям, данным мультимедиа (аудио- и видеоданным) и текстам могут быть применены различные преобразования, которые не изменяют восприятия семантики, но изменяют представление данных.

На рис. 1 представлено пространство изображений [6]. Пусть: I – исходное изображение; I_{ident} – множе-

ство изображений, полученных путем модификации исходного изображения I за счет применения преобразования, сохраняющего его представление: фильтрация, сжатие, геометрические искажения и др.; I_{diff} – множество, содержащее все изображения, в значительной степени отличные от I и I_{ident}.

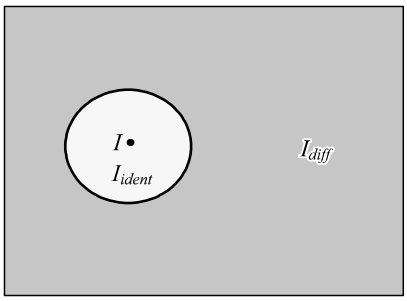

Рис. 1. Пространство изображений

В случае применения криптографической функции хэширования H_K^c к исходному изображению и изображениям из I_{ident} и I_{diff} результаты хэширования будут различными:

$$\begin{aligned} &\forall i \in I_{ident} : H_K^c(I) \neq H_K^c(i), \\ &\forall l \in I_{diff} : H_K^c(I) \neq H_K^c(l), \end{aligned} \quad (1)$$

где K – секретный ключ.

Данная особенность криптографического хэширования делает неприменимыми криптографические механизмы для аутентификации изменяемых типов данных ввиду специфики их представления. Для устранения указанного ограничения целесообразно использовать робастное хэширование, которое позволяет получить для близких по содержимому изображений близкие значения хэш-кодов [6, 7]. Задачу робастного хэширования можно формально описать следующим образом:

$$\forall i \in I_{ident} : d(H_K^r(I), H_K^r(i)) \leq \varepsilon, \quad (2)$$

$$\forall l \in I_{diff} : d(H_K^r(I), H_K^r(l)) > \varepsilon, \quad (3)$$

где ε – заданное значение функции расстояния d между хэш-кодами, K – секретный ключ.

Функция расстояния d представляет собой метрику. Наиболее распространенными метриками являются: Евклидово расстояния, расстояние Хэмминга, Манхэттенское расстояние. Выбор метрики определяется особенностями алгоритма робастного хэширования.

Процесс робастного хэширования в общем случае состоит из следующих этапов [7]:

1 этап. Извлечение характеристик – извлечение неизменяемых характеристик из входной последовательности или исходных данных. Данный шаг основан на использовании особенностей каждого типа данных. На данном этапе происходит выбор и извлечение характеристик, которые способны сохранять свойства инвариантности после осуществления различных преобразований.

2 этап. Рандомизация – однонаправленное снижение размерности, применяемое к извлеченным характеристикам, для обеспечения сжатия и необратимости преобразования выходных данных. Данный этап связан с приведением неизменяемых характеристик, полученных на предыдущем этапе, к виду, пригодному для их дальнейшей обработки. Для реализации данного этапа могут быть использованы такие преобразования, как логарифмически-полярное преобразование, криптографическое хэширование, шифрование и др. Критерии выбора и применения конкретного математического преобразования основаны на особенностях неизменяемых характеристик, полученных на первом этапе робастного хэширования. Для реализации данного этапа применяется секретный ключ K, который управляет процессом рандомизации и выполняет следующие задачи:

- аннулирование хэшей и перевод их в разряд непригодных к использованию посредством изменения секретного ключа;

- осуществление функции идентификации владельца данных, которая необходима в процессе аутентификации и проверки целостности.

3 этап. Квантование – разделение рандомизированных характеристик, полученных на предыдущем этапе, на дискретные уровни. Для реализации этапа квантования необходима предварительная оценка полученных характеристик с целью определения порогового значения (порогов квантования).

4 этап. Кодирование – присвоение каждому дискретному уровню уникальной двоичной последовательности установленной длины.

Стоит отметить, что в процессе практической реализации алгоритма робастного хэширования последовательность этапов хэширования может отличаться наличием или отсутствием одного или нескольких этапов.

Исходя из особенностей и этапов робастного хэширования, были определены требования, которым должна соответствовать робастная хэш-функция [6, 7, 11, 12, 16]:

- робастность – результаты хэширования изображений I и $\forall i \in I_{ident}$, должны удовлетворять следующему условию:

$$P(d(H_K^r(I), H_K^r(i)) \leq \varepsilon) \geq 1 - \theta_1, \quad (4)$$

при заданных ε, θ_1;

- хрупкость – результаты хэширования изображений I и $\forall l \in I_{diff}$, должны удовлетворять следующему условию:

$$P(d(H_K^r(I), H_K^r(l)) > \varepsilon) \geq 1 - \theta_2, \quad (5)$$

при заданных ε, θ_2;

- безопасность – результат хэширования не может быть вычислен без знания секретного ключа;

- случайность – невозможность вычисления пары исходных данных, генерирующей одинаковое значение хэш-кода [6]:

$$P(H_K^r(I) = \nu) \approx 2^{-q} \quad \forall I, \nu \in \{0,1\}^q, \quad (6)$$

где q – длина хэш-кода в битах;

- необратимость – исходные данные не могут быть восстановлены из значения хэш-кода.

В отличие от криптографической функции хэширования значение длины робастного хэш-кода определяется в каждом конкретном случае с учетом допустимого объема встраиваемой информации в изображение и требований по производительности, предъявляемых системами индексации и поиска.

Существующие методы робастного хэширования применяются для хэширования таких типов данных, как изображения, данные мультимедиа (аудио- и видеоданные) и текстовые данные. Наибольшее распространение данная технология получила в сфере обработки изображений.

2. Обзор методов робастного хэширования изображений

На данный момент робастное хэширование изображений является наиболее исследованной областью применения методов робастного хэширования. Прикладное применение методов робастного хэширования изображений осуществляется для решения следующих задач:

- аутентификация изображений, установление владельца и проверка целостности. Примером применения методов робастного хэширования для аутентификации изображений является технология создания цифрового водяного знака (ЦВЗ);
- индексация и поиск изображений.

Первый класс методов робастного хэширования основан на исследованиях в области аутентификации изображений. В общем виде процесс аутентификации может быть описан следующими этапами:

1) вычисление хэш-кода изображения на основе значений неизменяемых характеристик, выделенных из изображений;

2) внедрение хэш-кода в изображение с последующей отправкой или отправка хэш-кода без внедрения в изображение;

3) повторное хэширование полученного изображения на стороне приема;

4) сравнение исходного и полученного значений хэш-кода изображений.

Основная сложность в реализации на практике методов робастного хэширования изображений заключается в определении и извлечении признаков и характеристик из изображений, которые способны оставаться инвариантными в случае осуществления различных преобразований изображения и внесения в него искажений.

Одним из первых исследований в области робастного хэширования изображений было исследование 1996 года М. Шнайдера и др. [8], в котором был предложен метод аутентификации изображений на основе цифровой подписи, вычисляемой из гистограммы изображения. Достоинством данного метода является устойчивость к сжатию изображения с потерями. К недостаткам данного метода относится неспособность обеспечения требуемого уровня защиты данных в связи с тем, что содержимое изображений может быть изменено без изменения гистограммы.

В исследовании Р. Венкатесана и др. [9] робастная функция хэширования изображений основана на разработанном алгоритме хэширования с применением кода коррекции ошибок к результату разложения дискретного вейвлет-преобразования (ДВП) изображения. На первом этапе происходит вычисление вейвлет-разложения исходного изображения, каждый поддиапазон которого случайным образом покрывается прямоугольниками. На следующем этапе вычисляется значение средней величины и дисперсии статистических характеристик каждого прямоугольника, которые подвергаются квантованию по методу случайного округления (вероятностного квантования) посредством секретного ключа. На конечном этапе осуществляется декодирование полученной статистики декодером Рида–Маллера первого порядка. Длина полученного хэш-кода зависит от размера изображения. Метрика ε вычисляется посредством нормализованного расстояния Хемминга и выражается в процентном отношении. Значения метрики определяются экспериментально и могут находиться в диапазоне от 50 до 65 процентов. Результат хэширования обеспечивает устойчивость к таким преобразованиям, как поворот изображения не более чем на 2 градуса, обрезка и масштабирование не более 10 процентов изображения, удаление не более 5 строк, сжатие изображения по стандарту JPEG со степенью сжатия более 10 процентов и медианная фильтрация 4×4. Недостатком представленного алгоритма является отсутствие устойчивости к изменению контрастности и корректировки гаммы изображения.

В исследовании Е. Ченга и др. [10] в качестве робастной функции хэширования изображений выступает алгоритм создания цифровой подписи изображения. Данный алгоритм основан на низкоскоростном сжатии содержимого с потерями и ДВП. Сжатие содержимого основано на пространственно-изменяемой весовой функции, представляющей собой мультифовейную весовую функцию, имеющую сходство с фовеей биологической системы зрения человека. На первом этапе извлекаются характерные точки изображения (фовеи), представляющие собой локальные максимумы трехмерного масштабно-пространственного представления изображения. На втором этапе определяется весовая функция путем квантования значений характерных точек изображения со значениями вейвлет-коэффициентов ДВП. Полученные значения подвергаются сжатию с потерями посредством кодирования кодом Лемпеля–Зива и пространственно изменяемой весовой функции. На заключительном этапе результат сжатия и описание весовой функции подвергается асимметричному шифрованию на секретном ключе. Длина хэш-кода определяется алгоритмом криптографического шифрования. Метрика ε представляет собой нормализованную дисторсию, вычисляемую через взвешенную пространственно изменяемую норму, имеющую пороговые значения 1,15, 1,75 и 2,37. Результат хэширования представляет собой цифровую подпись изображения

и обеспечивает устойчивость к следующим преобразованиям: гауссовская фильтрация с частотой среза 0,25 Гц, внесение белого гауссовского шума с уровнем не выше 13 дБ и сжатие изображения по стандарту JPEG со степенью сжатия не более 20 процентов. Недостатком данного алгоритма является отсутствие устойчивости к подмене локальных областей изображения и независимость процесса хэширования от секретного ключа.

В исследовании А. Шваминатана и др. в [11] алгоритм создания робастной функции хэширования изображений основан на инвариантности вращения преобразования Фурье–Меллина и управляемой рандомизации. На первом этапе осуществляется предварительная обработка изображения, состоящая из низкочастотной фильтрации, понижающей дискретизации и выравнивания гистограммы изображения. Полученный результат подвергается преобразованию Фурье (ПФ), трансформирующему полученную последовательность в полярные координаты. На втором этапе полученные значения суммируются со значениями равнозначных точек изображения. Результат кругового суммирования подвергается рандомизации и кодированию на секретном ключе. На последнем этапе кодированная последовательность квантуется и декодируется трехранговым декодером Рида–Маллера. Неизменяемыми характеристиками хэширования выступают значения низкочастотных коэффициентов ПФ. Конечное значение хэш-кода равно 420 бит. Метрика ϵ определяется через нормализованное относительно длины хэш-кода расстояние Хемминга с пороговым значением 0,5. Результат хэширования обеспечивает устойчивость к сжатию изображения по стандарту JPEG со степенью сжатия не более 20 процентов, усредненной фильтрации 4×4, а также к таким геометрическим преобразованиям, как поворот не более чем на 10 градусов и обрезка не более 20 процентов изображения. Помимо этого, разработанный алгоритм способен обнаруживать изменения локальных областей изображения, которые обусловлены операцией «вырезать-вставить». Недостатком разработанного алгоритма является процесс кругового суммирования, погрешности которого порождают коллизии в конечных значениях хэш-кода.

В исследовании З. Тенга и др. [12] алгоритм робастного хэширования изображений основан на использовании неотрицательной матрицы факторизации. На первом этапе исходное изображение преобразуется к нормализированному монохромному массиву пикселей посредством изменения размера изображения, преобразования цветового пространства и низкочастотной фильтрации компоненты яркости. На втором этапе осуществляется построение вторичного изображения через перестановку по псевдослучайному закону элементов полученного массива пикселей с использованием секретного ключа. На заключительном этапе из вторичного изображения вычисляются функционально несущие коэффициенты посредством неотрицательной матрицы факторизации. Для вычисления конечного значения функции хэширования полученные коэффициенты квантуются и скремблируются на секретном ключе. Длина хэш-кода составляет 320 бит. Метрика ϵ определяется расстоянием Хемминга с установленным пороговым значением 25. Результат хэширования обеспечивает устойчивость к таким преобразованиям, как гауссовская фильтрация 3×3, внесение белого гауссовского шума с уровнем 1, 2, 3, 4 и 5 дБ, сжатие изображения по стандарту JPEG со степенью сжатия более 10 процентов, масштабирование изображения с множителем 0,5, 0,75, 0,9, 1,1, 1,5 и 2,0. Недостатком представленного алгоритма является отсутствие устойчивости к изменению цветности локальных областей изображения.

В исследовании Ю. Зао и др. [13] в качестве робастной функции хэширования изображений выступает алгоритм хэширования, основанный на использовании инвариантности характеристик моментов Цернике. Моменты Цернике представляют собой частный случай ортогональных моментов, устойчивых к вращению. На первом этапе осуществляется предварительная обработка изображения, состоящая из преобразования размера изображения, билинейной интерполяции, преобразования цветового пространства и низкочастотной фильтрации компоненты яркости изображения. На втором – вычисляются значения низкочастотных коэффициентов моментов Цернике для круга, вписанного внутрь предварительно обработанного квадратного изображения. Из полученных коэффициентов вычисляются значения величины и фазы, которые кодируются и перемешиваются посредством секретного ключа и генератора псевдослучайных чисел. Длина хэш-кода составляет 216 бит. Метрика ϵ определяется расстоянием Хемминга и имеет пороговое значение 30. Результат хэширования обеспечивает устойчивость к следующим преобразованиям: сжатие изображения по стандарту JPEG со степенью сжатия, не превышающей 20 процентов, внесение белого гауссовского шума с уровнем 1 и 2 дБ, поворот изображения не более чем на 20 градусов и гауссовская фильтрация 3×3. Недостатком данного метода является то, что значения моментов Цернике рассчитываются для вписанного в квадрат круга и не учитывают информацию, остающуюся по краям изображения. Данная особенность, в свою очередь, снижает устойчивость результата хэширования к подмене содержимого областей, оставшихся за пределами круга. Помимо этого, результат хэширования не обеспечивает устойчивости к корректировке яркости.

В исследовании Фа-Ксин Ю и др. [14] алгоритм робастного хэширования изображений основан на статистической инвариантности коэффициентов дискретного косинусного преобразования (ДКП). На первом этапе исходное изображение сегментируется на блоки установленной длины. После чего применяется ДКП к каждому из полученных блоков для выделения первых 9 коэффициентов АС. На втором этапе вычисляется статистическая инвариантность ко-

эффициентов посредством формулы оценки критерия максимального правдоподобия. Конечное значение хэш-функции формируется из полученной статистической инвариантности и значений коэффициентов АС. Длина хэш-кода составляет 36 бит. Результат хэширования обеспечивает устойчивость к следующим преобразованиям: сжатие изображения по стандарту JPEG со степенью сжатия, не превышающей 20 процентов, медианная и гауссовская фильтрация 3×3, увеличение яркости не более чем на 16 процентов, выравнивание гистограммы изображения и поворот не более чем на 10 градусов. Недостатком разработанного алгоритма является отсутствие устойчивости к подмене содержимого локальных областей изображения.

В исследовании Л. Себастьян и др. [15] схема создания робастной функции хэширования изображений основана на использовании текстур Харалик и усовершенствованных локальных двоичных шаблонов совместно с моментами Цернике. Первый этап хэширования состоит из предварительной обработки исходного изображения, включающей билинейную интерполяцию и конвертирование изображения. Далее вычисляются неизменяемые характеристики изображения, в качестве которых выступают локальные характеристики изображения, представленные текстурами Харалик, и глобальные – представленные моментами Цернике, извлеченные из компонент яркости и цветности изображения. Для извлечения локальных характеристик обработанное изображение разделяется на блоки и из каждого блока выделяются 14 характеристик текстур Харалик, также вычисляются значения гистограммы усовершенствованных локальных двоичных шаблонов. Полученные значения подвергаются рандомизации и кодированию на секретном ключе. Для извлечения глобальных характеристик исходное изображение конвертируется и из обоих изображений вычисляются моменты Цернике. Полученные значения моментов Цернике рандомизируются и кодируются на секретном ключе. Конечное значение хэш-кода вычисляется посредством рандомизации и кодирования на секретном ключе хэшей локальных и глобальных характеристик. Длина хэш-кода определяется длиной секретного ключа, а также глобальными и локальными параметрами изображения. Результат хэширования обеспечивает устойчивость к таким преобразованиям, как сжатие изображения по стандарту JPEG со степенью сжатия более 15 процентов, внесение белого гауссовского шума с дисперсией не более 0,005, корректировка яркости не более чем на 10 процентов и контрастности изображения не более чем на 20 процентов, а также к таким геометрическим преобразованиям, как масштабирование с множителем от 0,5 до 1,5, поворот не более чем на 1 градус и обрезка не более 10 процентов изображения. Кроме того, рассмотренный алгоритм обеспечивает устойчивость к внесению изменений в содержимое локальных областей изображения.

В исследовании С. Дипа и А. Нагайоти [16] в процессе вычисления значения робастной функции хэширования используются моменты Цернике совместно со свойствами гистограммы изображения. Моменты Цернике, как и в исследовании [15], извлекаются из глобальных характеристик изображения, представленных компонентами яркости и цветности. Локальные характеристики представляют собой информацию о положении и текстурах областей изображения с повышенной яркостью совместно с гистограммой изображения. На первом этапе преобразуется размер и цветовое пространство исходного изображения. Из компонент яркости и цветности вычисляются моменты Цернике, которые кодируются на секретном ключе. На втором этапе по значениям компоненты яркости из обработанного изображения извлекаются характеристики областей изображения с повышенной яркостью, которые кодируются на секретном ключе. На третьем этапе из преобразованного изображения вычисляется значение гистограммы, которое подвергается перестановке по псевдослучайному закону и кодированию на секретном ключе. Конечное значение функции хэширования формируется путем кодирования на секретном ключе полученных кодовых последовательностей. Длина хэш-кода зависит от секретного ключа, параметров яркости и гистограммы изображения. Пороговое значение метрики ϵ равно 7. Результат хэширования обеспечивает устойчивость к таким преобразованиям, как сжатие изображения по стандарту JPEG со степенью сжатия не более 30 процентов, внесение белого гауссовского шума с дисперсией не более 0,01, масштабирование с множителем 0,5 и поворот не более чем на 5 градусов. Кроме того, предложенный алгоритм хэширования, как и алгоритм хэширования в исследовании [15], обеспечивает устойчивость к внесению изменений в локальные области изображения.

В исследовании Д. Оюянга и др. [17] в качестве робастной функции хэширования изображений выступает алгоритм, основанный на сочетании кватерниона дискретного ПФ и логарифмически-полярного преобразования. Исходное изображение подвергается предварительной обработке, состоящей из изменения масштаба, медианной фильтрации и вписывания в круг полученного изображения. Обработанное изображение подвергается логарифмически полярному преобразованию. Из полученных значений вычисляются значения низкочастотных коэффициентов кватерниона дискретного ПФ. Полученные значения коэффициентов подвергаются преобразованию Арнольда, скремблированию, управляемому секретным ключом, и кодированию на секретном ключе для вычисления хэш-кода. Конечное значение хэш-кода составляет 224 бита. Метрика ϵ определяется нормализированным относительно размера низкочастотных коэффициентов расстоянием Хемминга с пороговым значением 0,2. Результат хэширования обеспечивает устойчивость к таким преобразованиям, как сжатие изображения по стандарту JPEG со степенью сжатия

от 10 до 90 процентов, усредненная и медианная фильтрация 3×3, 5×5 и поворот на углы 45 и 210 градусов. Недостатком разработанного метода является отсутствие устойчивости к внесению изменений в локальные области изображения.

Частным случаем применения методов робастного хэширования изображений для аутентификации является создание ЦВЗ-изображения, которое представляет собой видимый или невидимый знак (информационную последовательность), встраиваемый в изображение. Он может содержать в себе информацию о владельце изображения (для защиты авторских прав), о самом изображении (для обнаружения подмены данных изображения, проверки подлинности) или другую информацию (для вставки в изображение).

ЦВЗ делятся на три группы [18]:

- робастный водяной знак (обеспечивает устойчивость к внесению искажений и осуществлению различных преобразований);
- хрупкий водяной знак (разрушается путем внесения искажений и осуществлением различных преобразований);
- полухрупкий водяной знак (разрушается отдельным типом искажений или преобразований, однако обеспечивает устойчивость к определенным типам искажений или преобразований).

Особенность процесса создания ЦВЗ заключается в наличии этапа обнаружения и извлечения данного знака. Схемы извлечения водяного знака делятся на две группы: требующие для извлечения исходное изображение и не зависящие от исходного изображения алгоритмы.

В случае применения методов робастного хэширования для создания ЦВЗ-изображений процесс создания ЦВЗ-изображений отличается от процесса робастного хэширования изображений для аутентификации данных наличием этапа встраивания водяного знака. Данный факт обуславливает наличие этапов обнаружения и извлечения ЦВЗ на стороне приема.

Примером применения методов робастного хэширования для создания ЦВЗ-изображений является исследование Дж. Фридрича и М. Гольяна [19], в котором схема создания робастного ЦВЗ-изображения основана на свойствах инвариантности низкочастотных коэффициентов ДКП. На первом этапе из исходного изображения извлекаются низкочастотные коэффициенты DC посредством ДКП. На втором этапе путем синтезирования полученных результатов с Гауссовой псевдослучайной последовательностью генерируется конечное значение хэш-функции. Синтез осуществляется путем побитового суммирования равномерно распределенных псевдослучайных гауссовских последовательностей, сгенерированных генератором псевдослучайных чисел, секретного ключа и отдельных цепочек бит, извлеченных из значений низкочастотных коэффициентов. Полученная последовательность представляет собой ЦВЗ и может быть встроена как в изображение, так и в видеоданные. Длина хэш-кода равна 50 бит. Результат хэширования обеспечивает устойчивость к таким преобразованиям, как сжатие изображения по стандарту JPEG со степенью сжатия 15 процентов, корректировка контрастности не более чем на 50 процентов, корректировка яркости не более чем на 25 процентов, медианная фильтрация 3×3 и выравнивание гистограммы изображения.

В исследовании К. Ли и К. Зенга [20] в качестве робастной функции хэширования выступает алгоритм создания невидимого ЦВЗ изображений, основанный на стандарте сжатия изображения JPEG2000. ЦВЗ представляет собой информацию о владельце данных или другую метаинформацию. ЦВЗ внедряется в исходное изображение в процессе сжатия изображения по стандарту JPEG2000. На первом этапе из исходного изображения вычисляются вейвлет-коэффициенты ДВП. На втором – извлеченные коэффициенты и ЦВЗ подвергаются адаптивному сжатию. Полученная в процессе сжатия изображения по стандарту JPEG2000 последовательность встраивается в поддиапазоны вейвлет-коэффициентов средних частот промежуточного разложения ДВП исходного изображения. Использование стандарта сжатия JPEG2000 позволяет внедрять ЦВЗ в исходное изображение и в последующем, используя данный стандарт, извлекать его из подписанного изображения. Извлечение ЦВЗ происходит в порядке, обратном его встраиванию. Длина хэш-кода зависит от допустимой емкости встраивания информации в исходное изображение. Результат хэширования обеспечивает устойчивость к следующим преобразованиям: сжатие изображения по стандарту JPEG со степенью сжатия не более 40 процентов, сжатие по стандарту JPEG2000 со скоростью сжатия не более 0,5 бит/пиксель и медианная фильтрация 3×3.

В исследовании С. Лу и др. [21] схема создания невидимого ЦВЗ изображений основана на использовании особенностей масштабно-пространственной фильтрации. Масштабно-пространственная фильтрация предназначена для формирования сетки изображения, в которую осуществляется встраивание ЦВЗ. Исходное изображение подвергается гауссовской фильтрации для определения частотных компонент. Из полученных компонент формируются характерные точки изображения через процедуру определения локального максимума. Сетка изображения формируется посредством триангуляции Делоне (мозаика Делоне) из полученного набора характерных точек. На втором этапе происходит создание невидимого ЦВЗ-изображения. За счет применения аффинного преобразования из полученной сетки формируется нормализованная сетка изображения. Нормализованная сетка разделяется на блоки, и из каждого блока посредством ДКП извлекаются коэффициенты АС. Из полученных значений коэффициентов АС формируется конечное значение функции хэширования. Встраивание результата хэширования осуществляется в нормализованную сетку при помощи функции относительной спектральной световой эффективности шума. Полученное значение накладывается на исходное изображение. Извлечение ЦВЗ производится в обратной последовательности.

Для определения наличия ЦВЗ в изображении разработаны этапы двухэтапного извлечения характеристик и проверки ошибок первого рода. Длина хэш-кода составляет 128 бит. Разработан собственный алгоритм вычисления метрики ε, основанный на коэффициенте битовых ошибок и распределении Бернулли. Пороговое значение метрики составляет 0,375. Результат хэширования обеспечивает устойчивость к таким преобразованиям, как сжатие изображения по стандарту JPEG со степенью сжатия не более 80 процентов, медианная и гауссовская фильтрация 2×2, 3×3, изменение резкости 3×3 и яркости не более чем на 30 процентов, обрезка не более 20 процентов изображения, масштабирование с множителем 0,5, 1,1, 1,5, 2,0 и удаление не более 17 строк. Кроме того, представленная схема обеспечивает устойчивость к подмене водяного знака. Основной недостаток рассмотренного метода состоит в высокой сложности формирования сетки изображения.

В исследовании Ю. Мингуиллон и др. [22] для создания видимого ЦВЗ изображений в качестве робастной функции хэширования используется стандарт сжатия изображения JPEG2000. Исходное изображение подвергается сжатию и декомпрессии сжатого изображения по алгоритму JPEG2000. Полученное изображение сравнивается с исходным для определения битов, имеющих отличные значения. Данная информация определяет место вставки ЦВЗ. ЦВЗ содержит информацию о компоненте яркости изображения. Информационная последовательность ЦВЗ подвергается кодированию с применением кода коррекции ошибок – код Хэмминга (31, 26) и шифрованию на секретном ключе по алгоритму DES в режиме «обратной связи по выходу». На этапе вставки ЦВЗ происходит замена битов, имеющих отличные друг от друга значения, вычисленным ЦВЗ. Длина хэш-кода равна 434 бит. Пороговое значение метрики є равно 0,8. Результат хэширования обеспечивает устойчивость к следующим преобразованиям: медианная и гауссовская фильтрация 2×2, 3×3, сжатие изображения по стандарту JPEG со степенью сжатия не более 80 процентов, сжатие изображения по стандарту JPEG2000 со скоростью сжатия не более 2 бит / пиксель, обрезка на более 25 процентов изображения и удаление одновременно не более 1 строки и 1 столбца. Недостатком разработанной схемы является отсутствие устойчивости к внесению изменений в локальные области изображения.

В исследовании Р. Ридзона и Д. Левиски [23] в качестве функции хэширования в процессе создания ЦВЗ-изображений выступает алгоритм, основанный на дискретном ПФ в сочетании с логарифмически-полярным преобразованием. Исходное изображение подвергается дискретному ПФ для извлечения коэффициентов преобразования (спектра сигнала). Данные коэффициенты определяют место встраивания ЦВЗ. Для формирования ЦВЗ осуществляется хэширование данных по алгоритму RIPEMD-160 с использованием секретного ключа и последующей перестановкой по псевдослучайному закону. В ходе внедрения ЦВЗ в полученные на первом этапе коэффициенты преобразования полученные данные подвергаются обратному логарифмически-полярному преобразованию и обратному дискретному ПФ. Длина хэш-кода составляет 160 бит. Результат хэширования обеспечивает устойчивость к следующим преобразованиям: поворот не более 30 градусов, масштабирование с множителем 0,5, сжатие изображения по стандарту JPEG2000 со скоростью сжатия, не превышающей 1 бит / пиксель, внесение белого гауссовского шума с дисперсией не более 0,001, увеличение яркости не более чем на 30 процентов и обрезка не более 25 процентов изображения. К недостаткам данного алгоритма относится применимость его только к изображениям в оттенках серого.

В исследовании В. Китановски и др. [24] алгоритм создания невидимого ЦВЗ изображений основан на объединении схемы создания полухрупкого ЦВЗ и робастного хэширования. Процесс создания скрытого ЦВЗ состоит из двух этапов. На первом этапе осуществляется робастное хэширование изображения, состоящее из разделения изображения на блоки, вычисления значения коэффициентов DC ДКП, определения разницы коэффициентов DC между блоками и двух раундовом кодировании поученных значений с использованием секретного ключа. Результат хэширования представляет ЦВЗ. На втором этапе происходит встраивание вычисленного ЦВЗ в исходное изображение. Встраивание ЦВЗ осуществляется в низкочастотные компоненты блоков ДКП, которые промодулированы квантованными импульсами. Пороговое значение метрики разработанного алгоритма хэширования ε выбирается экспериментально из следующих значений: 0,15, 0,2 и 0,25. Результат хэширования обеспечивает устойчивость к таким преобразованиям, как сжатие изображения по стандарту JPEG со степенью сжатия не более 80 процентов, усредненная и медианная фильтрация 3×3, внесение белого гауссовского шума и корректировка яркости и контрастности изображения не более чем на 15 процентов. Недостатком рассмотренного алгоритма является возможность ошибок в процессе извлечения ЦВЗ из отдельных изображений.

Проведенный анализ методов робастного хэширования изображений позволяет сделать вывод о том, что рассмотренные алгоритмы и схемы могут быть применены не только для аутентификации изображений, но также и для индексации и поиска с целью повышения надежности хранимых данных и сокращения времени поиска.

В исследовании К. Винтера и др. [25] реализовано две стратегии индексации изображений методами робастного хэширования. Исходное цветное изображение преобразуется в серое, при этом информация о яркости пикселей сохраняется. Полученное серое изображение разделяется на блоки и вычисляется среднее значение яркости всех блоков. Конечное значение функции хэширования рассчи-

тывается из полученного значения яркости. Результат хэширования обеспечивает устойчивость к таким преобразованиям изображения, как сжатие изображения по стандарту JPEG со степенью сжатия 10, 40 и 90 процентов, гауссовская фильтрация 3×3, внесение белого гауссовского шума с дисперсией не более 0,01, увеличение контрастности не более чем на 20 процентов и корректировка цветности изображения. В альтернативном варианте для преобразования метрического пространства изображения к хэмминговому пространству и генерации конечного значения хэш-функции к полученному результату применяется одна из двух предложенных стратегий. Первая основана на применении метрического дерева (VP-дерева), являющегося разновидностью дерева двоичного разбиения пространства, к полученному результату хэширования. Из значений, удовлетворяющих установленным критериям отбора VP-дерева, формируется конечное значение хэш-функции. Вторая стратегия основана на использовании локально-чувствительного хэширования, которое представляет собой хэширование с большой вероятностью коллизий. Длина хэш-кода равна 256 бит. Пороговое значение метрики ε обеих стратегий равно 32. Применение второй стратегии в системе индексации в значительной степени уступает первой по времени формирования системы индексов, однако в случае применения обеих стратегий для поиска изображений, вторая система выдает результат поиска значительно быстрее и точнее первой. Кроме того, данные методы могут быть применены для индексации и поиска в видеоданных.

В исследовании Я. Янга и др. [26] для индексации изображений предлагается использовать дискретное робастное хэширование. Процесс создания системы индексации состоит из двух этапов: первый этап предполагает использование дискретного двоичного кодирования, а второй – дискретного робастного хэширования. На первом этапе создается представление исходного изображения за счет применения к исходному изображению следующих операций: хэширование по методу главных компонент и спектральное хэширование. Посредством эвристической бинаризации данное представление преобразуется в вид двоичных кодов (преобразование цветного изображения в монохромное, основанное на эвристических методах). На втором этапе к полученному значению двоичных кодов применяется разработанный алгоритм дискретного робастного хэширования с последующей оптимизацией полученных результатов в вид, необходимый для работы системы индексации. Длина хэш-кода может варьироваться от 32 до 128 бит в зависимости от требуемого уровня производительности системы индексации.

Результат робастного хэширования может быть передан двумя способами:

– совместно с изображением (путем внедрения хэша в изображение),

– отдельно от изображения.

В первом случае процесс внедрения хэша реализован в работах [8, 10] в виде цифровой подписи изображения, а в работах [19–24] – в виде скрытого/видимого ЦВЗ.

В работах [9, 11–17, 25, 26] встраивание хэша в изображение не производится. В работах [25, 26] создается база индексов изображений, содержащая выработанные значения робастных хэшей для последующего поиска по ней.

3. Обсуждение результатов

Проведенный анализ исследований в области робастного хэширования изображений позволяет разделить рассмотренные методы, в зависимости от используемых математических преобразований в процессе хэширования, на следующие группы [27]:

- методы, основанные на ДВП [9, 10, 20, 22];
- методы, основанные на ДКП [14, 19, 21, 24];
- методы, основанные на ПФ [11, 17, 23];
- методы, основанные на моментах Цернике [13, 15, 16];
- методы, основанные на других математических преобразованиях [12, 25, 26].

Результаты проведенного анализа методов робастного хэширования изображений представлены в табл. 1.

Табл. 1. Преобразования, применяемые для извлечения неизменяемых характеристик

Исследование	**Математическое преобразование**	**Неизменяемые характеристики**
Р. Венкатесан [9]	ДВП, кодирование кодом Рида–Маллера	Статистика поддиапазонов вейвлет-разложения
Е. Ченг [10]	ДВП, кодирование кодом Лемпеля–Зива	Коэффициенты вейвлет-преобразования
А. Швами натан [11]	ПФ, кодирование кодом Рида–Маллера	Низкочастотные коэффициенты
З. Тенг [12]	Неотрицательная матрица факторизации	Коэффициенты неотрицательной матрицы факторизации компоненты яркости
Ю. Зао [13]	Моменты Цернике	Коэффициенты моментов Цернике компоненты яркости
Фа-Ксин Ю [14]	ДКП, критерий максимального правдоподобия	Коэффициенты АС
Л. Себасть яна [15]	Моменты Цернике, текстуры Харалик	Коэффициенты моментов Цернике компонента яркости и цветности
С. Дип А. Нагайо ти [16]	Моменты Цернике	Коэффициенты моментов Цернике компонента яркости и цветности

Исследование	Математическое преобразование	Неизменяемые характеристики
Д. Оюянг [17]	ПФ, логарифмически-полярное преобразование, преобразование Арнольда	Низкочастотные коэффициенты кватерниона ДПФ
Дж. Фридрич М. Гольян [19]	ДКП	Коэффициенты DC
К. Ли К. Зенг [20]	ДВП, MQ-кодер	Коэффициенты вейвлет-преобразования
С. Лу [21]	ДКП, триангуляция Делоне	Коэффициенты AC
Ю. Мингуиллон [22]	ДВП, код Хэмминга (31,26), шифрование DES, MQ-кодер	Коэффициенты вейвлет-преобразования компоненты яркости
Р. Ридзон Д. Левиски [23]	ДПФ, логарифмически-полярное преобразование, хэширование RIPEMD-160	Низкочастотные коэффициенты
В. Китановски [24]	ДКП, модуляция квантованными импульсами	Коэффициенты DC
К. Винтер [25]	Двоичное разбиение пространства, локально чувствительное хэширование	Значения яркости блоков

Исходя из анализа полученных результатов, можно сделать вывод, что в большинстве исследований в качестве неизменяемой характеристики процесса хэширования выступает компонента яркости изображения, которая не зависит от вида математического преобразования, используемого в процессе хэширования.

Данные о длине хэш-кода, а также параметрах функции расстояния d и соответствующего ей порогового значения ε приведены в табл. 2.

Табл. 2. Длина хэш-кода и параметры метрик

Исследование	Длина хэш-кода	Параметры метрики	Пороговое значение метрики
[9]	Определяется размером изображения	Нормализованное расстояние Хемминга	0,5–0,65
[10]	Определяется алгоритмом шифрования	Взвешенная пространственно изменяемая норма	1,15, 1,75, 2,37
[11]	420 бит	Нормализованное расстояние Хемминга	0,5
[12]	320 бит	Расстояние Хемминга	25
[13]	216 бит	Расстояние Хемминга	30
[14]	36 бит	Параметры метрики не определены	
[15]	Определяется длиной секретного ключа и параметрами изображения	Параметры метрики не определены	
[16]	Определяется длиной секретного ключа и параметрами изображения	Алгоритм вычисления метрики не указан	7
[17]	224 бита	Нормализованное расстояние Хемминга (относительно размера низкочастотных коэффициентов)	0,2
[19]	50 бит	Параметры метрики не определены	
[20]	Определяется допустимой емкостью встраивания информации в изображение	Параметры метрики не определены	
[21]	128 бит	Алгоритм, основанный на коэффициенте битовых ошибок и распределении Бернулли	0,375
[22]	434 бит	Алгоритм вычисления метрики не указан	0,8
[23]	160 бит	Параметры метрики не определены	
[24]	Длина хэш-кода и алгоритм вычисления метрики не указаны		0,15, 0,2, 0,25
[25]	256 бит	Алгоритм вычисления метрики не указан	32
[26]	От 32 до 128 бит (в зависимости от производительности системы индексации)	Параметры метрики не определены	

В табл. 3 приведена сравнительная оценка устойчивости функций хэширования к различным преобразованиям, применяемым к изображениям (* – значения величины дисперсии белого гауссовского шума представлены в параграфе 2 при рассмотрении соответствующих работ).

Результаты, полученные на основе анализа устойчивости методов и алгоритмов робастного хэширования изображений к различным видам преобразований, позволяют утверждать, что ни один из рассмотренных методов и алгоритмов не обеспечивает в полной мере защиту данных изображения от различного рода преобразований. Алгоритмы хэширования в исследованиях [15] и [21] обеспечивают устойчивость к большему числу преобразований.

Заключение

Проведенный сравнительный анализ методов робастного хэширования изображений показал, что рассмотренные методы хэширования имеют ограничения и не могут в полной мере обеспечить защиту изображений от нарушений авторских прав.

В связи с этим разработка новых алгоритмов робастного хэширования изображений является актуальной задачей. Одним из возможных вариантов синтеза такого алгоритма может быть композиция отдельных этапов алгоритмов хэширования в исследованиях [15], [21], [22], [25], которая, предположительно, позволит обеспечить устойчивость результата хэширования к наибольшему числу преобразований. Возможность такой реализации основана на наличии общей неизменяемой характеристики в виде компоненты яркости. Практическое подтверждение данного тезиса является направлением дальнейших исследований.

Табл. 3. Устойчивость результата хэширования к различным преобразованиям

Тип преобразования	**Исследование**															
	[9]	**[10]**	**[11]**	**[12]**	**[13]**	**[14]**	**[15]**	**[16]**	**[17]**	**[19]**	**[20]**	**[21]**	**[22]**	**[23]**	**[24]**	**[25]**
Поворот (%)	≤2	-	≤10	-	≤20	≤10	≤1	≤5	45, 210	-	-	-	-	≤30	-	-
Обрезка (%)	≤10	-	≤20	-	-	-	≤10	-	-	-	-	≤20	≤25	≤25	-	-
Масштабирование (%)	≤10	-	-	≤2,0	-	-	≤1,5	≤0,5	-	-	-	≤2,0	-	0,5	-	-
Удаление строк	≤5	-	-	-	-	-	-	-	-	-	-	≤17	≤1	-	-	-
Сжатие по стандарту JPEG (%)	≤10	≤20	≤20	≤10	≤20	≤20	≤15	≤30	10-90	15	≤40	≤80	≤80	-	≤80	10, 40, 90
Сжатие по стандарту JPEG2000 (%)	-	-	-	-	-	-	-	-	-	-	≤0,5	-	≤2,0	≤1,0	-	-
Медианная фильтрация	4×4	-	-	-	-	3×3	-	-	3×3 5×5	3×3	5×5	2×2 3×3	2×2 3×3	-	3×3	-
Гауссовская фильтрация	-	+	-	3×3	3×3	3×3	-	-	-	-	-	2×2 3×3	2×2 3×3	-	-	3×3
Внесение белого гауссовского шума (дБ)	-	≤13	-	≤5	≤2	-	+(*)	+(*)	-	-	-	-	-	+(*)	+(*)	+(*)
Усредненная фильтрация	-	-	4×4	-	-	-	-	-	3×3	-	-	-	-	-	3×3	-
Корректировка яркости (%)	-	-	-	-	-	≤16	≤10	-	-	≤25	-	≤30	-	≤30	≤15	-
Корректировка контрастности (%)	-	-	-	-	-	-	≤20	-	-	≤50	-	-	-	-	≤15	≤20
Выравнивание гистограммы	-	-	-	-	-	+	-	-	-	+	-	-	-	-	-	+
Подмена локальных областей изображения	-	-	+	-	-	-	+	+	-	-	-	+	-	-	-	-
Зависимость процесса хэширования от секретного ключа	+	-	+	+	+	-	+	+	+	+	-	+	+	+	+	+

Благодарности

Данная работа выполнена при поддержке Министерства образования и науки Российской Федерации в рамках проектной части государственного задания ТУСУР на 2017–2019 гг. (проект № 2.3583.2017/4.6).

Литература

1. **Weber, R.H.** Internet of Things – New security and privacy challenges / R.H. Weber // Computer Law & Security Review. – 2010. – Vol. 26, Issue 1. – P. 23-30. – DOI: 10.1016/j.clsr.2009.11.008.
2. Глобальное исследование утечек конфиденциальной информации в 2016 году // InfoWatch. – 2017.
3. **Chaudhuri, A.** Internet of things data protection and privacy in the era of the General Data Protection Regulation / A. Chaudhuri // Journal of Data Protection & Privacy. – 2016. – Vol. 1, No. 1. – P. 64-75.
4. **Kougianos, E.** Design of a high-performance system for secure image communication in the internet of things / E. Kougianos, S.P. Mohanty, G. Coelho, U. Albalawi, P. Sundaravadivel // IEEE Access. – 2016. – Vol. 4. – P. 1222-1242. – DOI: 10.1109/ACCESS.2016.2542800.
5. **ГОСТ Р 34.11-2012.** Информационная технология. Криптографическая защита информации. Функция хэширования. – Введ. 2012-08-07. – М.: Стандартинформ, 2012. – 34 с.
6. **Hsu, C.Y.** Geometric distortion-resilient image hashing scheme and its applications on copy detection authentication / C.Y. Hsu, C.S. Lu // Multimedia Systems. – 2005. – Vol. 11, Issue 2. – P. 159-173. – DOI: 10.1007/s00530-005-0199-y.
7. **Chen, B.** Robust image hash functions using higher order spectra : A Thesis submitted in fulfilment of the requirements for the Degree of Doctor of Philosophy / B. Chen. – London: Queensland University of Technology, 2012. – P. 159.
8. **Schneider, M.** A robust content based digital signature for image authentication / M. Schneider, S-F. Chang // Proceedings of the 3rd IEEE International Conference on Image Processing. – 1996. – Vol. 3. – P. 227-230. – DOI: 10.1109/ICIP.1996.560425.
9. **Venkatesan, R.** Robust image hashing / R. Venkatesan, S. Koon, M. Jakubowski, P. Moulin // Proceedings of the 2000 IEEE International Conference on Image Processing. – 2000. – Vol. 3. – P. 664-666. – DOI: 10.1109/ICIP.2000.899541.
10. **Chang, E-C.** Robust image authentication using content based compression / E-C. Chang, M.S. Kankanhalli, X. Guan, Z. Huang, Y. Wu // Multimedia Systems. – 2003. – Vol. 9, Issue 2. – P. 121-130. – DOI: 10.1007/s00530-003-0083-6.
11. **Swaminathan, A.** Robust and secure hashing for images / A. Swaminathan, Y. Mao, M. Wu // IEEE Transactions on Information Forensics and Security. – 2006. – Vol. 1, Issue 2. – P. 215-230. – DOI: 10.1109/TIFS.2006.873601.
12. **Tang, Z.** Robust image hashing for tamper detection using non-negative matrix factorization / Z. Tang, S. Wang, X. Zhang, W. Wei, S. Su // Journal of Ubiquitous Convergence and Technology. – 2008. – Vol. 2, No. 1. – P. 18-26.

13. **Zhao, Y.** A robust image hashing method based on Zernike moments / Y. Zhao, S. Wang, G. Feng, Z. Tang // Journal of Computational Information Systems. – 2010. – Vol. 6, Issue 3. – P. 717-725.
14. **Yu, F.-X.** Robust image hashing based on statistical invariance of DCT coefficients / F.-X. Yu, Y.-Q. Lei, Y.-G. Wang // Journal of Information Hiding and Multimedia Signal Processing. – 2010. – Vol. 1, No. 4. – P. 286-291.
15. **Sebastian, L.S.** Image authentication by content preserving robust image hashing using local and global features / L.S. Sebastian, A. Varghese, T. Manesh // Procedia Computer Science. – 2015. – Vol. 46. – P. 1554-1560. – DOI: 10.1016/j.procs.2015.02.081.
16. **Deepa, S.** A secure hashing scheme for image authentication using Zernike moment and local features with histogram features / S. Deepa, A. Nagajothi // American International Journal of Research in Science, Technology, Engineering & Mathematics. – 2014. – Vol. 5, Issue 2. – P. 190-195.
17. **Ouyang, J.** Robust hashing for image authentication using quaternion discrete Fourier transform and log-polar transform / J. Ouyang, G. Coatrieux, H. Shu // Digital Signal Processing. – 2015. – Vol. 41, Issue C. – P. 98-109. – DOI: 10.1016/j.dsp.2015.03.006.
18. **Woo, Ch.-S.** Digital image watermarking methods for copyright protection and authentication : Thesis submitted in accordance with the regulations for Degree of Doctor of Philosophy / Ch.-S. Woo. – London: Queensland University of Technology, 2007. – 223 p.
19. **Fridrich, J.** Robust hash functions for digital watermarking / J. Fridrich, M. Goljan // Proceedings of the International Conference on Information Technology: Coding and Computing. – 2000. – P. 178-183. – DOI: 10.1109/ITCC.2000.844203.
20. **Li, K.** Reliable adaptive watermarking scheme integrated with JPEG2000 / K. Li, X. Zhang // Proceedings of the 3rd International Sympososium on Image and Signal Processing and Analysis. – 2003. – P. 117-122. – DOI: 10.1109/ISPA.2003.1296879.
21. **Lu, C.S.** Robust hash-based image watermarking with resistance to geometric distortions and watermark-estimation attack / C.S. Lu, S.W. Sun, P.C. Chang // Proceedings of SPIE. – 2005. – Vol. 5681. – P. 147-163. – DOI: 10.1117/12.586637.
22. **Minguillon, J.** A robust watermarking scheme based on the JPEG2000 standard / J. Minguillon, J. Herrera-Joancomarti, D. Megias // Journal of Electronic Imaging. – 2005. – Vol. 14. – P. 681-684. – DOI: 10.1117/1.1988334.
23. **Ridzon, R.** Robust digital watermarking based on the log-polar mapping / R. Ridzon, D. Levicky // Radioengineering. – 2007. – Vol. 16, No. 4. – P. 76-81.
24. **Kitanovski, V.** Combined hashing/watermarking method for image authentication / V. Kitanovski, D. Taskovski, S. Bogdanova // International Journal of Computer, Electrical, Automation, Control and Information Engineering. – 2007. – Vol. 1, No. 6. – P. 575-581.
25. **Winter, C.** Fast indexing strategies for robust image hashes / C. Winter, M. Steinebach, Y. Yannikos // Digital Investigation. – 2014. – Vol. 11, Supplement 1. – P. S27-S35. – DOI: 10.1016/j.diin.2014.03.004.
26. **Yang, Y.** Robust discrete spectral hashing for large-scale image semantic indexing / Y. Yang, F. Shen, H. Shen, H. Li, X. Li // IEEE Transactions on Big Data. – 2015. – Vol. 1, Issue 4. – P. 162-171. – DOI: 10.1109/TBDATA.2016.2516024.
27. **Козачок, А.В.** Сравнительный анализ методов робастного хэширования изображений / А.В. Козачок, С.А. Копылов // Вопросы технических наук: новые подходы в решении актуальных проблем. – 2016. – Вып. III. – С. 24-27.

Сведения об авторах

Козачок Александр Васильевич, 1988 года рождения, в 2010 году окончил Академию ФСО России по специальности «Информационная безопасность телекоммуникационных систем», в 2012 году защитил диссертацию по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность», является сотрудником Академии ФСО России. Область научных интересов: информационная безопасность, защита от несанкционированного доступа, математическая криптография, теоретические проблемы информатики. E-mail: *a.kozachok@academ.msk.rsnet.ru* .

Копылов Сергей Александрович, 1988 года рождения, в 2010 году окончил Академию ФСО России по специальности «Информационная безопасность телекоммуникационных систем», является сотрудником Академии ФСО России. Область научных интересов: информационная безопасность, защита от несанкционированного доступа, обработка изображений. E-mail: *gremlin.kop@mail.ru* .

Мещеряков Роман Валерьевич, 1974 года рождения, доктор технических наук, профессор, проректор ТУСУР по научной работе и инновациям. В 1997 году окончил Алтайский государственный технический университет им. И. И. Ползунова по специальности «Информационно-измерительная техника и технологии». Кандидат технических наук (2000 год), доктор технических наук (2011 год). Область научных интересов: обработка, анализ, синтез речевого сигнала и текста, системный анализ, информационная безопасность, математическое моделирование. E-mail: *mrv@tusur.ru* .

Евсютин Олег Олегович, 1987 года рождения, в 2009 году с отличием окончил Томский государственный университет систем управления и радиоэлектроники (ТУСУР) по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем». Кандидат технических наук (2012 год), работает доцентом кафедры комплексной информационной безопасности электронно-вычислительных систем ТУСУР. Область научных интересов: информационная безопасность, обработка цифровых изображений, приложения клеточных автоматов. E-mail: *eoo@keva.tusur.ru* .

ГРНТИ: 81.93.29
Поступила в редакцию 11 мая 2017 г. Окончательный вариант – 16 августа 2017 г.

REVIEW OF THE CURRENT METHODS FOR ROBUST IMAGE HASHING

A.V. Kozachok[1], S.A. Kopylov[1], R.V. Meshcheryakov[2], O.O. Evsutin[2]
[1] Academy of the Federal Guard Service, Oryol, Russia,
[2] Tomsk State University of Control Systems and Radioelectronics, Tomsk, Russia

Abstract

The development of an *Internet of things* concept has led to an essential increase in the amount of data processed via the Internet. Multimedia data constitute a significant proportion of this information. This type of data often contains user's personal information or copyright protected data. The issue of copyright protection of digital imagery has remained topical for the last decades. Traditional information protection tools cannot provide the required level of image protection from possible threats due to specific features of format representation. This article contains a comparative analysis of published research papers concerned with the robust image hashing as one of possible methods of copyright protection of digital imagery. It also includes a classification of robust image hashing methods, discussing their advantages and drawbacks, and their major characteristics. At the end of the article some directions of further research are outlined.

Keywords: image processing, data integrity, copyright protection, robust hashing, discrete cosines transform, discrete wavelet transform, Fourier transform, Zernike moments.

Citation: Kozachok AV, Kopylov SA, Meshcheryakov RV, Evsutin OO. Review of the current methods for robust image hashing. Computer Optics 2017; 41(5): 743-755. DOI: 10.18287/2412-6179-2017-41-5-743-755.

Acknowledgments: This work was financially supported by the Ministry of Education and Science of the Russian Federation as part of the state project TSUCSR in 2017-2019. (Project No. 2.3583.2017/4.6).

References

[1] Weber R.H. Internet of Things – New security and privacy challenges. Computer Law & Security Review 2010; 26(1): 23-30. DOI: 10.1016/j.clsr.2009.11.008.

[2] InfoWatch 2017 Global data leakage report [In Russian]. Moscow; 2017.

[3] Chaudhuri A. Internet of things data protection and privacy in the era of the General Data Protection Regulation. Journal of Data Protection & Privacy 2016; 1(1): 64-75.

[4] Kougianos E, Mohanty SP, Coelho G, Albalawi U, Sundaravadivel P. Design of a high-performance system for secure image communication in the internet of things. IEEE Access; 2016: 4; 1222-1242. DOI: 10.1109/ACCESS.2016.2542800.

[5] GOST R 34.11-2012 Information technology. Cryptographic data security. Hash-function. Moscow: "Standartinform" Publisher; 2012.

[6] Hsu CY, Lu CS. Geometric distortion-resilient image hashing scheme and its applications on copy detection authentication. Multimedia systems 2005: 11(2); 159-173. DOI: 10.1007/s00530-005-0199-y.

[7] Chen B. Robust image hash functions using higher order spectra. A Thesis submitted in fulfilment of the requirements for the Degree of Doctor of Philosophy. London: Queensland University of Technology; 2012.

[8] Schneider M., Chang S-F. A robust content based digital signature for image authentication. Proceedings of the 3rd IEEE International Conference on Image Processing 1996; 3: 227-230. DOI: 10.1109/ICIP.1996.560425.

[9] Venkatesan R, Koon S, Jakubowski M, Moulin P. Robust image hashing. ICIP 2000; 3: 664-666. DOI: 10.1109/ICIP.2000.899541.

[10] Chang E-C, Kankanhalli MS, Guan X, Huang Z, Wu Y. Robust image authentication using content based compression. Multimedia systems 2003; 9(2): 121-130. DOI: 10.1007/s00530-003-0083-6.

[11] Swaminathan A, Mao Y, Wu M. Robust and secure hashing for images. IEEE Transactions on Information Forensics and Security 2006; 1(2): 215-230. DOI: 10.1109/TIFS.2006.873601.

[12] Tang Z, Wang S, Zhang X, Wei W, Su S. Robust image hashing for tamper detection using non-negative matrix factorization. Journal of Ubiquitous Convergence and Technology 2008; 2(1): 18-26.

[13] Zhao Y, Wang S, Feng G, Tang Z. A robust image hashing method based on Zernike moments. Journal of Computational Information Systems 2010; 6(3): 717-725.

[14] Yu F-X, Lei Y-Q, Wang Y-G. Robust image hashing based on statistical invariance of DCT coefficients. Journal of Information Hiding and Multimedia Signal Processing 2010; 1(4): 286-291.

[15] Sebastian LS, Varghese A, Manesh T. Image authentication by content preserving robust image hashing using local and global features. Procedia Computer Science 2015; 46: 1554-1560. DOI: 10.1016/j.procs.2015.02.081.

[16] Deepa S, Nagajothi A. A secure hashing scheme for image authentication using Zernike moment and local features with histogram features. American International Journal of Research in Science, Technology, Engineering & Mathematics 2014; 5(2): 190-195.

[17] Ouyang J, Coatrieux G, Shu H. Robust hashing for image authentication using quaternion discrete Fourier transform and log-polar transform. Digital Signal Processing 2015; 41(C): 98-109. DOI: 10.1016/j.dsp.2015.03.006.

[18] Woo Ch-S. Digital image watermarking methods for copyright protection and authentication. Thesis submitted in accordance with the regulations for Degree of Doctor of Philosophy. London: Queensland University of Technology; 2007.

[19] Fridrich J., Goljan M. Robust hash functions for digital watermarking. ITCC 2000: 178-183. DOI: 10.1109/ITCC.2000.844203.

[20] Li K, Zhang X. Reliable adaptive watermarking scheme integrated with JPEG2000. ISPA 2003: 117-122. DOI: 10.1109/ISPA.2003.1296879.
[21] Lu CS, Sun SW, Chang PC. Robust hash-based image watermarking with resistance to geometric distortions and watermark-estimation attack. Proc SPIE 2005; 5681: 147-163. DOI: 10.1117/12.586637.
[22] Minguillon J, Herrera-Joancomarti J, Megias D. A robust watermarking scheme based on the JPEG2000 standard. Journal of Electronic Imaging 2005; 14: 681-684. DOI: 10.1117/1.1988334.
[23] Ridzon R, Levicky D. Robust digital watermarking based on the log-polar mapping. Radioengineering 2007; 16(4): 76-81.
[24] Kitanovski V, Taskovski D, Bogdanova S. Combined hashing/watermarking method for image authentication. International Journal of Computer, Electrical, Automation, Control and Information Engineering 2007; 1(6): 575-581.
[25] Winter C, Steinebach M, Yannikos Y. Fast indexing strategies for robust image hashes. Digital Investigation 2014; 11(1): S27-S35. DOI: 10.1016/j.diin.2014.03.004.
[26] Yang Y, Shen F, Shen H, Li H, Li X. Robust Discrete Spectral Hashing for Large-Scale Image Semantic Indexing. IEEE Transactions on Big Data 2015: 1(4) 162-171. DOI: 10.1109/TBDATA.2016.2516024.
[27] Kozachok AV, Kopylov SA. Comparative analysis of robust image hashing methods [In Russian]. Questions of technical sciences: new approaches in the decision of topical problems 2016; III: 24-27.

Authors' information

Alexander Vasilievich Kozachok (b. 1988) graduated from Academy of the Federal Guard Service in 2010, with a degree in Information Security of Telecommunication Systems. In 2012 he defended his Candidate in Engineering degree majoring in Methods and Systems of Data Protection, Information Security. Currently he works as an officer at the Academy of Federal Guard Service. His research interests are information security, protection from unauthorized access, mathematical cryptography and theoretical problems of informatics. E-mail: *a.kozachok@academ.msk.rsnet.ru* .

Sergey Alexandrovich Kopylov (b. 1988) graduated from Academy of the Federal Guard Service in 2010, with a degree in Information Security of Telecommunication Systems. He works as an officer at the Academy of Federal Guard Service. His research interests are currently focused on information security, protection from unauthorized access and image processing. E-mail: *gremlin.kop@mail.ru* .

Roman Valeryevich Meshcheryakov (b. 1974) is Doctor in Engineering, professor, and vice-rector for research and innovation of the Tomsk State University of Control Systems and Radioelectronics. He is graduated (1997) from the Altai State Technical University majoring in Information Processing and Measurement Equipment and Technology. He received his Candidate in Engineering (2000) and Doctor in Engineering (2011) degrees. His current research interests include processing, analysis, synthesis of speech signals and texts, system analysis, information security, mathematical modeling. E-mail: *mrv@tusur.ru* .

Oleg Olegovich Evsutin (b. 1987) graduated with honours from the Tomsk State University of Control Systems and Radioelectronics in 2009, majoring in Complex Information Security of Computer Systems. He received his Candidate in Engineering (2012) degree from Tomsk State University. He is the associate professor at the TSUCSR's Complex Information Security of Computer Systems sub-department. His current research interests include information security, digital images processing, applications of cellular automata theory. E-mail: *eoo@keva.tusur.ru* .

Received May 11, 2017. The final version – August 16, 2017.