

Новая схема разработки быстрых алгоритмов обнаружения дубликатов

А.В. Кузнецов^{1,2}, В.В. Мясников^{1,2}

¹Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34А, Самара, Россия, 443086

²Институт систем обработки изображений РАН – филиал ФНИЦ «Кристаллография и фотоника» РАН, Молодогвардейская 151, Самара, Россия, 443001

Аннотация. В современном мире искажение цифровых изображений может быть выполнено с использованием широко доступного бесплатного программного обеспечения. Для выполнения операций по сокрытию или изменению каких-либо данных в содержимом сцены не требуется специальных навыков, и эта процедура не требует длительных временных затрат. При этом ущерб, нанесенный использованием таких данных, может быть существенным и необратимым. Для решения задачи обнаружения одного из наиболее часто применяемых видов искажений (встраивание дубликатов) в работе предлагается комплексная технология быстрого обнаружения дубликатов, которая позволяет в режиме реального времени выполнять обнаружение искаженных областей. Основным преимуществом предложенной технологии является высокая скорость работы алгоритмов обнаружения и отсутствие пропусков дубликатов. В рамках экспериментальных исследований приводятся результаты сравнения предложенной технологии с существующими решениями. В работе также сделаны выводы относительно ограничений на методы и параметры методов вносимых в дубликаты искажений.

1. Введение

Обнаружение подделок изображений является сложной и важной проблемой на протяжении многих лет. Одним из наиболее часто используемых типов подделки изображений является копирование и вставка фрагмента изображения в пределах того же изображения (встраивание дубликатов). Существуют два основных подхода при встраивании дубликатов:

- фрагменты перед вставкой не подвергаются каким-либо изменениям (неискаженные дубликаты);
- для сокрытия следов встраивания фрагменты изображений подвергаются различным преобразованиям (искаженные дубликаты).

Чтобы решить задачу обнаружения дубликатов, мы предлагаем несколько новых методов, описанных далее.

Во-первых, мы разработали быстрый алгоритм обнаружения неискаженных дубликатов в режиме скользящего окна с использованием специального структурного шаблона и хэш-функции Рабина-Карпа. Новизна предлагаемого подхода - это отсутствие пропусков дубликатов и низкая вычислительная сложность при обработке больших изображений

(например, данные дистанционного зондирования Земли). Основным недостатком этого решения является невозможность его применения для обнаружения искаженных дубликатов.

Что касается разработки алгоритма обнаружения искаженных дубликатов, мы предлагаем новое решение, которое базируется на применении специального шага предварительной обработки, позволяющего устранить вносимые в дубликат искажения. Проведенные исследования показали высокое качество обнаружения дубликатов с внесенными искажениями в виде локального контрастирования и аддитивного шума.

Следует отметить, что существующая схема обнаружения дубликатов широко используется в настоящее время. Тем не менее, ученые проводят исследования методов, обладающих низкой вычислительной сложностью, которые можно использовать для поиска искаженных дубликатов, преобразованных в широком диапазоне параметров искажений. В этой области исследований мы предлагаем алгоритм обнаружения искаженных дубликатов, который использует функции, основанные на бинарных градиентных контурах, которые устойчивы к линейному контрастированию, аддитивному шуму и сжатию JPEG. Сравнение качества обнаружения при помощи алгоритмов, основанных на бинарных градиентных контурах и основанных на различных формах локальных бинарных шаблонов, показало существенное преимущество в точности обнаружения дубликатов - 20-30%.

2. Обзор литературы

Ситуационный анализ невозможен без использования цифровых изображений. В бытовом смысле передача цифровых изображений производится посредством социальных сетей для обмена информацией о каких-то важных событиях. Суммарное количество цифровых изображений, передаваемых в день посредством популярных веб-приложений колоссально: почти 350 миллионов изображений через Facebook [1] и 80 миллионов изображений через Instagram [2]. Эти данные не являются защищенными, никто не обеспечивает защиту своего авторства.

В настоящее время защита от подделки цифровых изображений является сложной проблемой. Каждый может внести изменения в цифровое изображение с помощью современных программных средств как на персональном компьютере, так и на любом мобильном устройстве за несколько минут. Но никто не может предсказать последствия этих изменений, вносящих искажение в содержание сцены.

Одной из наиболее часто используемых атак на цифровые изображения является встраивание дубликата. Дубликаты на изображении представляют из себя фрагменты с похожим содержанием, полученные путем копирования и вставки локальной области этого изображения. Скопированные области и называются дубликатами. Для сокрытия следов копирования и встраивания фрагмента могут применяться такие преобразования как локальное контрастирование, изменение условий освещения, добавление шума, применение сжатия и аффинных преобразований.

В настоящее время опубликованы четыре обзорных статьи по разработке схем обнаружения дубликатов. В обзоре Christlein et al. [3] авторы обсудили эффективность популярных методов извлечения признаков в задаче обнаружения дубликатов. Затем эффективность подхода на основе различных признаков была проанализирована на собственном наборе данных, содержащих дубликаты. Lin et al. [4] классифицировали методы сопоставления областей на изображении путем прямого сравнения блоков. Между тем, Al-Qershi и Khoo в 2013 году классифицировали [5] существующие методы извлечения признаков и проанализировали их преимущества и недостатки. Warif N.B.A. и другие (2016) в [6] представили новый взгляд на актуальные исследования алгоритмов обнаружения дубликатов и описали схемы обнаружения дубликатов.

Последняя обзорная статья, опубликованная в 2017 году, Salleh S.F.M. и другими [7] содержит анализ проблемы вычислительной сложности в алгоритмах обнаружения дубликатов и пути решения этой проблемы. Авторы сопоставили схему прямого блочного сравнения, а также более сложные параллельные методы.

Методы обнаружения подделок изображений могут быть широко классифицированы как активные и пассивные подходы, в зависимости от наличия априорной информации. Активный подход основан на встраивание дополнительной информации в цифровое изображение для обнаружения несанкционированного доступа, такого как цифровые водяные знаки и цифровые подписи. Такая информация используется для подтверждения оригинальности данных. С другой стороны, пассивный подход способен обнаруживать изменения на изображениях без использования дополнительной информации. Обзор методов активной и пассивной защиты цифровых изображений от подделок показан на рисунке 1 [6].

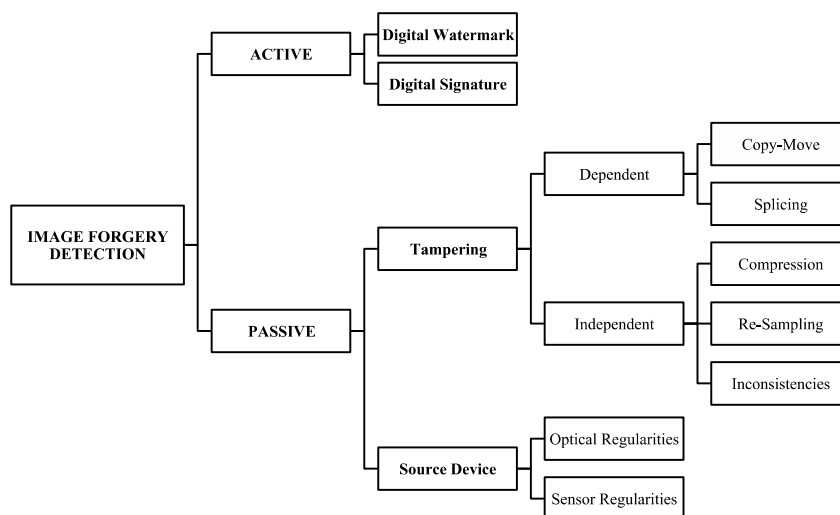


Рисунок 1. Методы активной и пассивной защиты цифровых изображений.

3. Схемы обнаружения дубликатов. Блочные подходы и методы выделения ключевых точек

В настоящее время существует множество работ по разработке алгоритмов обнаружения дубликатов. Большинство из них соответствуют единой схеме алгоритма, представленной в 2005 году Farid и Popescu [8], и, как правило, отличаются способом выбора схемы сравнения: регулярное разбиение на (возможно перекрывающиеся) блоки и основанный на поиске ключевых точек. Исторически первый подход появился ранее [8]. Его существенным недостатком является высокая вычислительная сложность - количество блоков, полученных путем разбиения изображения по регулярной сетке, пропорционально количеству отсчетов изображения, и поэтому количество выполненных сравнений зависит от количества блоков квадратично. Непосредственным следствием этого факта является необходимость выбора блоков как можно ближе друг к другу, что приводит к росту вероятности отсутствия дубликатов. Вычислительная сложность второго подхода на практике оказывается ниже из-за относительно небольшого числа (по сравнению с размерами изображения) обнаруженных ключевых точек. К сожалению, тот же факт является причиной невозможности гарантировать обнаружение всех дубликатов, особенно для фрагментов изображения с низкой дисперсией или регулярной структурой (например, текстуры). Обе схемы могут быть объединены, как показано на рисунке 2.

Итогом анализа обеих схем является важный результат, заключающий в себе невозможность гарантировать 100% обнаружение дубликатов. Наиболее содержательным критерием оценки качества разрабатываемого решения обнаружения дубликатов является мера F1, объединяющая в себе значения Precision и Recall метрик, которые характеризуют количество ложно обнаруженных дубликатов и количество пропущенных дубликатов:

$$F1 = \frac{2 \cdot tp}{2 \cdot tp + fp + fn},$$

где tp – количество верно обнаруженных дубликатов, fp – количество пропущенных дубликатов, fn – количество ложно обнаруженных дубликатов.

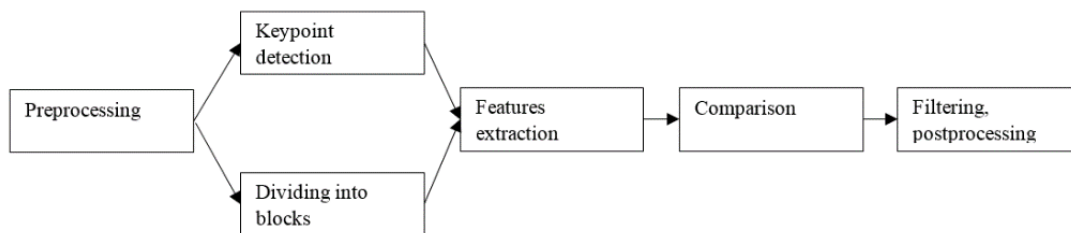


Рисунок 2. Схема работы алгоритмов обнаружения дубликатов.

Как было сказано ранее, основной целью нашего исследования является разработка вычислительно эффективного алгоритма, не допускающего пропуск дубликатов.

4. Алгоритм обнаружения неискаженных дубликатов на основе аппарата хэш-функций

Пусть введены структурный шаблон $\mathfrak{N}(\{(0,0)\}, a, b)$ [9] и изображение f , где $f(m, n) \in [0, 2^q - 1]$. Тогда хэш-значение для фрагмента изображения будет вычисляться посредством двумерного обобщения хэш-функции Рабина-Карпа:

$$\begin{aligned}
 H(m, n, f) \equiv & f(m, n) \cdot 2^{q(ab-1)} + f(m, n+1) \cdot 2^{8(ab-2)} + \dots \\
 & \dots + f(m, n+b-1) \cdot 2^{q(ab-b)} + \dots + f(m+a-1, n) \cdot 2^{q(b-1)} + \\
 & + f(m+a-1, n+1) \cdot 2^{q(b-2)} + \dots + f(m+a-1, n+b-1) \cdot 2^0.
 \end{aligned}
 \tag{1}$$

Полученные таким образом хэш-значения трудно хранить в ходе выполнения алгоритма вычисления:

- отсутствие стандартных программных типов для хранения значений, размер которых превышает 64 бита;
- невозможность хранения хэш-таблицы (гистограммы хэш-значений) требуемого размера в памяти.

Для решения этих проблем мы предлагаем использовать китайскую теорему об остатках, благодаря которой мы формируем R остатков, определяемых следующим образом:

$$H_r(m, n, f) \equiv H(m, n, f) \bmod b_r,
 \tag{2}$$

где b_r взаимно простые числа. Более того, система R функций вида (2) гарантирует соответствие блока изображения конкретному хэш-значению. Этот факт позволяет использовать любой из остатков (3) в качестве хэш-значения. Значения b_r должны удовлетворять условию $b_r \gg 2^q - 1$.

Объединив (1) и (2), получим следующее выражение для $H_r(m, n, f)$:

$$H_r(m, n, f) \equiv \left(\begin{aligned} & \left(f(m, n) \bmod b_r \cdot 2^{q(ab-1)} \bmod b_r \right) \bmod b_r + \\ & + \left(f(m, n+1) \bmod b_r \cdot 2^{q(ab-2)} \bmod b_r \right) \bmod b_r + \dots \\ & \dots + f(m+a-1, n+b-1) \bmod b_r \end{aligned} \right) \bmod b_r.
 \tag{3}$$

Примем также следующие упрощения:

- $f(m, n) \bmod b_r = f(m, n)$ ввиду $f(m, n) \in [0, 2^q - 1]$ и $b_r \gg 2^q - 1$;
- $p_r^i = 2^{qi} \bmod b_r$, $i \in [1, b-1]$ вычисляется однократно при загрузке изображения;
- вычисление $\bmod b_r$ для слагаемых можно опустить, потому что значение суммы не превосходит размер разрядной сетки.

Результат применения упрощений приводит к выражению (4):

$$H_r(m, n, f) = \left(\begin{matrix} f(m, n)p_r^{ab-1} + \\ + f(m, n+1)p_r^{ab-2} + \dots \\ + f(m+a-1, n+b-1) \end{matrix} \right) \text{mod } b_r \tag{4}$$

Хэш-значение (2) может быть вычислено рекурсивно для структурного шаблона $\mathfrak{N}(\{(0,0)\}, 1, b)$ как для исходного, так и для модулярного представлений:

$$H(m, n, f) = 2^q (H(m, n-1, f) - 2^{q(b-1)} f(m, n)) + f(m, n+b-1).$$

Рекурсивная форма вычисления хэш-значений для прямоугольного варианта структурного шаблона выглядит следующим образом (для строк и столбцов соответственно):

$$\begin{aligned} H(m, n+1, f) &= 2^q H(m, n, f) - \\ &- 2^{qab} f(m, n) + \sum_{i=1}^{a-1} 2^{qb(a-i)} (f(m+i-1, n+b-1) - f(m+i, n)) + \\ &+ f(m+a-1, n+b-1), \\ H(m+1, n, f) &= 2^{qb} \left(H(m, n, f) - \sum_{i=0}^{b-1} 2^{q(ab-i-1)} f(m, n+i) \right) + \sum_{i=1}^b 2^{q(b-i)} f(m+a, n+i). \end{aligned}$$

Операции умножения на степени 2 выполняются путем применения высокоэффективной операции битового сдвига. Все это приводит к снижению вычислительной сложности решения.

Схема алгоритма обнаружения неискаженных дубликатов представлена на рисунке 3.

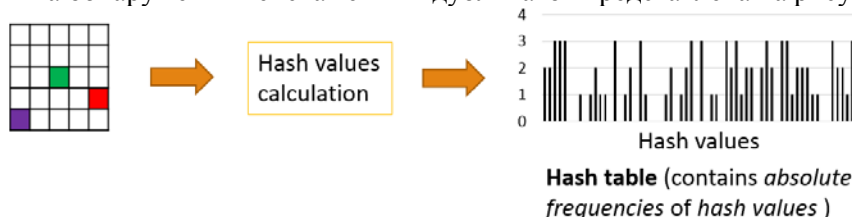


Рисунок 3. Схема алгоритма обнаружения неискаженных дубликатов.

5. Общий подход к обнаружению дубликатов на основе аппарата хэш-функций

Ядром предлагаемого решения, как уже упоминалось выше, является алгоритм обнаружения неискаженных дубликатов, ранее разработанный авторами [9]. Алгоритм основан на хэш-функции Рабина-Карпа [9], значения которой вычисляются в скользящем окне и хранятся в хэш-таблице для оценки частоты хэш-значений. Таким образом, для использования этого алгоритма в целях обнаружения искаженных дубликатов необходимо «привести» некоторым образом преобразованные локальные области к неискаженному виду. Чтобы решить эту проблему, мы предлагаем использовать новый этап предварительной обработки (рисунок 4).

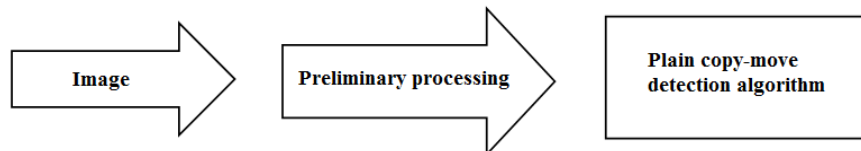


Рисунок 4. Общая схема быстрого алгоритма обнаружения дубликатов на изображении.

Очевидным требованием для процедуры предварительной обработки является совпадение результатов обработки для блоков-дубликатов. В общем, это требование не может быть гарантировано. В то же время, для определенных яркостных преобразований и некоторых параметров предварительной обработки это требование может быть выполнено. В рамках данной работы мы использовали такие преобразования как снижение диапазона яркостных

уровней изображения, вычисление градиента, адаптивное линейное контрастирование, разложение по ортонормированному базису, различные формы локальных бинарных шаблонов.

6. Экспериментальные исследования

Для проведения экспериментов мы использовали стандартный ПК (Intel Core i5-3470 3,2 ГГц, 8 ГБ оперативной памяти). Мы выбрали 10 8-битных изображений с размерами 512×512 для проведения исследований. Для создания подделок мы использовали ранее разработанную процедуру автоматической генерации дубликатов [9, 10], поддерживающую контроль размеров встраиваемых дубликатов, их количество, а также тип и параметры преобразований. В ходе генерации выборки, содержащей дубликаты, использовались следующие искажения локальных фрагментов-дубликатов:

- Яркостный сдвиг;
- Линейный контраст (мультипликативный и аддитивный коэффициенты);
- Аддитивный белый шум.

Для оценки качества предлагаемого решения мы использовали количество верно обнаруженных дубликатов – tp и ложно обнаруженных дубликатов – fp ; tp - количество верно обнаруженных дубликатов, fp - количество пропущенных дубликатов.

Используя разработанную процедуру автоматического встраивания дубликатов, было создано 90 подделок (30 изображений для каждого вида искажений) для каждого из 10 изображений, которые были дополнительно обработаны предложенным алгоритмом обнаружения дубликатов на основе 8 различных предварительных преобразований: уменьшение яркостного диапазона, вычисление градиента, разложение по ортонормированному базису (с нормализацией и без него), адаптивное линейное контрастирование (АЛК), его упрощенная версия АЛК и АЛК на основе функции softmax.

На рисунках 5 и 6 показана зависимость значений tp и fp от значения аддитивного коэффициента b яркостного сдвига. Большинство предварительных преобразований приводят к росту значения tp . Наименьшее качество достигается при помощи преобразование уменьшения интенсивности изображения.

Если дубликат искажается при помощи линейного контрастирования, то наилучшими предварительными преобразованиями, ведущими к высокому качеству обнаружения, являются ЛБШ и АЛК. Ясно, что для всех преобразований ниже значения a соответствуют более низкому качеству обнаружения (рисунки 7 и 8).

Основной характеристикой аддитивного белого шума является отношение сигнал/шум (SNR). Мы добавляли шум в рамках процедуры встраивания дубликатов. Результаты экспериментов показаны на рисунках 9 и 10.

Как видно из проведенных экспериментов, мы получили хорошие результаты в смысле выбранного критерия качества tp и fp . Большинство преобразований приводят к устойчивому обнаружению дубликатов для широкого диапазона параметров искажений. В то же время вычислительную сложность предложенного метода существенно ниже, чем для блочных подходов с использованием инвариантных к преобразованиям признаков. Недостатком является все же узкий спектр искажений, которые могут быть устранены при помощи предварительной процедуры обработки.

7. Выводы

Рассматривая результаты всех экспериментов, исследования в области методов предварительной обработки изображений для обнаружения дубликатов являются перспективными. Наилучшее решение в соответствии со значениями tp и fp для всех диапазонов параметров применяемых преобразований – это метод, основанный на процедуре предварительной обработки на основе локальных бинарных шаблонов. При достаточно низкой вычислительной сложностью посредством разработанной схемы можно добиться высокого качества обнаружения по сравнению с существующими решениями на основе признаков и

ключевых точек, которые обеспечивают хорошие результаты при значительно большей вычислительной сложности.

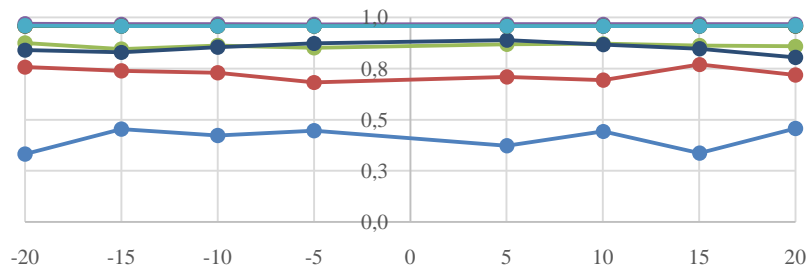


Рисунок 5. Зависимость tp от коэффициента b яркостного сдвига.

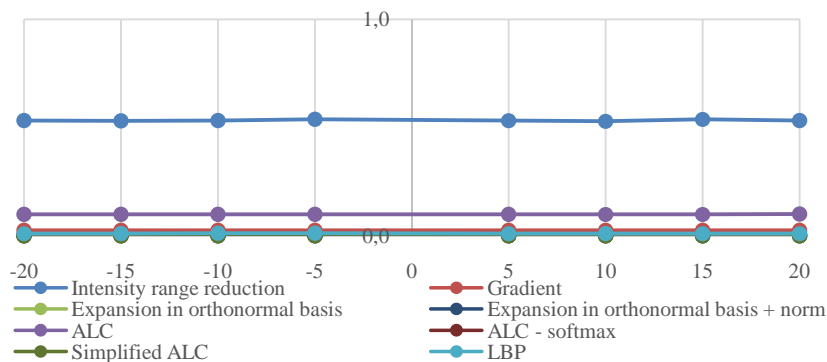


Рисунок 6. Зависимость fp от коэффициента b яркостного сдвига.

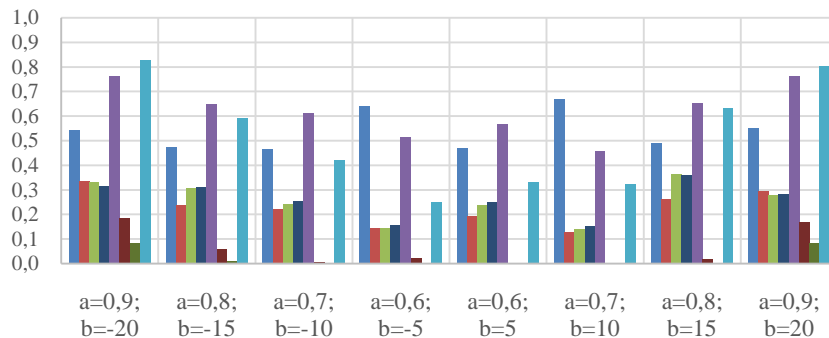


Рисунок 7. Зависимость tp от значений a и b яркостного сдвига.

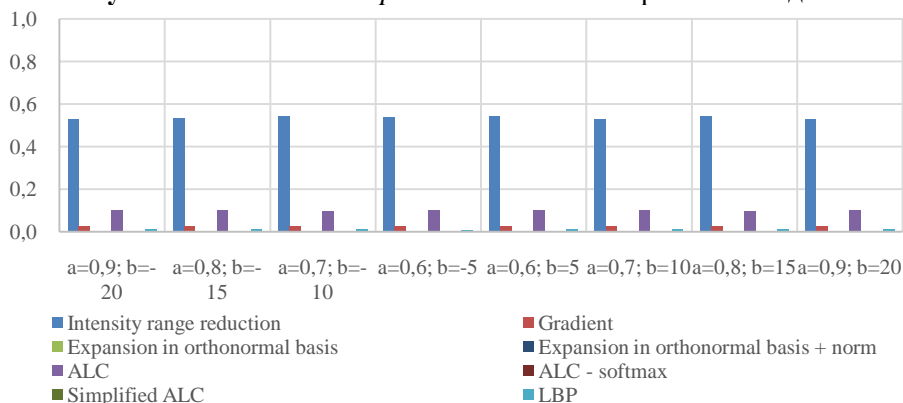


Рисунок 8. Зависимость fp от значений a и b яркостного сдвига.

8. Благодарности

Работа выполнена при поддержке Федерального агентства научных организаций (соглашение № 007-ГЗ/Ч3363/26) и грантов РФФИ 18-07-01312 А "Методы нелинейного снижения

размерности гиперспектральных изображений и их применение", 17-29-03190 "Методы и алгоритмы совместной обработки данных камеры и сенсоров мобильных устройств для реконструкции трехмерных моделей окружающей обстановки".

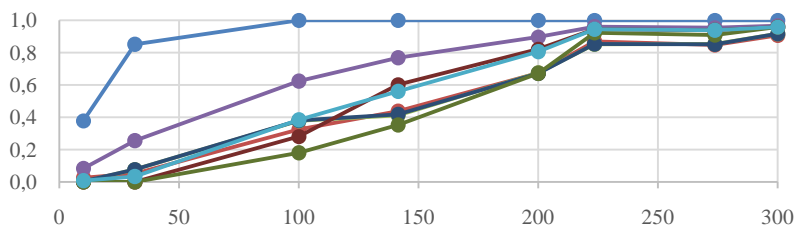


Рисунок 9. Зависимость tp от SNR .

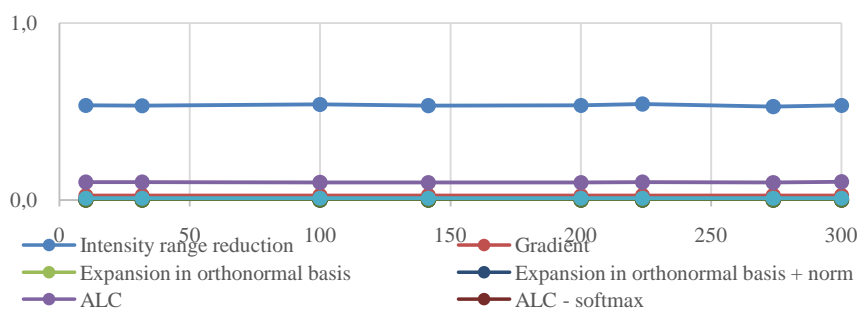


Рисунок 10. Зависимость fp от SNR .

9. Литература

- [1] <https://www.brandwatch.com/blog/47-facebook-statistics-2016/>.
- [2] <https://www.brandwatch.com/blog/37-instagram-stats-2016/>.
- [3] Christlein, V. An Evaluation of Popular Copy-Move Forgery Detection Approaches / V. Christlein, C. Riess, J. Jordan, E. Angelopoulou // IEEE Trans. Inf. Forensics Secur. – 2012. – Vol. 7. – P. 1841-1854.
- [4] Lin, W. Survey on blind image forgery detection / W. Lin, S.U. Khan, K.C. Yow, T. Qazi, S.A. / Madani, C.-Z. Xu, J. Kołodziej, I.A. Khan, H. Li, K. Hayat // IET Image Process. – 2013. – Vol. 7. – P. 660–670. DOI: 10.1049/iet-ipr.2012.0388.
- [5] Al-Qershi, O.M. Passive detection of copy-move forgery in digital images: state-of-the-art / O.M. Al-Qershi, B.E. Khoo // Forensic Sci.Int. – 2013. – Vol. 231. – P. 284-295. DOI: 10.1016/j.forsciint.2013.05.027.
- [6] Warif, N.B.A. Copy-move forgery detection: Survey, Challenges, and Future Directions / N.B.A. Warif, A.W.A. Wahab, M.Y.I. Idris, R. Ramli, R. Salleh, S. Shamshirband, K.K.R. Choo // J. Network Comp. Apps. – 2016. DOI: 10.1016/j.jnca.2016.09.008.
- [7] Salleh, S.F.Md. Copy-Move Forgery Detection: A Survey On Time Complexity Issues And Solutions / S.F.Md Salleh, M.F. Rohani, V.A. Maarof // Journal of Theoretical & Applied Information Technology. – 2017. – Vol. 95(11). – P. 2552-2566.
- [8] Popescu, A.C. Exposing Digital Forgeries by Detecting Duplicated Image Regions / A.C. Popescu, H. Farid, 2004.
- [9] Kuznetsov, A. A fast plain copy-move detection algorithm based on structural pattern and 2D Rabin-Karp rolling hash / A. Kuznetsov, V. Myasnikov // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). – 2014. – Vol. 8814(1). – P. 461-468.
- [10] Kuznetsov, A. A Copy-Move Detection Algorithm Using Binary Gradient Contours / A. Kuznetsov, V. Myasnikov // International Conference on Image Analysis and Recognition, ICIAR 2016. – 2016. – Vol. 9730. – P. 349-357.

New scheme for fast copy-move detection

A.V. Kuznetsov^{1,2}, V.V. Myasnikov^{1,2}

¹Samara National Research University, Moskovskoe Shosse 34A, Samara, Russia, 443086

²Image Processing Systems Institute of RAS - Branch of the FSRC "Crystallography and Photonics" RAS, Molodogvardejskaya street 151, Samara, Russia, 443001

Abstract. Image forgery detection is a challenging and important problem for many years. One of the most frequently used type of forgery (copy-move) is copying and pasting image fragment within the same image. There are exist two main types of copy-move forgeries: on one hand, they are created without applying transformations (plain copy-move) and on the other – different digital transforms can be used to hide the traces of copy-move forgery (transformed copy-move). To solve the task of copy-move forgery detection in a complex way we propose several novel techniques, described further. The carried out research showed high quality of copy-move detection with intensity shift, contrast enhancement and additive noise distortions. In conclusion part we provide limitations of the scheme and the ranges of distortion parameters that can be detected.

Keywords: forgery, detection algorithm, copy-move, hash-based, F1 score.