УДК 004.056+004.932

МЕТОД ГЕНЕРАЦИИ НАБОРА ПОДДЕЛЬНЫХ ИЗОБРАЖЕНИЙ ДЛЯ ОБУЧЕНИЯ СИСТЕМЫ ОБНАРУЖЕНИЯ ПОДДЕЛОК ТИПА «COPY-MOVE»

Спирин Руслан Николаевич, Насретдинов Рауф Салаватович

Алтайский государственный университет, г. Барнаул
e-mail: spirinruslan2002@mail.ru, uniform97@gmail.com

METHOD FOR GENERATING A SET OF FAKE IMAGES FOR TRAINING A “COPY-MOVE” TYPE FAKE DETECTION SYSTEM

Spirin Ruslan N., Nasretdinov Rauf S.

Altai State University, Barnaul

Аннотация. В современном мире подделка изображений является очень распространенным явлением. Самым распространенным методом подделки изображений является «copy-move». Преимущества «copy-move» над другими методами изменения заключается в том, что вставляется область из этого же изображения, то есть она имеет яркость и контрастность такую же, как и остальные объекты. Так же, к этим изображениям могут применятся различные методы постобработки и различные манипуляции, такие как сжатие JPEG, изменение яркости или выравнивание, которые могут уменьшить следы, затрудняют обнаружение. Для того, чтобы тренировать системы обнаружения подделок типа «copy-move» или оценивать качество их работы, необходимы специальные наборы данных. В данной работе представлен метод адаптивной генерации набора поддельных изображений для обучения системы обнаружения подделок типа «copy-move», основанной на нейросетевой модели BusterNet. Предложенный в работе метод адаптивной генерации набора изображений продемонстрировал высокий уровень качества созданных подделок. При его работе применялся широкий спектр методов пред- и постобработки, что позволило сделать сгенерированный набор устойчивым к обнаружению современными нейросетевыми методами. Его применение позволит в перспективе эффективно

Abstract. In today's world, image forgery is very common. The most common method of falsifying images is «copy-move». The advantage of «copy-move» over other modification methods is that an area from the same image is inserted, that is, it has the same brightness and contrast as other objects. Also, these images can be subject to various post-processing techniques and various manipulations, such as JPEG compression, brightening or straightening, which can reduce traces that make detection difficult. In order to train copy-move counterfeit detection systems or evaluate the quality of their work, special data sets are needed. This paper presents a method for adaptively generating a set of fake images for training a copy-move type forgery detection system based on the BusterNet neural network model [1]. The method of adaptive generation of a set of images proposed in the work demonstrated a high level of quality of the created fakes. During its work, a wide range of pre- and post-processing methods was used, which made it possible to make the generated set resistant to detection by modern neural network methods. Its use will make it possible in the future to effectively carry out further training of new methods for detecting «copy-move» counterfeits.

Keywords: «copy-move», BusterNet, F1-score, analysis of connected components, binarization, neural network.

проводить дообучение новых методов обнаружения подделок типа «copy-move».

Ключевые слова: «copy-move», BusterNet, F1-score, анализ связанных компонентов, бинаризация, нейронная сеть.

Для цитирования: Спирин Р.Н., Насретдинов Р.С. Метод генерации набора поддельных изображений для обучения системы обнаружения подделок типа «Copy-Move» // Проблемы правовой и технической защиты информации. 2023. №11. С. 52-60.

For citation: Spirin R.N., Nasretdinov R.S. Method for generating a set of fake images for training a "Copy-Move" type fake detection system // Legal and Technical Problems Information Protection. 2023. No. 11. P. 52-60.

Введение. В современном мире большинству людей доступны хорошие камеры, которые позволяют делать качественные снимки, и различные инструменты для редактирования изображений, которые позволяют создавать подделки, настолько качественные, что их сложно отличить от обычных изображений. Самым распространенным методом подделки изображений является «copy-move». Суть метода заключается в том, что область из изображения копируется и вставляется в то же изображения. Он устойчив к обнаружению, так как вставляется область из этого же изображения, то есть она имеет яркость и контрастность такую же, как и остальные объекты и при умелой обработке оно не будет выглядеть чужим на этом изображении. Методы для решения проблемы можно разделить на две группы, первая группа, это методы, основанные на выделении различных признаков, вторая это методы на основе нейронных сетей. Для того, чтобы тренировать системы обнаружения подделок типа «copy-move» или оценивать качество их работы, необходимы специальные наборы данных. Для решения задач связанных с «copy-move» уже существуют наборы данных, например CASIA2.0 [1] и CoMoFoD [2], однако они были созданы вручную, и данные наборы являются неизменяемыми, что ограничивает их применение для обучения нейронных сетей.

В данной работе представлен метод адаптивной генерации набора поддельных изображений для обучения системы обнаружения подделок типа «copy-move», основанной на нейросетевой модели BusterNet [3]. Суть метода заключается в том, что мы генерируем все возможные «copy-move» подделки и отбираем из них те, которые хуже всего были распознаны.

Алгоритм генерации поддельных изображений. Генерацию набора данных можно разделить на несколько этапов, которые представлены на рисунке 1.

Для начала необходимо получить одно изображение из набора данных. Далее необходимо обнаружить все объекты на нем.

В качестве системы обнаружения объектов используется Detectron2 [4]. Detectron2 является библиотекой компьютерного зрения, которая предоставляет самые современные алгоритмы обнаружения и сегментации. С помощью Detectron2 можно извлечь маски объектов изображений (рисунок 2). Тут важно понимать, что Detectron2 сможет обнаружить только те объекты, на которых обучена конкретная модель. После выделение масок необходимо изменить размер оригинального изображения и масок на 256x256. Сначала нужно извлечь маски, а потом изменять их размер, по той причине, что уменьшение оригинального изображения до извлечения масок может привести к ухудшению точности обнаружения.

Рисунок 1. Алгоритм генерации «copy-move» изображений

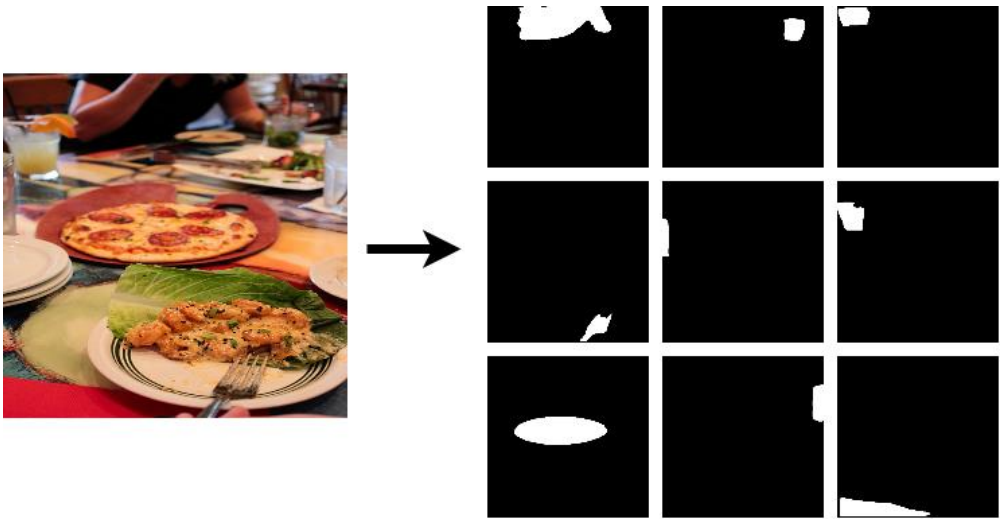

Рисунок 2. Алгоритм генерации «copy-move» изображений

Создание подделок типа «copy-move» довольно часто сопровождается с тем, что перемещаемую область увеличивают, уменьшают или поворачивают. Набор данных будет генерироваться с учетом этого, и изображения будут специально помечаться.

Далее генерируются все возможные «copy-move» изображения для всех объектов и отбирается k лучших. Объекты могут увеличиваться, уменьшаться, и поворачиваться. Так же границы объектов сглаживаются.

Для оценки качества обнаружения подделок типа «copy-move» был использован F1-score. F1-score вычисляется на уровне пикселей. Необходимо определить количество правильно обнаруженных пикселей поддельной/настоящей области, количество пикселей, которые были ошибочно определены как поддельные/настоящие, и ложно пропущенные поддельные / настоящие пиксели.

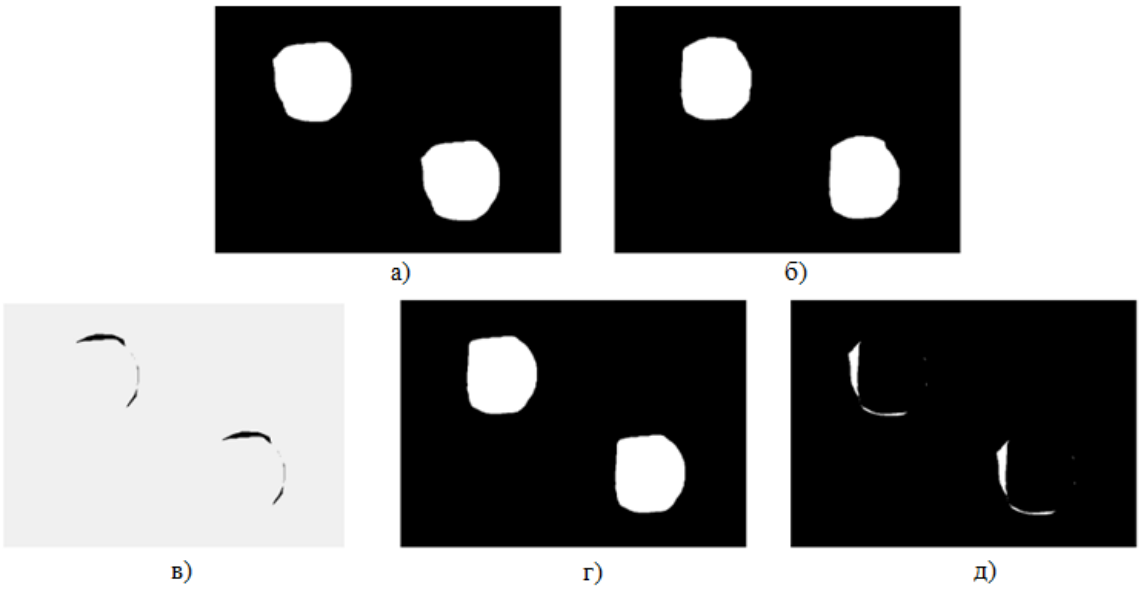

Рисунок 3. Пример выделения параметров для обнаружения «copy-move»: а) реальная маска; б) предсказанная маска; в) ошибочно определённые пиксели как поддельные (Fp); г) правильно определённые пиксели (Tp); д) пропущенные поддельные пиксели (Fn)

С помощью этих значений высчитывается точность (Precision) и полнота (Recall). Точность (1) означает вероятность того, что обнаруженная подделка действительно является подделкой, а полнота (2) показывает вероятность обнаружения поддельного изображения. А с помощью этих двух параметров высчитывается оценка F_1 (3), которая и позволяет определить точность предсказаний.

$$\text{Precision} = \frac{\text{Tp}}{\text{Tp+Fp}}. \quad (1)$$

$$\text{Recall} = \frac{\text{Tp}}{\text{Tp+Fn}}. \quad (2)$$

$$\text{F}_1 = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}. \quad (3)$$

Минимальный порог точности равен 0,456. Это средняя точность для набора CASIA 2.0. Если точность сгенерированного изображения меньше, чем минимальный порог, то мы сохраняем весь набор.

В качестве исходных изображений были взяты изображения из набора данных COCO. COCO (Microsoft Common Objects in Context) [5] – это крупномасштабный набор данных для обнаружения объектов, сегментации, обнаружения ключевых точек и подписей. Набор данных состоит из 328 тыс. изображений.

В качестве системы обнаружения подделок была взята BusterNet – двухветвевая архитектура, основанная на сверточных нейронных сетях.

Результаты генерации. В результате было сгенерировано 1505 наборов изображений, из которых 1220 будут использоваться для обучения, а 285 для тестирования. Каждый из наборов состоит из: оригинального изображения, «copy-move» подделки и RGB маски (рисунок 4).

Если сравнить сгенерированный набор данных с другими (таблица 1), то можно увидеть, что в отличии от CASIA2.0 и CoMoFoD он генерируется автоматически без участия человека, что позволяет легко получать RGB маски.

а) б) в)

Рисунок 4. Пример набора: а) оригинальное изображение; б) «copy-move» подделка; в) RGB маска

Таблица 1. Сравнение сгенерированного набора с существующими наборами данных

Набор данных	Сгенерированный	CASIA 2.0	CoMoFoD
Количество изображений	1505	3274	5000
Создан	Автоматически	Вручную	Вручную
Размеры	256X256	-	512X512
Предобработка	Изменение размеров (0,8:1,2), поворот (-180°:180°)	Изменение размеров, поворот	Изменение размеров, поворот
Постобработка	Сглаживание границ	Размытие, сглаживание границ	Размытие, сглаживание границ, шум, яркость, контрастность, сжатие JPEG
Маски	RGB	RGB, частично размечено 1313 изображений	Черно-белая/цветная

Анализ полученных результатов. Все методы оценки качества изображений (IQA) можно разделить на две категории: методы с использованием эталонного изображения и методы без использования эталонного изображения.

Результат оценки Inception score можно увидеть на рисунке 5. Для сравнения, на рисунке 6 приведен результат для CASIA2.0. Чем выше оценка, тем качественней изображение, что можно увидеть на приведенных подделках на рисунке 7. На каждое использованное изображение из COCO приходится максимум пять «copy-move» изображений, поэтому можно назвать сгенерированный набор данных разнообразным. Однако CASIA 2.0 насчитывает 3274 изображений, поэтому средняя оценка Inception score оценка больше.

Таблица 2. Сравнение методов оценки изображений

Название	Уровень оценки	Интерпретация оценки
Inception Score (IS) [7]	Набор изображений	Чем больше Inception score, тем качественней и разнообразней является весь набор данных
BRISQU [8]	Изображение без сравнения с эталонным	Чем больше оценка BRISQU, тем реалистичнее кажется данное изображение
DISTS [9]	Изображение в сравнении с эталонным	Чем меньше оценка DIST, тем реалистичнее кажется изображение относительно изначального (эталонного) изображения

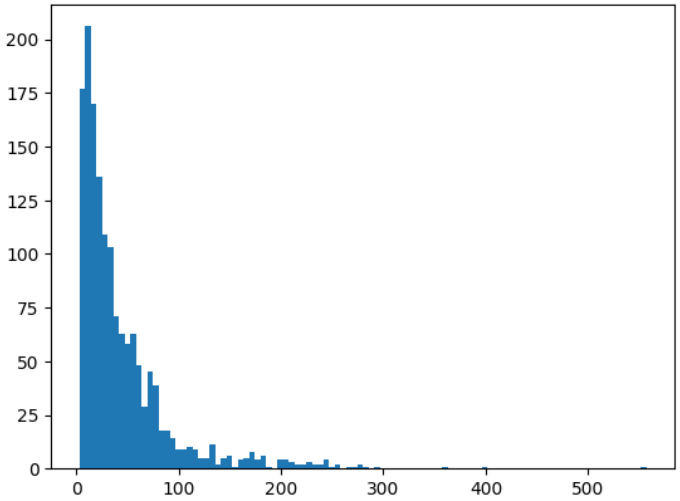

Рисунок 5. Inception score для сгенерированного набора данных

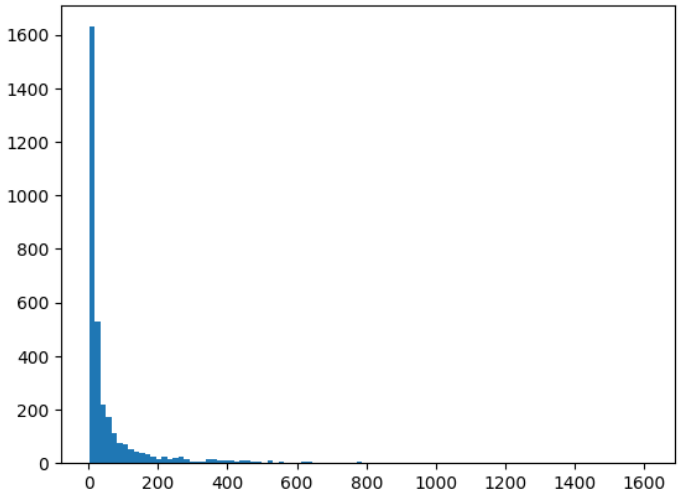

Рисунок 6. Inception score для набора данных CASIA2.0

а) б) в) г)

Рисунок 7. Примеры изображений с оценками: а) 3,33; б) 90; в) 150,6; г) 338,78

Результат BRISQUE можно увидеть на рисунке 8. Для сравнения, на рисунке 9 приведен результат для CASIA2.0. BRISQUE имеет высокую корреляцию с мнением человека. Чем выше оценка, тем реалистичнее кажется изображение, что можно увидеть на приведенных подделках на рисунке 10. Как видно на гистограмме распределения BRISQUE считает сгенерированный набор более качественным, так как среднее значение оценки выше.

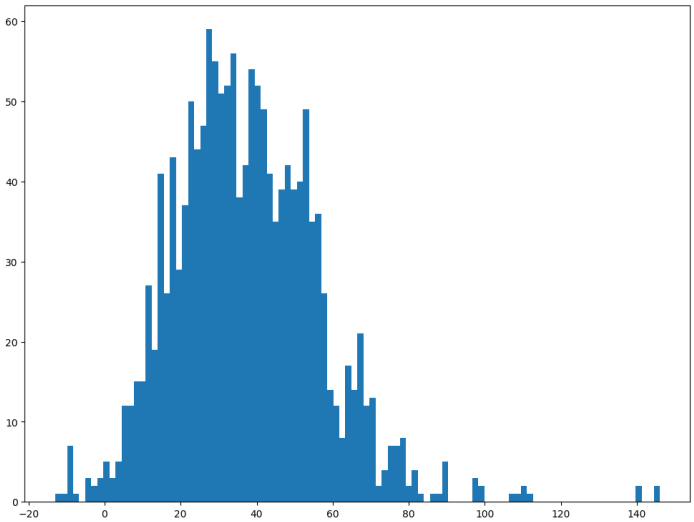

Рисунок 8. BRISQUE для сгенерированного набора данных

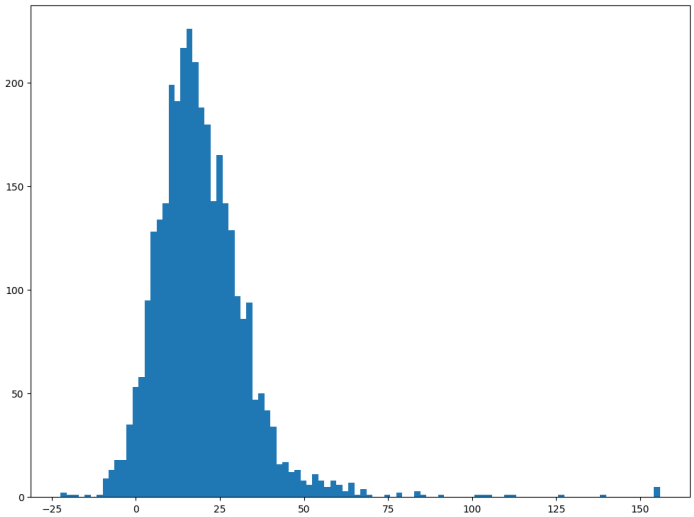

Рисунок 9. BRISQUE для набора данных CASIA2.0

а) б) в) г)

Рисунок 10. Примеры изображений с оценками по метрике: а) 0,46; б) 30,05; в) 82,55; г) 140,66

Результат DISTS можно увидеть на рисунке 11. Для сравнения, на рисунке 12 приведен результат для CASIA2.0. Чем ниже оценка, тем выше качество (относительно оригинального изображения), что можно увидеть на приведенных подделках на рисунке 13. Как видно из распределения, модель считает сгенерированный набор данных более качественным, чем CASIA2.0, так как все оценки меньше 0,2.

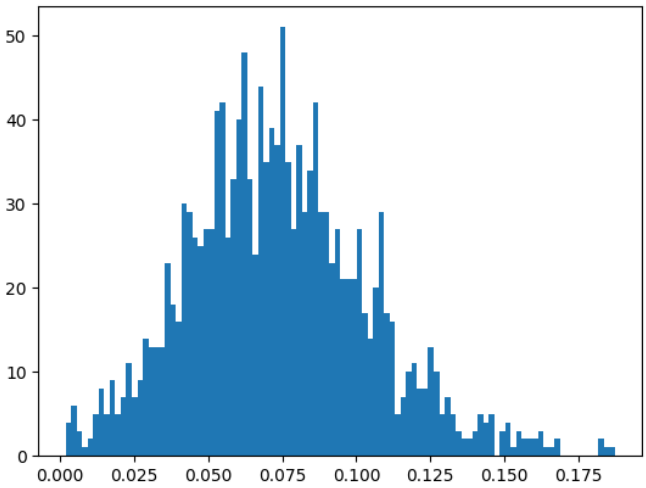

Рисунок 11. DISTS для сгенерированного набора данных

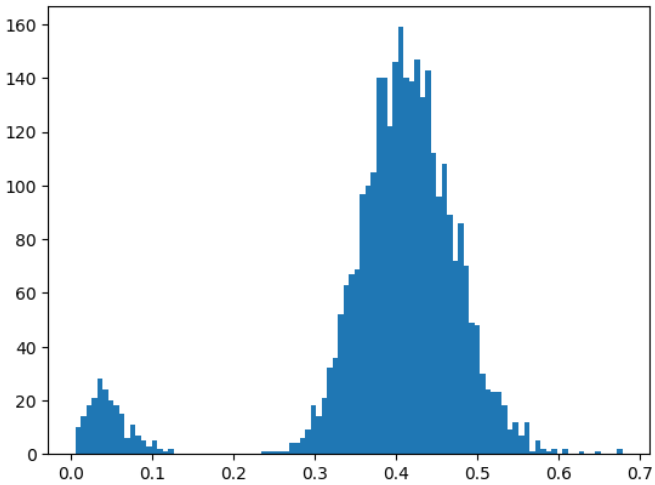

Рисунок 12. DISTS для набора данных CASIA2.0

а) б) в) г)

Рисунок 13. Примеры изображений с оценками: а) 0,187; б) 0,126; в) 0,06; г) 0,015

Заключение. Предложенный в работе метод адаптивной генерации набора изображений продемонстрировал высокий уровень качества созданных подделок. При его работе применялся широкий спектр методов пред- и постобработки, что позволило сделать сгенерированный набор устойчивым к обнаружению современными нейросетевыми методами. Его применение позволит в перспективе эффективно проводить дообучение новых методов обнаружения подделок типа «copy-move».

Библиографический список

1. *Dong, W. Wang, T. Tan. CASIA Image Tampering Detection Evaluation Database / Dong, Jing et al. "CASIA Image Tampering Detection Evaluation Database." 2013 IEEE China Summit and International Conference on Signal and Information Processing. 2013. С. 422-426.*
2. *D. Tralic, I. Zupancic, S. Grgic, M. Grgic. CoMoFoD — New database for «copy-move» forgery detection / Proceedings ELMAR-2013. 2013. С. 49-54.*
3. *Yue Wu, Wael Abd-Almageed, Prem Natarajan "BusterNet: Detecting «copy-move» Image Forgery with Source/Target Localization" / Proceedings of the European Conference on Computer Vision (ECCV). 2018. С. 168-184.*
4. *Detectron2. github.com: сайт. URL: https://github.com/facebookresearch/detectron2 (дата обращения: 23.11.2023).*
5. *Microsoft COCO: Common Objects in Context arXiv.org: сайт. URL: https://arxiv.org/abs/1405.0312 (дата обращения: 23.11.2023).*
6. *Note on the Inception Score. arXiv.org: сайт. URL: https://arxiv.org/abs/1801.01973 (дата обращения: 23.11.2023).*
7. *A. Mittal, A. K. Moorthy, A. C. Bovik. No-Reference Image Quality Assessment in the Spatial Domain. / Transactions on Image Processing. 2012. № 21 (12). С. 4695-4708.*
8. *B. Schölkopf, A. J. Smola, R. C. Williamson, P. L. Bartlett Multiscale skewed heavy-tailed model for texture analysis. / Neural Computю 2000. № 12 (5) С. 1207– 1245.*