ОПРЕДЕЛЕНИЕ ПОДЛИННОСТИ БАНКНОТ НА ОСНОВЕ АНАЛИЗА ИЗОБРАЖЕНИЙ ДЛЯ СМАРТФОНА

Ю.Б. Блохинов[1], А.В. Бондаренко[1], В.А. Горбачев[1], С.Ю. Желтов[1], Ю.О. Ракутин[1]
[1]Государственный научно-исследовательский институт авиационных систем, Государственный научный центр Российской Федерации (ГНЦ ФГУП «Гос НИИАС»), Москва, Россия

Аннотация

Разработана технология определения подлинности банкнот по цифровому снимку для серийных смартфонов. Данная технология не требует разработки и внедрения в изделие новых защитных графических элементов и основана на применении цифровых методов анализа и обработки изображений, позволяющих выявлять и анализировать тонкие детали патернов, и на основе этого анализа классифицировать образец как оригинал или имитацию. Особенность предлагаемого подхода связана с построением набора признаков для каждого типа образцов и последующей их классификацией с машинным обучением на основе обучающей выборки. Метод реализован в виде законченного приложения для смартфона, выполняющего автоматически детектирование объекта в кадре, съемку образца камерой при попадании его в область захвата, отбраковку некорректных снимков, определение номинала и модификации банкноты и собственно определение ее подлинности.

Ключевые слова: цифровая обработка изображений, анализ изображений, распознавание образов, банкнота, имитация, смартфон, идентификация, аутентификация, набор признаков, классификация с обучением.

Цитирование: **Блохинов, Ю.Б.** Определение подлинности банкнот на основе анализа изображений для смартфона / Ю.Б. Блохинов, А.В. Бондаренко, В.А. Горбачев, С.Ю. Желтов, Ю.О. Ракутин // Компьютерная оптика. – 2017. – Т. 41, № 2. – С. 237-244. – DOI: 10.18287/2412-6179-2017-41-2-237-244.

Введение

Проверка подлинности банкнот является слишком сложной задачей для большинства обычных людей, однако сталкиваться с данной проблемой так или иначе приходится каждому. При этом специализированные средства проверки денежных купюр, паспортов и других документов по понятным причинам имеются только в достаточно крупных торговых организациях и на проверочно-пропускных пунктах и не являются общедоступными. В то же время исключительно распространенными устройствами в настоящее время являются смартфоны, доступные абсолютному большинству граждан. Современные смартфоны обладают развитой операционной системой, открытой для разработки программного обеспечения сторонними разработчиками, а также фотокамерами и дисплеями достаточно высокого разрешения. Поэтому весьма перспективной выглядит идея анализировать защитный комплекс купюр и документов при помощи смартфона с установленным на нем специализированным программным обеспечением (ПО, приложение). В течение последних лет появились работы, в которых авторы предлагают различные подходы для решения данной задачи, однако такие попытки немногочисленны [1 – 7].

Разработанная авторами оригинальная технология анализа цифрового снимка печатного оттиска для смартфона включает в себя выделение зон интереса, формирование набора признаков для каждой из зон, идентификацию образца и его последующую аутентификацию на основе машинно-обучаемых классификаторов. В качестве тестируемых оттисков были использованы купюры номиналов 1000 и 5000 российских рублей в модификациях 1997-го и 2010-го годов и соответствующие их имитации, сделанные на доступных принтерах фирм CANON, EPSON, XEROX и HP. Производилась обработка цифровых изображений оттисков оборотной стороны купюр, выполненных смартфоном Samsung Galaxy S6. Все представленные алгоритмы проектировались для процессора этого смартфона, который по многим характеристикам на сегодня заметно уступает среднему ПК. Данное ограничение в условиях требований работы в режиме почти реального времени накладывает чрезвычайно жесткие требования на состав алгоритмов, включенных в финальное решение.

Функционально полное решение данной задачи было разработано и опубликовано авторами в работах [8, 9]. Однако предложенное в них решение не отвечает требованиям, предъявляемым к рабочему варианту технологии, поскольку точность классификации образцов недостаточно высока, а общее время работы алгоритмов превышает допустимое более чем на порядок. Создание рабочей версии технологии для смартфона Samsung Galaxy S6 потребовало разработки ее практически заново, включая и формирование новой обучающей базы изображений. В настоящей статье представлено полное аппаратно-алгоритмическое решение задачи, позволяющее одновременно поддерживать высокие показатели точности классификации образцов и малое время выполнения всех вычислительных процессов.

1. Особенности технологии для смартфона

Особенности проектируемого программного приложения определяются функциональными и пользовательскими требованиями, связанными с его эксплу-

атацией. Для программы определения подлинности банкнот определяющими являются два обстоятельства: 1) приложение производит анализ *тонких* деталей цифрового изображения, сделанного камерой смартфона, 2) время работы приложения должно составлять не более 10 с, в противном случае реальный интерес к нему значительно снижается. Второе означает, что требования по быстродействию ко всем используемым алгоритмам очень высоки. Условие трудное, но абсолютно ясное. Первое значительно сложнее, поскольку результат анализа *тонких* деталей зависит от различных факторов, таких как качество снимка, его чёткость, размер и положение купюры в кадре, точность позиционирования ее фрагментов. По небрежно сделанному снимку невозможно получить надёжные результаты. Поэтому приложение проектировалось так, чтобы автоматизировать весь цикл обработки и исключить возможность ошибки на каждом этапе. Это означает полный контроль самого процесса съёмки образца, проверку корректности снимка, распознавание типа образца и определение его подлинности по полученному изображению. Для успешного выполнения основной задачи в приложении реализованы следующие функции:

– детектирование и анализ образца,
– контроль в кадре положения образца перед камерой,
– автоматическая съёмка при достижении захвата образца,
– проверка корректности снимка,
– определение номинала и модификации банкноты,
– определение подлинности банкноты.

Каждая из перечисленных функций требует разработки оригинальных алгоритмов, описанию которых и посвящена главным образом данная статья.

2. Описание алгоритмов

2.1. Детектирование и анализ образца на изображении

Программа начинает работу с анализа экранного изображения смартфона, проверки наличия на нем объекта и последующей проверки того, что объект является банкнотой одного из четырех заданных типов (рис. 1). Для того чтобы определять, имеются ли в кадре эти объекты и только они, разработан оригинальный алгоритм детектирования на основе метода Виолы–Джонса [10].

Детектор Виолы–Джонса имеет вид каскада решающих деревьев, использующих признаки Хаара [11]. Его структура определяется в процессе настройки на обучающей выборке методом AdaBoost [12]. Обучающая выборка должна содержать набор изображений – «позитивов», на которых присутствует объект, и набор изображений – «негативов», на которых объект отсутствует.

В рамках алгоритма детектирования было обучено два детектора – для банкнот номиналов 1000 и 5000 рублей. В качестве набора позитивных примеров была использована обширная коллекция снимков оригинальных банкнот и их имитаций.

Рис. 1. Примеры некорректных объектов в кадре

В качестве набора негативных примеров была использована коллекция изображений других банкнот Российской Федерации и банкнот стран мира, а также коллекция различных фоновых изображений.

Благодаря эффективной структуре детектора Виолы–Джонса и простоте используемых им признаков (рис. 2), удалось добиться высокой производительности детектирования. На смартфоне Galaxy S6 по превью-изображению камеры (разрешение 720 p) возможно последовательно запускать детекторы для каждого из рассматриваемых типов банкнот 27 раз в секунду.

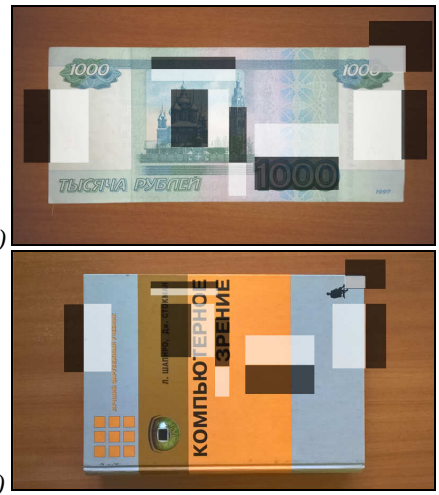

Рис. 2. Иллюстрация признаков Хаара

2.2. Автоматическая съёмка банкноты

После детектирования банкноты автоматически производится ее фотографирование, что позволяет избежать возможных вибраций камеры при съёмке. Для корректности дальнейшей обработки снимков

необходимо, чтобы банкнота полностью помещалась в кадр, плоскость снимка была параллельна плоскости банкноты, края банкноты были расположены параллельно краям кадра, размер банкноты в кадре был заданного размера. Выполнение этих требований проверяется ещё до выполнения съёмки, при помощи анализа превью-изображения камеры смартфона (рис. 3).

Рис. 3. Пример неправильного расположения банкноты

Для проверки корректности положения используется оригинальный метод детектирования угловых точек банкноты, использующий анализ кумулятивных гистограмм $S_x(y)$, $S_y(x)$ (то есть сумм яркостей по столбцам и строкам изображения):

$$S_x(y)=\sum_{x=1}^{W} I(x,y), S_y(x)=\sum_{y=1}^{H} I(x,y),$$

где I – полутоновое изображение.

Предполагается, что банкнота фотографируется на контрастном фоне и её можно приближённо представить как светлый прямоугольник на тёмном фоне, параллельный краям кадра. В этом случае сумма значений яркостей по столбцу и строке изображения будет иметь существенный скачок в угловой точке банкноты (рис. 4):

$$y^*=\underset{y\in[N,H-N]}{\operatorname{argmax}}\left(\sum_{i=y}^{y+N} S_x(i)-\sum_{j=y-N}^{y} S_x(j)\right),$$

$$x^*=\underset{x\in[N,W-N]}{\arg\max}\left(\sum_{i=x}^{x+N} S_x(i)-\sum_{j=x-N}^{x} S_x(j)\right),$$

где (x^*, y^*) – координаты уголковой точки, N – апертура усреднения, которая определяет сглаживание гистограммы перед поиском максимального скачка (подбирается вручную), H, W – размеры изображения.

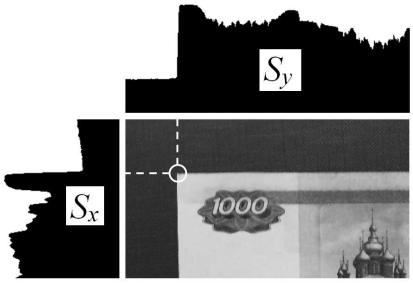

Рис. 4. Поиск угловой точки с помощью кумулятивных гистограмм. Слева и сверху – графики сумм яркостей по столбцам и строкам фрагмента изображения

Для того чтобы определить положение всех четырёх угловых точек банкноты, изображение разбивается на четыре равные части, в каждой из которых ищется угловая точка. Ясно, что при отклонении ориентации сторон банкноты от параллельного осям координат данный метод будет давать ошибку. Однако при малых отклонениях ошибка мала, а для больших отклонений точное значение угла не важно, так как фиксируется только сам факт отклонения и блокируется спуск камеры устройства.

Данный метод в силу простоты реализации позволяет определять положение банкноты на превью-изображении как минимум 25 раз в секунду. По определённым координатам угловых точек вычисляются параметры ориентации банкноты и контролируется выполнение указанных выше требований (рис. 5). При корректном положении банкноты включается подсветка на смартфоне и производится снимок. При этом анимация на экране в виде пузырька помогает пользователю держать смартфон горизонтально.

Рис. 5. Результат сегментации

2.3. Проверка корректности снимка

Несмотря на все перечисленные выше меры контроля съёмки, снимок может получиться некорректным. Фокусировка и выполнение снимка камерой занимает определённое время, на протяжении которого пользователь может сместить смартфон или случайно дёрнуться. Кроме того, в процессе фокусировки камеры визуальный размер банкноты в кадре несколько изменяется. Поэтому полученный снимок снова анализируется. На нём выделяются угловые точки банкноты, и проверяется её положение на изображении. В случае, если положение некорректно, на экран выводится сообщение о необходимости повторной съемки банкноты (рис. 6).

Рис. 6. Пример некорректного снимка, угол банкноты находится за пределами кадра

2.4. Определение номинала банкноты

Для дальнейшей обработки на этом этапе необходимо знать тип банкноты. В отличие от [8] в данной работе тип определяется еще на этапе детектирования по экранному изображению. При этом последовательно применяется несколько детекторов, каждый из которых обучен распознавать только один конкретный тип образцов и обладает высокой избирательно-

стью. После того как один из детекторов банкноты сработал, тип банкноты становится известен ещё до момента фотографирования.

2.5. Определение модификации банкноты

В Российской Федерации в обращении находятся одновременно различные модификации банкнот 1000 и 5000 рублей, которые различаются как расположением, так и дизайном защитных элементов. Поэтому для анализа подлинности банкнот различных модификаций используются отличающиеся алгоритмы. Для определения модификации банкнот перед определением их подлинности применяется оригинальный метод, основанный на вычислении набора признаков Хаара [11] и машинном обучении. Признаки Хаара позволяют количественно описать смещение элементов дизайна банкнот и отличия в относительной яркости текстур. Величина признака представляет собой разность сумм яркостей пикселей изображения в двух смежных прямоугольниках. В частности, признак Хаара для вертикально-ориентированной маски вычисляется следующим образом:

$$F(x,y)=\sum_{\xi=1}^{w}\sum_{\eta=1}^{h}I(x+\xi,y+\eta)-\sum_{\xi=1}^{w}\sum_{\eta=1}^{h}I(x+\xi,y+\eta+h),$$

где I – полутоновое изображение; h, w – размеры прямоугольников.

Набор областей, по которым вычисляются признаки Хаара, сформирован на основе анализа различий плотности заполнения участков банкнот различных модификаций (рис. 7).

Рис. 7. Зоны вычисления признаков Хаара для различения модификаций

По отдельности такие признаки не позволяют надёжно отличить модификации, так как при печати банкнот допускается определённое смещение их элементов. Поэтому, для того чтобы принимать решение по совокупности набора откликов различных признаков, на коллекции примеров необходимо производить обучение классификатора, использующего все выбранные признаки. В качестве классификатора используется композиция решающих деревьев, построенная методом градиентного бустинга (GBT) [13].

2.6. Определение подлинности банкноты

После определения номинала и модификации производится проверка подлинности банкноты с помощью алгоритмов, специфичных для данного типа образцов. В работе [9] для анализа изображений банкнот вводится ряд признаков, позволяющих отличить оригинальные купюры от принтерных имитаций. Признаки строятся на основе характеристик Фурье-спектра [14], откликов фильтра Гаусса, Лапласа [15], операторов интереса (в частности, Харриса [16]), функции автокорреляции, морфологических операций. Они вычисляются для семи различных областей интереса на изображении банкноты. Области интереса выбираются экспертным способом отдельно для каждого типа банкноты на основе наличия в них рисунков или символов, которые не могут быть точно воспроизведены при печати на цифровых печатающих устройствах. В их составе области микротекста, микроузоры, элементы центральной части банкноты с рисунком, выполненным тонкими линиями различного направления. Всего для каждой банкноты берется суммарно 56 различных численных признаков.

В качестве метода обучения классификатора используется *градиентный бустинг* [13] над решающими деревьями. Данный метод не требует нормировки признаков, устойчив к мультиколлинеарности признаков (в отличие от линейных методов), менее склонен к переобучению. Основная идея градиентного бустинга заключается в построении композиционного классификатора в виде взвешенного голосования (линейной комбинации) нескольких базовых алгоритмов:

$$a(x)=\operatorname{sign}\left(F_m(x)\right)=\operatorname{sign}\left(\sum_{i=1}^{N}\alpha_m b(x,\theta_m)\right),$$

где F_m – композиция, состоящая из m отдельных классификаторов, b – решающее дерево с параметрами θ_m.

При этом классификатор строится таким образом, чтобы достичь минимума функционала ошибки Q. Его минимизация производится итеративно методом градиентного спуска:

$$F_m(x)=F_{m-1}(x)-\alpha_m\nabla Q.$$

Для этого на каждой итерации обучается новый классификатор, оптимально приближающий вектор антиградиента функционала ошибки, и добавляется к линейной комбинации:

$$F_m(x)=F_{m-1}(x)+\alpha_m b(x,\theta_m).$$

Коэффициент α_m подбирается из условия одномерной оптимизации функционала ошибки.

2.7. Отбор признаков

Вычисление полного набора признаков требует значительного времени при выполнении задачи на смартфоне. Поэтому в целях повышения производительности программы из общего набора было выбрано подмножество из 16 признаков. Критерием выбора подмножества признаков являлась точность классификатора, обученного на этом подмножестве. Точность классификатора вычислялась методом перекрёстной проверки (кросс-валидации). Полный перебор всех возможных подмножеств признаков размера 16 потребовал бы $C_{56}^{16}\approx 4\cdot 10^{13}$ $C_{56}^{16}\approx 4\cdot 10^{13}$циклов обучения и тестирования классификатора, что неприемлемо для практики. Поскольку для каждого отдельного признака затруднительно заранее оценить

его информативность (по отдельности ни один признак не позволяет разделить выборку), то для выбора подмножества признаков был применён метод последовательного добавления и удаления [17]. На шаге добавления к подмножеству последовательно добавляется один не включённый в него признак, производится обучение классификатора на этом наборе и замеряется его точность. К подмножеству добавляется тот признак, при добавлении которого точность максимальна. На шаге удаления из подмножества последовательно удаляется один из его элементов, производится обучение классификатора на этом наборе и замеряется его точность. Из множества удалялся тот элемент, при удалении которого точность классификации снижается минимально. Сравнение точностей классификации на полном наборе признаков и на отобранном приведено в табл. 1.

Табл. 1. Точность классификации при эффективном сокращении числа признаков

	Имитации		**Оригиналы**	
Кол-во призн.	**16**	**56**	**16**	**56**
1000 р. 2004 г.	99,78%	99,96%	99,59%	99,80%
1000 р. 2010 г.	99,92%	99,94%	99,92%	99,91%
5000 р. 1999 г.	99,40%	99,96%	99,77%	99,85%
5000 р. 2010 г.	99,75%	99,80%	99,73%	99,77%
В среднем	99,71%	99,91%	99,75%	99,83%

Как видно из табл. 1, в результате применения метода последовательного добавления и удаления удалось добиться существенного сокращения числа признаков при незначительном снижении точности классификации.

3. Эксперименты

Для обучения классификаторов модификации и подлинности банкнот была создана база изображений, включающая около 64000 различных снимков подлинных купюр и принтерных имитаций четырёх типов купюр (два номинала, две модификации каждого номинала). Такой большой объём обучающих примеров необходим из-за большой вариативности данных, обусловленной разнообразными условиями съёмки, различиями камер, которыми производится съёмка, а также способами изготовления имитаций банкнот.

Для того чтобы результаты классификации не зависели от способа получения имитации банкноты и степени её изношенности, обучающая выборка формировалась на основе имитаций, полученных различными моделями печатающих устройств основных марок, изъятых из обращения подделок, а также большого набора оригинальных банкнот из обращения. Для того чтобы результат классификации не зависел от конкретного образца камеры смартфона, съёмка образцов производилась несколькими различными аппаратами. Благодаря этому в рамках исследованного модельного семейства (Galaxy S6) была достигнута высокая независимость результатов классификации от конкретного образца смартфона. Всего для каждого из типов банкнот было подготовлено около 16 тысяч обучающих примеров.

Результаты точности опознавания модификаций банкнот представлены в табл. 2.

Табл. 2. Точность распознавания модификаций банкнот

Модификация	**2004 года**	**2010 года**
1000 р.	99,95%	99,94%
5000 р.	99,82%	99,72%

Точность распознавания модификаций банкноты 1000 рублей оказалась выше, чем 5000 рублей, так как различия в их дизайне гораздо более заметные.

Показатели точности классификации подлинности, полученные методом градиентного бустинга на усечённом наборе признаков (GBT), в сравнении с результатами, полученными в статье [9] методом SVM (SVM), приведены в табл. 3. Точность классификации контролировалась по методу перекрёстной проверки (кросс-валидации).

Табл. 3. Точность классификации подлинности

	Имитации		**Оригиналы**	
Тип образца	**GBT**	**SVM**	**GBT**	**SVM**
1000 р. 2004 г.	99,78%	99,73%	99,59%	99,20%
1000 р. 2010 г.	99,92%	97,25%	99,92%	92,63%
5000 р. 1999 г.	99,40%	99,34%	99,77%	93,53%
5000 р. 2010 г.	99,75%	99,89%	99,73%	99,47%
В среднем	99,71%	99,05%	99,75%	96,20%

Сравнение показывает, что при оценке точности на имеющейся выборке полученная модель классификации практически по всем позициям превосходит результаты, полученные в статье [9]. Достигается точность не ниже 99,4 %, что соответствует требованиям, предъявляемым к программным приложениям такого типа.

В результате разработки и внедрения высокоэффективных вычислительных алгоритмов, выбора и редукции пространства признаков, а также за счет использования аппаратной оптимизации общее время работы приложения удалось уменьшить в 10–12 раз по сравнению с [9]. В представленной версии технологии время, затрачиваемое приложением на анализ изображения, составляет 3–5 секунд.

Заключение

Разработана технология определения подлинности банкнот по цифровому снимку, сделанному камерой смартфона Samsung Galaxy S6. Технология реализована в виде законченного приложения для смартфона. Приложение выполняет полный цикл процесса идентификации и аутентификации банкноты: детектирование объекта в кадре, автоматическое выполнение снимка камерой смартфона при попадании объекта в область захвата, отбраковка некорректных снимков, определение номинала и модификации банкноты и собственно определение подлинности банкноты. Технология не требует разработки и внедрения в изделие новых защитных графических элементов и основана на применении цифровых методов анализа и обработки изображений, позволяющих выявлять и анализировать тонкие детали паттернов и на основе этого анализа относить образец к одному из двух классов: оригиналов или имитаций. Особенность предлагаемо-

го подхода связана с построением набора признаков для каждого типа образцов и последующей их классификацией с машинным обучением на основе обучающей выборки [9]. Набор признаков включает в себя ряд показателей, характеризующих качество изображения печатного оттиска на снимке, сделанном камерой смартфона. Для определения подлинности образцов применяется такой эффективный современный подход, как классификация с машинным обучением, в данном случае градиентный бустинг над решающими деревьями (GBT). Программное приложение реализовано на мобильном устройстве Samsung Galaxy S6 под операционной системой Android 6. В процессе проведенных испытаний приложение продемонстрировало на тестовой выборке достаточно высокие показатели как по времени, так и по надежности распознавания предъявленных образцов.

Благодарности

Авторы выражают благодарность руководству и специалистам НИИ филиала ФГУП «Гознак» за участие в постановке технических задач исследования и обсуждение полученных результатов.

Литература

1. **Lohweg, V.** Banknote authentication with mobile devices / V. Lohweg, J.L. Hoffmann, H. Dörksen, R. Hildebrand, E. Gillich, J. Hofmann, J. Schaede // Proceedings of SPIE. – 2013. – Vol. 8665. – 866507. – DOI: 10.1117/12.2001444.
2. **Pat. EP 2000992 A1 G 07 D 7/00, G 07 D 7/20.** Authentication of security documents, in particular of banknotes / V. Lohweg, E. Gillich, J. Schaede; Applicant: Kba-Giori S.A.; No EP20070109470, filed of June 01, 2007, published of December10, 2008, bulletin 2008/50.
3. **Lohweg, V.** Renaissance of intaglio / V. Lohweg // Keesing Journal of Documents & Identity. – 2010. – Issue 33. – P. 35-41.
4. **Lohweg, V.** Document production and verification by optimization of feature platform exploitation / V. Lohweg, J. Schaede // Optical Document Security – The Conference on Optical Security and Counterfeit Detection II. – 2010. – P. 1-15.
5. **Lohweg, V.** Mobile devices for banknote authentication – is it possible? / V. Lohweg, H. Dörksen, E. Gillich, R. Hildebrand, J.L. Hoffmann, J. Schaede // Optical Document Security – The Conference on Optical Security and Counterfeit Detection III. – 2012. – P. 1-15.
6. **Yang, C.-N.** Enhancing privacy and security in RFID-enabled banknotes / C.-N. Yang, J.-R. Chen, C.-Y. Chiu, G.-C. Wu, C.-C. Wu // IEEE International Symposium on Parallel and Distributed Processing with Applications. – 2009. – P. 439-444. – DOI: 10.1109/ISPA.2009.77.
7. **Omatu, S.** Bank note classification using neural networks / S. Omatu, M. Yoshioka, Y. Kosaka // IEEE Conference on Emerging Technologies and Factory Automation. – 2007. – P. 413-417. – DOI: 10.1109/EFTA.2007.4416797.
8. **Блохинов, Ю.Б.** Идентификация образцов защищённой печатной продукции с использованием смартфона / Ю.Б. Блохинов, В.А. Горбачев, Ю.О. Ракутин, В.В. Волков // Вестник компьютерных и информационных технологий. – 2016. – № 3. – С. 11-17. – DOI: 10.14489/vkit.2016.03.pp.011-017.
9. **Блохинов, Ю.Б.** Анализ подлинности образцов защищённой печатной продукции с использованием смартфона / Ю.Б. Блохинов, В.А. Горбачев // Вестник компьютерных и информационных технологий. – 2016. – № 4. – С. 23-29. – DOI: 10.14489/vkit.2016.04.pp.023-029.
10. **Viola, P.A.** Rapid object detection using a boosted cascade of simple features / P.A. Viola, M.J. Jones // Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2001). – 2001. – Vol. 1. – P. 511-518. – DOI: 10.1109/CVPR.2001.990517.
11. **Papageorgiou,C.P.** A general framework for object detection / C.P. Papageorgiou, M. Oren, T. Poggio // Sixth International Conference on Computer Vision. – 1998. – P. 555-562. – DOI: 10.1109/ICCV.1998.710772.
12. **Freund, Y.** A decision-theoretic generalization of on-line learning and an application to boosting / Y. Freund, R.E. Schapire // Computational Learning Theory. EuroCOLT 1995 / ed. by P. Vitányi. – Berlin, Heidelberg: Springer, 1995. – P. 23-37. – DOI: 10.1007/3-540-59119-2_166.
13. **Friedman, J.H**. Greedy function approximation: A gradient boosting machine / J.H. Friedman // The Annals of Statistics. – 2001. – Vol. 29(5). – P. 1189-1232. – DOI: 10.1214/aos/1013203451.
14. **Гонсалес, Р.** Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. – М.: Техносфера, 2005. – 1072 с. – ISBN: 5-94836-028-8.
15. **Шапиро, Л.** Компьютерное зрение / Л. Шапиро, Дж. Стокман; пер. с англ. – М.: БИНОМ, 2006. – 752 с. – ISBN: 5-94774-384-1.
16. **Harris, C.** Combined corner and edge detector / C. Harris, M.A. Stephens // Proceedings of the Alvey Vision Conference. – 1988. – P. 147-151. – DOI: 10.5244/C.2.23.
17. **Molina, L.C.** Feature selection algorithms: A survey and experimental evaluation / L.C. Molina, L. Belanche, A. Nebot // Proceedings of the IEEE International Conference on Data Mining. – 2002. – P. 306-313. – DOI: 10.1109/ICDM.2002.1183917.

Сведения об авторах

Блохинов Юрий Борисович, 1956 года рождения, в 1980 году окончил Московский физико-технический институт по специальности «Динамика полета и управление», в 1990 году защитил кандидатскую диссертацию во ВНИИ Системных исследований, в 2012 году защитил докторскую диссертацию в Московском государственном университете геодезии и картографии (МИИГАиК). Работает начальником лаборатории в ГНЦ ФГУП «Гос НИИАС». Область научных интересов: цифровая фотограмметрия, компьютерное зрение, анализ изображений, распознавание образов. E-mail: *yury.blokhinov@gosniias.ru* .

Бондаренко Александр Викторович, 1953 г.р., в 1976 году окончил Московский физико-технический институт по специальности «Системы автоматического управления», в 1980 году защитил кандидатскую диссертацию в МФТИ, в 2009 году – докторскую диссертацию в ИПМ им. М.В. Келдыша РАН, работает заместителем

генерального директора ГНЦ ФГУП «Гос НИИАС», область научных интересов: информационные системы. E-mail: cod@fgosniias.ru .

Горбачев Вадим Александрович, 1988 года рождения, в 2011 году окончил Московский физико-технический институт (МФТИ (ГУ)) по специальности «Системный анализ, управление и обработка информации», в 2014 году защитил кандидатскую диссертацию в МФТИ (ГУ). Работает начальником сектора в ГНЦ ФГУП «Гос НИИАС». Область научных интересов: компьютерное зрение, машинное обучение, распознавание образов, анализ изображений. E-mail: vadim.gorbachev@gosniias.ru .

Желтов Сергей Юрьевич,1956 года рождения, в 1979 году окончил Московский физико-технический институт по специальности «Системы автоматического управления», в 1984 году защитил кандидатскую диссертацию в МФТИ, в 2002 – докторскую диссертацию в МАИ. Заведует кафедрой автоматического и интеллектуального управления МАИ, работает Генеральным директором ГНЦ ФГУП «Гос НИИАС». Область научных интересов: авиастроение, обработка информации в системах управления. E-mail: zhl@gosniias.ru .

Ракутин Юрий Олегович, 1994 года рождения, в 2015 году окончил бакалавриат Московского физико-технического института по направлению 03.03.01 «Прикладные математика и физика». Учится в магистратуре МФТИ, работает инженером в ГНЦ ФГУП «Гос НИИАС». Область научных интересов: компьютерное зрение, машинное обучение, анализ данных. E-mail: rakutin@phystech.edu .

ГРНТИ: 28.23.15 .
Поступила в редакцию 12 декабря 2016 г. Окончательный вариант – 8 февраля 2017 г.

COUNTERFEIT BILL DETECTION BY IMAGE ANALYSIS FOR SMARTPHONES

Y.B. Blokhinov[1], A.V. Bondarenko[1], V.A. Gorbachev[1], S.Y. Zheltov[1], Y.O. Rakutin[1]
[1]State Research Institute of Aviation Systems, Moscow, Russia

Abstract

A method for counterfeit bill detection based on a digital image for mass-production smartphones is developed. The method under consideration does not require new protective elements to be designed and introduced into the print and is based on the use of digital image analysis and recognition methods, allowing one to carry out an automatic search and verification of known protective elements of the print. The peculiarity of the proposed approach is associated with constructing a feature vector for each type of samples and their subsequent classification using machine learning based on a training sample. The method is realized as a program application for smartphones, performing the automatic detection of an object in the frame, shooting the camera-captured object, rejection of unsuitable images, determination of a face-value and type of the banknote, and finally, verification of the authenticity.

Keywords: digital image processing, image analysis, pattern recognition, banknote, counterfeit, smartphone, identification, authentication, feature vector, learning classification.

Citation: Blokhinov YB, Bondarenko AV, Gorbachev VA, Zheltov SY, Rakutin YO. Counterfeit bill detection by image analysis for smartphones. Computer Optics 2017; 41(2): 237-244. DOI: 10.18287/2412-6179-2017-41-2-237-244.

Acknowledgements: Authors are grateful to a management and specialists of Scientific Research Institute Branch of “GOZNAK” for participation in statement of technical research problems and discussion of the received results.

References

[1] Lohweg V, Hoffmann JL, Dörksen H, Hildebrand R, Gillich E, Hofmann J, Schaede J. Banknote authentication with mobile devices. Proc SPIE 2013; 8665: 866507. DOI: 10.1117/12.2001444.

[2] Lohweg V, Gillich E, Schaede J. Authentication of security documents, in particular of banknotes. Patent EP 2000992 A1 of December 10, 2008, bulletin 2008/50.

[3] Lohweg V. Renaissance of intaglio. Keesing Journal of Documents & Identity 2010; 33: 35-41.

[4] Lohweg V, Schaede J. Document production and verification by optimization of feature platform exploitation. Optical Document Security – The Conference on Optical Security and Counterfeit Detection II 2010: 1-15.

[5] Lohweg V, Dörksen H, Gillich E, Hildebrand R, Hoffmann JL, Schaede J. Mobile devices for banknote authentication – is it possible? Optical Document Security – The Conference on Optical Security and Counterfeit Detection III 2012: 1-15.

[6] Yang C-N, Chen J-R, Chiu C-Y, Wu G-C, Wu C-C. Enhancing privacy and security in RFID-enabled banknotes. IEEE International Symposium on Parallel and Distributed Processing with Applications 2009: 439-444. DOI: 10.1109/ISPA.2009.77.

[7] Omatu S, Yoshioka M, Kosaka Y. Bank note classification using neural networks. IEEE Conference on Emerging

Technologies and Factory Automation 2007: 413-417. DOI: 10.1109/EFTA.2007.4416797.
[8] Blokhinov YB, Gorbachev VA, Rakutin YO, Volkov VV. Identification of samples of the protected printed materials with use of the smartphone. Vestnik Komp'iuternykh i Informatsionnykh Tekhnologii 2016; 3: 11-17. DOI: 10.14489/vkit.2016.03.pp.011-017.
[9] Blokhinov YB, Gorbachev VA. The authenticity analysis of samples of the protected printed materials with use of the smartphone. Vestnik komp'iuternykh informatsionnykh tekhnologii 2016; 4: 23-30. DOI: 10.14489/vkit.2016.04.pp.023-029.
[10] Viola P, Jones MJ. Rapid object detection using a boosted cascade of simple features. Proc CVPR 2001; 1: 511-518. DOI: 10.1109/CVPR.2001. 990517.
[11] Papageorgiou CP, Oren M, Poggio T. A general framework for object detection. ICCV 1998: 555-562. DOI: 10.1109/ICCV.1998.710772.
[12] Freund Y, Schapire RE. A decision-theoretic generalization of on-line learning and an application to boosting. In: Vitányi P, ed. Computational Learning Theory. EuroCOLT 1995. Berlin, Heidelberg: Springer; 1995: 23-37. DOI: 10.1007/3-540-59119-2_166.
[13] Friedman JH. Greedy function approximation: A gradient boosting machine. The Annals of Statistics 2001; 29(5): 1189-1232. DOI: 10.1214/aos/1013203451.
[14] Gonsales R, Woods R. Digital image processing. 3rd ed. Upper Saddle River, NJ: Pearson Education, Inc., 2008. ISBN: 978-0-13-168728-8.
[15] Shapiro LG, Stockman JC. Computer vision. Seattle, Washington: Pearson; 2001. ISBN: 978-0-13-030796-5.
[16] Harris C, Stephens MA. Combined corner and edge detector. Proc Alvey Vision Conference 1988: 147-151. DOI: 10.5244/C.2.23.
[17] Molina LC, Belanche L, Nebot A. Feature selection algorithms: A survey and experimental evaluation. Proc ICDM 2002: 306-313. DOI: 10.1109/ICDM.2002.1183917.

Authors' information

Yury Borisovich Blokhinov (b. 1956) graduated from Moscow Institute of Physics and Technology in 1980 in the speciality "Space Flight Dynamics and Control". In 1990 he defended his PhD thesis in the State Research Institute of System Analysis, in 2012 he defended his DE thesis in Moscow State University of Geodesy and Cartography. He works as head of the laboratory in State Research Institute of Aviation Systems. His research interests currently are digital photogrammetry, computer vision, image analysis, pattern recognition. E-mail: *yury.blokhinov@gosniias.ru* .

Alexander Victorovich Bondarenko (b. 1953) graduated from Moscow Institute of Physics and Technology (MIPT) in 1976. Specialization: "Automatic Control Systems". In 1980 defended his PhD thesis in MIPT. In 2009 defended his DE thesis in the Keldysh Institute of Applied Mathematics (Russian Academy of Sciences). At present Deputy Director General of State Research Institute of Aviation Systems (State Scientific Centre of Russian Federation) FGUP "GosNIIAS". Area of job interests: information systems. E-mail: *cod@fgosniias.ru* .

Vadim Aleksandrovich Gorbachev, born in 1988, graduated from the Moscow Institute of Physics and Technology (MIPT (SU)) in 2011, in the specialty "System Analysis, Control and Information Processing". In 2014 he defended his PhD thesis at MIPT. He works as head of sector at the FSUE State Research Institute of Aviation Systems (SSC of RF). Research interests: computer vision, machine learning, pattern recognition, image analysis. E-mail: *vadim.gorbachev@gosniias.ru* .

Sergey Yurievich Zheltov (b. 1956) graduated from Moscow Institute of Physics and Technology (MIPT) in 1979 in the speciality "Automatic Control Systems". In 1984 he defended his PhD thesis in the MIPT, in 2002 he defended his DE thesis in the Moscow Aviation Institute. Correspondent member of Russian Academy of Science (RAS) from 2006. He works as director general of State Research Institute of Aviation Systems. His research interests currently are new avionics technologies, information processing in modern control systems, computer vision, and image analysis. E-mail: *zhl@gosniias.ru* .

Yury Olegovich Rakutin (b. 1994) got the Bachelor's degree in "Applied Mathematics and Physics" in Moscow Institute of Physics and Technology in 2015. He receives the Master's degree in Moscow Institute of Physics and Technology and works as an engineer in State Research Institute of Aviation Systems. His research interests currently are computer vision, machine learning, and data analysis. E-mail: *rakutin@phystech.edu* .

Received December 12, 2016. The final version – February 8, 2017.