СЕНСОРНЫЕ СИСТЕМЫ, 2019, том 33, № 2, с. 142–156

ТЕХНИЧЕСКОЕ ЗРЕНИЕ И РАСПОЗНАВАНИЕ ОБРАЗОВ

УДК 004.93

ИСПОЛЬЗОВАНИЕ МОБИЛЬНЫХ УСТРОЙСТВ ДЛЯ ВЫЯВЛЕНИЯ ПРИЗНАКОВ ФАБРИКАЦИИ ДОКУМЕНТОВ, УДОСТОВЕРЯЮЩИХ ЛИЧНОСТЬ

© 2019 г. Д. В. Полевой[1,2,3,*]

[1]Федеральное государственное учреждение "Федеральный исследовательский центр "Информатика и управление" Российской академии наук", 19333 Москва, ул. Вавилова, д. 44, корп. 2, Россия

[2]Федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский технологический университет "МИСиС" 119991 Москва, Ленинский проспект, д. 4, Россия

[3]SmartEnginesLtd., 117312 Москва, проспект 60-летия Октября, д. 9, Россия

**E-mail: dvpsun@gmail.com*

Поступила в редакцию 23.11.2018 г.

Вместе с повышающимся интересом к использованию изображений документов, удостоверяющих личность, в процессах регистрации и обеспечении доступа пользователей мобильных сервисов к услугам, растут и риски потерь от мошеннических действий при использовании технологий такого рода. В настоящей работе рассматриваются подходы и методы решения актуальной проблемы выявления фабрикации документов непосредственно на мобильных устройствах с учетом слабо контролируемых условий получения изображений и особенностей документов, удостоверяющих личность.

Ключевые слова: выявление подделок документов, распознавание изображений документов, обработка изображений, мобильное устройство, смартфон, удостоверение личности, идентификация

DOI: 10.1134/S0235009219020070

ВВЕДЕНИЕ

Повышение интереса к финансовым технологиям является общемировой тенденцией (Gaia et al., 2018), при этом имеется большой потенциал дальнейшего роста (ЦБ РФ, 2018) доли цифровых финансовых услуг:

– инвестиции в финтех-компании в 2016 г. составили 24.7 млрд долларов США (за первое полугодие 2017 г. – 11.6 млрд долларов США), что в 2 раза выше уровня 2013 г. и свидетельствует о высоких темпах роста финтех-индустрии;

– 56% финансовых организаций включили цифровую трансформацию в основу стратегии своего бизнеса;

– к 2020 г. 35–50% клиентов банков будут пользователями мобильного банка.

По мере расширения проникновения цифровых технологий в бизнес-процессы растет и уровень цифрового мошенничества. По оценкам Ассоциации страховщиков России (Герасимов, 2017) каждый сотый страховой случай может быть фальшивым, при этом за год раскрывается примерно две сотни махинаций по ОСАГО и КАСКО на сумму 15 млн рублей. По оценкам сотрудников Национального бюро кредитных историй (НБКИ, 2016) ежегодно кредиторы теряют от действий кредитных мошенников 50–70 млрд рублей.

Получение изображений и распознавание документов при помощи мобильного устройства используются для организации дистанционного доступа к услугам и сервисам (Winarski, 2016; Арлазаров и др., 2016; Cook, 2017). Максимальная защита персональных данных при этом обеспечивается распознаванием реквизитов документов на устройстве без передачи изображений на удаленные сервера (Арлазаров и др., 2016). Разработка и внедрение мобильных технологий контроля подлинности предъявляемых пользователем документов позволят уменьшить потери от мошеннических действий.

РАСПОЗНАВАНИЕ ДОКУМЕНТОВ, УДОСТОВЕРЯЮЩИХ ЛИЧНОСТЬ, НА МОБИЛЬНЫХ УСТРОЙСТВАХ

Понятие "удостоверение личности" или "документ, удостоверяющий личность" (ДУЛ) не имеет однозначного определения в законодательстве РФ, однако существует ряд нормативных актов, определяющих конкретные перечни доку-

ментов, которые в той или иной ситуации могут использоваться для удостоверения личности владельца документа (КонсультантПлюс, 2018). Наиболее распространенными и часто используемыми являются паспорт гражданина РФ, водительское удостоверение, удостоверение личности военнослужащего РФ, военный билет, паспорт гражданина РФ, удостоверяющий личность гражданина РФ за пределами территории РФ, паспорт моряка (удостоверение личности моряка).

Технологии защиты документов, удостоверяющих личность

Документы, удостоверяющие личность, могут быть подразделены на подлинные и подложные. Подлинные документы изготовлены надлежащей государственной службой и содержат соответствующие действительности сведения. Содержание или реквизиты подложных документов не соответствуют действительности. Фабрикацией документа далее будет называться материальный подлог (подделка), который состоит в изменении содержания подлинного документа в результате внесения в него ложных сведений или путем полного изготовления поддельного документа. При полной подделке документ воспроизводится целиком с подражанием подлинному образцу. Частичная подделка осуществляется путем изменения отдельных реквизитов подлинного документа. Помимо подделки ДУЛ, при использовании для получения изображений документов малоформатных цифровых камер возможно предъявление не физического документа, а его изображения на экране монитора, смартфона или планшета. По отношению к документам этот тип атак не описан в литературе, но он хорошо известен разработчикам биометрических систем (Boulkenafet et al., 2017) под названием “повторное воспроизведение” (replay attack).

Документы, удостоверяющие личность, относятся к защищенной полиграфической продукции утвержденной формы единого образца, нормативное определение которой содержится в ГОСТ Р 54109-2010 (ГОСТ, 2011). Согласно работе (Вашкевич и др., 2017) “защита документов от подделки представляет собой комплекс защитных элементов, вносимых в документ при его изготовлении с целью предотвращения фальсификации и облегчения диагностики подделки”. Рассмотрим далее особенности ДУЛ, которые могут наблюдаться и использоваться для выявления фабрикации при съемке в фото или видеорежиме штатной камерой мобильного устройства в обычных условиях.

Обязательным (ГОСТ, 2011) элементом полиграфической защиты документов является использование в качестве графических элементов документа нескольких гильошировых рисунков. Каждый такой рисунок представляется комбинацией тонких образующих периодические узоры в соответствии с определенными математическими закономерностями и взаимно пересекающихся линий. Гильошировые рисунки могут формировать фоновые сетки, розетты, бордюры, виньетки, уголки. Часто комбинируют наложение нескольких рисунков такого рода. Дополнительным элементом защиты является использование орловской и/или ирисовой печати. Защитный эффект последней заключается в трудновоспроизводимом плавном изменении цвета в одном направлении в графических элементах без разрывов, наложения и смещения линий или границ графических элементов как с одинарным, так и с двойным красочным переходом. Номера документов в защищенной полиграфической продукции печатаются способом высокой печати, причем знаки серийного номера выполняются специальными нумераторами с гарнитурой шрифтов, отличающейся от гарнитуры, применяемой в общей полиграфии.

Современные ДУЛ могут содержать машиносчитываемую зону (МСЗ), а соблюдение стандартов (правил) исполнения МСЗ является одним из признаков подлинности документа. МСЗ – зона установленного размера, выделенная на странице данных и содержащая обязательные и дополнительные данные, сформатированные для машинного считывания с применением методов оптического распознавания текста. Если документ используется для пересечения границ, то МСЗ должна соответствовать международным рекомендациям, представленным в документе Doc 9303 Международной организации гражданской авиации (International Civil Aviation Organization, ICAO). Примером изготовленного в соответствии с данными рекомендациями документа является паспорт гражданина РФ, удостоверяющий личность гражданина РФ за пределами РФ. МСЗ национальных ДУЛ могут выполняться с отклонениями от международных рекомендаций, но в соответствии с национальным законодательством (примером последнего служит паспорт гражданина РФ).

Данные в МСЗ должны быть набраны прописными буквами (верхний регистр) латинского алфавита и цифрами 0123456789 знаками одного типоразмера шрифта OCR-B со штрихом постоянной толщины. Печать текста в МСЗ, согласно ICAO 9303, должна быть визуально разборчивой и иметь черный цвет (на длинах волн B425–B680 согласно стандарту ИСО 1831), а так же краска должна хорошо поглощать в ближней части инфракрасного диапазона (диапазоне B900 в соответствии со стандартом ИСО 1831). Никакие защитные слои не должны отрицательно влиять на это свойство. Требования к контрастности налагаются только для инфракрасной области спек-

Рис. 1. Примеры фрагментов изображений машиносчитываемых зон с “плотным” в оптическом диапазоне фоновым заполнением (цит. по Булатов и др., 2015).

трального диапазона, что на практике приводит к тому, что при формальном соблюдении стандарта некоторые страны используют для печати фонового заполнения машиносчитываемой зоны “прозрачные” в инфракрасном диапазоне краски, которые в то же время довольно “плотны” в оптическом. Примеры фрагментов изображений таких зон представлены на рис. 1.

Распространенным и доступным для визуального наблюдения элементом защиты документов являются защитные голограммы (ЗГ). Под ЗГ понимается “выполненная на тонкопленочном полимерном носителе специализированная голограмма, восстанавливающая в белом свете видимые изображения (с многочисленными особыми эффектами объемности, движения, изменения цвета) и содержащая скрытые изображения (микротексты, микролинзы), позволяющие значительно повысить степень защищенности как хранящейся в ней информации, так и самой голограммы” (Одиноков, 2013). ЗГ являются оптически изменяемыми элементами (Optically Variable Device). При перемене угла освещения происходит замещение изображений, которые бывают однопозиционными объемными (голограммы) или многопозиционными (кинеграммы).

Для предохранения бумажных страниц документов от механических повреждений и повышения срока службы на часть страницы или на всю страницу может наноситься прозрачная полимерная пленка – ламинат. Также ламинат используется для защиты документа от изменения первоначального содержания. Например, на внутренней стороне ламината страницы паспорта гражданина РФ содержатся изображения, часть которых находится в месте расположения фотографии владельца, другая часть на бланке. При отделении ламината от бланка и попытке замены фотографии, фрагменты рисунка с ламината должны оставаться на первоначальной фотографии. Признаки нарушения целостности рисунка по ламинату или дорисовка, допечатка рисунка другим способом печати могут свидетельствовать о замене фотографии.

Для повышения степени защищенности ДУЛ в последние годы активно идет переход с бумажных документов на пластиковые. Страница поликарбонатного (пластикового) документа представляет собой пакет, состоящий из пластиковых слоев: основа (может содержать микросхему), полиграфические слои для печати изображений, ламинационные (внешние) для защиты от внешних воздействий. Реквизиты документа, в том числе изображение владельца, не печатаются на поверхности поликарбоната, а внедряются внутрь материала способом лазерного гравирования и перфорирования. Использование линзового растра позволяет добиться эффекта изменения изображения страницы пластикового документа в зависимости от угла наблюдения. Примером такого документа является страница с персональной информацией паспорта гражданина РФ, удостоверяющего личность гражданина РФ за пределами РФ.

Особенности получения изображений документов малоформатными цифровыми камерами

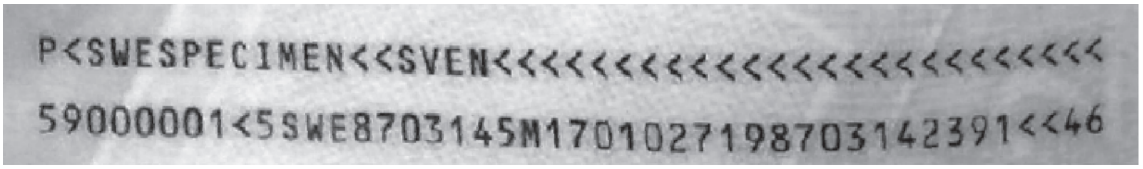
При съемке для распознавания защищенных документов мобильными устройствами возникают типичные для съемки малоформатными цифровыми камерами проблемы (Арлазаров и др., 2014; Булатов и др., 2015; Полевой и др., 2016). Оптическая система камеры искажает изображение из-за аберраций, бликов и внутренних отражений. При использовании фотосенсоров (матриц) и аналоговой электроники для регистрации изображений появляется так называемый цифровой шум. Еще один источник искажений – алгоритмы сжатия изображений, что особенно заметно для кадров видеопотока. Неточность фокусировки камеры или смещение камеры относительно документа во время экспозиции приводит к “размытию” или “смазыванию” изображения. В зависимости от взаимного положения камеры и документа происходит проективное искажение изображения документа, примеры которого представлены на рис. 2.

В общем случае перед распознаванием документа оцениваются параметры проективного базиса и осуществляется проективное исправление изображения зоны документа. Ошибки в опреде-

а *б*

Рис. 2. Примеры слабого – *а* и сильного – *б* проективного искажения изображения документа (цит. по Арлазаров и др., 2014).

а



б

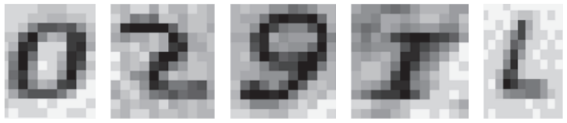


Рис. 3. Примеры результатов проективной нормализации зоны документа при наличии деформации страниц исходного документа для строк – *а* и отдельных символов – *б* (цит. по Арлазаров и др., 2014).

лении параметров проективного исправления приводят к геометрическим искажениям изображения документа. Другим источником искажений изображений документа является комбинирование механической деформации страницы исходного физического документа с проективным искажением. В результате даже после правильной проективной нормализации всего документа искаженными могут оставаться как строки, так и отдельные символы. Примеры искаженных изображений представлены на рис. 3.

Малоформатные цифровые камеры мобильных устройств производят съемку документов в оптическом диапазоне, поэтому неоднородный фон самого документа существенно усложняет процесс оптического распознавания значений реквизитов особенно в условиях “неудачного” освещения. Защитные пленки на страницах ДУЛ обладают хорошими отражающими свойствами, что часто приводит к появлению бликов в зонах реквизитов. “Переливы” ЗГ тоже искажают изображение документа. Примеры искажений такого типа представлены на рис. 4. Защитные элементы вносят дополнительные искажения и мешают работе систем оптического распознавания текста. Однако именно анализ таких искажений (или их отсутствия) позволяет подтверждать соответствующие признаки подлинности ДУЛ.

Использование мобильных устройств для распознавания документов

Краткий обзор и сравнение коммерческих SDK для распознавания ДУЛ на мобильных устройствах представлены в работе (Vironit, 2018). Более подробно дизайн и особенности внутренней реализации системы распознавания ДУЛ для использования в мобильных телефонах и планшетах с использованием вычислительных возможностей самого устройства рассматриваются в работах (Bulatov et al., 2017; Арлазаров и др., 2018а). В связи с неконтролируемыми условиями съемки, распознавание защищенных документов

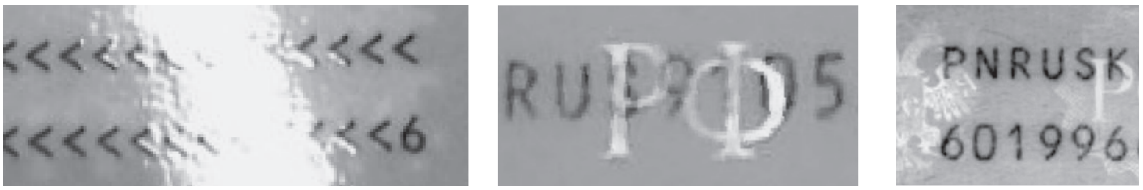


Рис. 4. Примеры искажений изображения документа в связи с защитным покрытием страниц документов (цит. по Арлазаров и др., 2014).

на мобильном устройстве с использованием кадров видеопотока (Bulatov et al., 2017) предпочтительней распознавания на основе одного изображения (кадра) (Wang et al., 2014). Поскольку при этом скорость захвата изображений камерой обычно превышает скорость обработки отдельных кадров, есть возможность выбирать кадры оптимальным с точки зрения качества распознавания способом (Chernov et al., 2017б).

Методы детектирования кредитных карт (Skoryukina et al., 2015) и текстовых документов (Zhukovsky et al., 2017; Xu et al., 2017), в полученном с камеры мобильного устройства кадре, применимы в задаче детектирования защищенных документов. При этом продолжаются разработки более совершенных методов (Skoryukina et al., 2018; Жуковский, 2018), в том числе для учета специфики ДУЛ (Ngoc et al., 2018) и повышения производительности на мобильных устройствах (Puybareau, Geraud, 2018).

В условиях сложного фона естественной сцены, низкой плотности и неоднородности заполнения ДУЛ текстовыми строками, использование простых методов ректификации зоны документа (Williem et al., 2014) часто не представляется возможным и требует разработки более сложных подходов (Shemyakina et al., 2017; Skoryukina et al., 2018).Кадрирование цифровых изображений при проективном преобразовании (Шемякина и др., 2018) может использоваться для экономии ресурсов мобильного устройства. Улучшение качества изображения ДУЛ может достигаться путем совмещения нескольких кадров видеопотока (Тропин и др., 2018).

Определение типа ДУЛ может осуществляться на исходном проективно искаженном изображении (Лынченко и др., 2018), хотя большее распространение получили методы классифицирующие ДУЛ после или в процессе выделения и ректификации зоны документа (Usilin et al., 2010; Simon et al., 2015; Awal, 2017; Sicre et al., 2017). Обычно такая классификация происходит до оптического распознавания текстового содержимого документа, что позволяет на дальнейших этапах использовать более точные работающие в контексте типа документа специализированные методы обработки и распознавания. При этом даже элементы защиты документов, например, гильош, тоже могут использоваться для идентификации типа документа (или номера страницы) (Усилин и др., 2013).

В связи с особенностями распознавания ДУЛ на мобильных устройствах для извлечения текстового содержимого реквизитов могут использоваться специализированные методы локализации положения (Ильин и др., 2018) и предобработки зоны поля (Bezmaternykh et al., 2018), оптического распознавания текста (Sheshkus et al., 2016; Limonova et al., 2017; Ilin et al., 2017) и постобработки результатов распознавания (Петрова, Булатов, 2018). Для мобильных приложений актуальной тематикой является своевременная остановка процессов обработки входного видеопотока (Булатов, 2017; Arlazarov et al., 2017) и передача пользователю окончательных результатов.

Эталонные наборы данных

Эталонные наборы изображений, сопутствующие им данные и инструменты замеров контроля качества распознавания являются критически важным элементом разработки систем распознавания промышленного уровня (Безматерных и др., 2018). Общедоступные наборы данных позволяют воспроизводить и верифицировать научные исследования. В связи с естественными ограничениями законодательства на распространение изображений удостоверяющих личность документов (персональные данные) результаты большинства исследований приводятся для закрытых наборов данных и не могут быть воспроизведены и/или проверены. Единственным примером открытого набора данных с изображениями персональных документов является (Arlazarov et al., 2018). На рис. 5 представлены примеры изображений из этого набора.

Открытые наборы данных с изображениями текстовых документов являются более доступными и могут быть полезны при разработке и анализе систем распознавания ДУЛ. Например, эталонные изображения текстовых документов на захваченных при помощи малоформатной цифровой камеры кадрах видеопотока (Burie et al., 2015; Chazalon et al., 2017) использовались при проведении конкурсов в рамках конференции

Рис. 5. Пример изображений документов из набора данных MIDV-500 (цит. по Arlazarov et al., 2018).

ICDAR. Особенности полученных при использовании камер мобильных устройств изображений представлены в работах (Kumar et al., 2013; Nayef et al., 2015). Примеры фабрикации бизнес-документов представлены в наборах данных (Sidere et al., 2017; Artaud et al., 2017).

Недостаточные объемы изображений ДУЛ до некоторой степени могут компенсироваться изощренными методами синтеза изображений. Позитивный опыт использования такого рода генерации, например, для изображений зон текстовых реквизитов, представлен в работах (Гайер и др., 2018а; 2018б; Емельянов и др., 2018; Chernyshova et al., 2018;).

ВЫЯВЛЕНИЕ ПРИЗНАКОВ ФАБРИКАЦИИ ДОКУМЕНТОВ

Поскольку документ теряет юридическую силу при отсутствии одного из обязательных реквизитов, начальным уровнем контроля подлинности ДУЛ является проверка правильности заполнения по результатам распознавания значений реквизитов. При наличии МСЗ производится сверка данных в этой зоне и информации из основной части документа (Kwon, Kim, 2007). Далее возможна проверка соответствия бланка утвержденной и действующей формы, проверка наличия и содержания печатей и штампов (Арлазаров и др., 2018б), проверка наличия подписи должностных лиц.

Проверка фоновых типографских элементов защиты

Методы выявления фактов подделки по результатам анализа типографских элементов защиты документов для отсканированных изображений высокого разрешения ДУЛ рассмотрены в работах (Dewaele et al., 2016; Berenguel et al., 2016). Намного более доступными для исследователей и близкими к ДУЛ с точки зрения методов полиграфической защиты являются банкноты. Подходы к реализации приложений для выявления подделок денежных знаков на мобильных устройствах описаны в следующих работах (Блохинов, Горбачев, 2016; Блохинов и др., 2017; Rahman et al., 2017; Dittimi etal., 2018). При наличии достаточного количества эталонных изображений ДУЛ для выявления признаков фабрикации возможно использование локальных информативных признаков, которые рассматриваются в работе (Блохинов, Горбачев, 2016). Такие признаки вычисляются для областей интереса на изображении банкноты, которые 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.

Анализ шрифтовых особенностей

Результаты контроля однородности шрифта для отдельных символов, слов и строк в контексте групп полей, а так же проверка соответствия стандартам параметров шрифтов может использоваться для выявления фактов фабрикации ДУЛ. Простой вариант сравнения выровненных и бинаризованных изображений отдельных символов реквизитов документа для шрифта OCR-B используется в работе (Kwon, Kim, 2007). Решение общей задачи классификации шрифта по изображению фрагмента текста с использовани-

Рис. 6. Примеры изображений символов сфабрикованной – *а* и подлинной – *б* машиносчитываемой зоны документа, изображения цифр зоны номера сфабрикованного – *в* и подлинного – *г* паспорта гражданина РФ (цит. по Chernyshova et al., 2018).

ем шрифтовых баз рассматривается в работах (Chen et al., 2014; Wang et al., 2015; 2018). В работе (Baluja, 2016) описан нейросетевой метод оценки стилистической шрифтовой близости символов. Варианты постановки и решения задач верификации шрифта или контроля однородности шрифтового оформления текста в указанных работах не рассматриваются.

Выделение типографских признаков различных шрифтов для классификации типа шрифта по изображению текста рассматривается в работах (Zramdini, Ingold, 1998; Satkhozhina et al., 2013). Неоднородность признаков такого рода используется в работе (Bertrand et al., 2015) для обнаружения символов, слов или предложений в бизнес-документе со свойствами шрифта, отличными от их окружения. Эти работы используют полученные при помощи сканирующего оборудования в высоком разрешении (не менее 300–400 dpi) изображения коммерческих документов.

Решение задачи выявления признаков фабрикации защищенных документов на основе анализа полученных при помощи мобильных устройств изображений рассматривается в работе (Chernyshova et al., 2018). Поскольку в ряде документов есть поля, которые должны печататься стандартизованными шрифтами, отклонения от стандарта используются для выявления фактов подделки. Анализ заполнения машиносчитываемой зоны (шрифт OCR-B) является примером постановки задачи, когда все параметры шрифта известны, а сам шрифт доступен для генерации обучающих примеров. Примеры изображений символов машиносчитываемой зоны представлены на рис. 6, *а* и *б*. На примере шрифта зоны серии и номера паспорта гражданина РФ рассматриваются особенности решения задачи в условиях, когда точные параметры шрифта неизвестны (непубличная информация), а исследователям доступны только образцы реальных документов. Примеры изображений символов зоны номера паспорта РФ представлены на *в* и *г*. Авторы используют многозадачное обучение сверточного нейросетевого классификатора. Этот классификатор одновременно решает задачи оптического распознавания символа и проверки соответствия конкретного символа стандарту. По результатам исследования использование многозадачного обучения приводит к повышению чувствительности и специфичности классификатора. Полученный классификатор демонстрирует высокую обобщающую способность, поскольку он позволяет контролировать на соответствие эталонному представлению символы шрифтов, не представленные в обучающей выборке.

Анализ защитных голограмм

В ряде работ (Hartl et al., 2013; 2015; 2016) продемонстрирована возможность использования встроенной вспышки (фонарика) мобильного устройства для устойчивого детектирования и верификации ЗГ. Основное внимание в работах уделено анализу поведения пользователя в процессе визуальной проверки голографического защитного элемента. Авторами предлагается вариант пользовательского интерфейса с использованием технологий виртуальной реальности, в котором на экран выводятся подсказки о положении и статусе проверки конкретных защитных элементов, а также инструкции пользователю о желательном поведении. В проведенном исследовании для небольшого эталонного набора ЗЭГ и ракурсов прототип мобильного приложения с предложенным интерфейсом позволил при увеличении числа ракурсов наблюдения время верификации голографического элемента сократить до 15 с. Для детектирования голограмм (Hartl et al., 2014) предлагается формировать “стопку” проек-

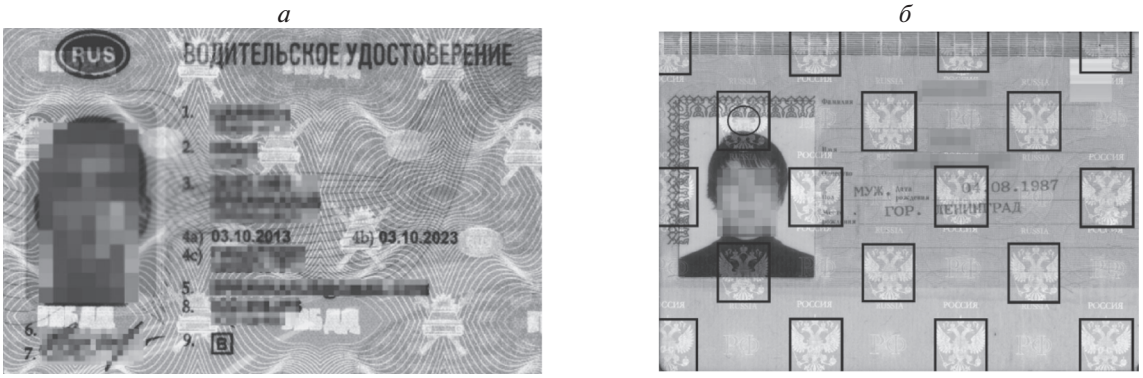


Рис. 7. Пример изображения регулярной структуры защитных элементов на бланке водительского удостоверения РФ – *а* и локализации периодической структуры защитных элементов паспорта гражданина РФ – *б* (цит. по Chernov et al., 2017).

тивно исправленных изображений документа и выделять области пикселей с существенными статистическими отклонениями яркости при усреднении по “стопке” (между разными ракурсами). Отметим, что этот подход не использует цветовую информацию и потенциально неустойчив к бликам на изображениях. Верификация ЗГ производится путем сравнения извлеченных из видеопотока проективно исправленных изображений элемента с эталонными ракурсами. Сами авторы отмечают, что такая методика верификации требует существенной доработки и не применима для произвольных голографических защитных элементов.

Метод детектирования произвольных голографических элементов в видеопотоке описан в патенте (Арлазаров и др., 2018в). Поскольку защищенные документы часто изготавливаются по технологии со специальным (пленочным) покрытием страниц документа, особого внимания требует устойчивость методов детектирования к присутствию световых отражений (бликов). Наличие отражений источников освещения при съемке страниц документов приводит к зашкаливанию (забеливанию) регионов изображения, тем самым сильно влияя как на яркостные, так и на цветовые характеристики этих регионов. Для повышения надежности метода предлагается после стабилизации изображения документа и построения карт насыщенности и цветового тона проводить анализ цветовых характеристик для отдельных кадров. Затем на основе межкадровых изменений цветовых характеристик строится интегральная карта оценок присутствия голограмм для всех кадров видеопотока и осуществляется выделение итоговых областей голографических элементов с учетом карты оценок присутствия ЗГ.

Защитные голограммы некоторых ДУЛ расположены не в фиксированном месте на бланке документа, а образуют регулярные структуры. Примеры изображений таких документов представлены на рис. 7. Детектирование наличия таких регулярных структур на изображении документа, оценка локализации элементов и оценка геометрических параметров таких структур при помощи дискретного преобразования Фурье рассматриваются в работах (Chernov et al., 2015; 2017a). Предложенный метод поиска периодических паттернов на изображениях документов пригоден для реализации на мобильных устройствах и показал среднюю ошибку локализации в 6% на наборе из 484 изображений. Этот метод не требует непосредственного анализа одиночного изображения элемента периодической структуры, что особенно ценно для анализа (образ такого элемента может сильно меняться для голографических защитных элементов). Метод также устойчив к отсутствию на изображении части элементов регулярной структуры. Дополнительно локализация подобных регулярных помех позволяет повышать точность и надежность распознавания реквизитов документов за счет удаления вносимых защитными элементами искажений с максимально возможным сохранением текстовой информации, а также за счет использования специальных настроек для подсистем оптического распознавания в зонах присутствия защитных элементов.

Проверка личности владельца документа

При необходимости сопоставления изображение владельца документа и ДУЛ возможно при помощи съемки владельца в режиме “селфи” с документом в руках с последующим сличением изображения лица и фотографии на документе (crossbiometry) (Folego et al., 2016; Oliveira et al., 2018). Отметим, что все доступные публикации опираются на клиент-серверную модель обработки данных, хотя существует принципиальная возможность верификацию производить на самом мобильном устройстве.

ЗАКЛЮЧЕНИЕ

Мобильные технологии оценки подлинности документов, удостоверяющих личность, являются перспективным направлением развития методов предоставления удаленного доступа к услугам и сервисам. Несмотря на показанную в рассмотренных работах техническую возможность использования мобильных устройств для выявления признаков фабрикации документов, удостоверяющих личность, сейчас невозможно использовать такого рода технологий в прикладных задачах из-за требования дальнейших исследований:

– разработке моделей угроз и нарушителей при использовании мобильных устройств для оптического ввода и контроля подлинности документов;

– усовершенствования методов и средств анализа устойчивости и надежности выявления признаков фабрикации для выведения технологий на промышленный уровень качества;

– разработке и комплексировании методов выявления признаков фабрикации документов с достаточными для практического применения характеристиками.

Достижение промышленного качества возможно за счет усовершенствования моделей и методов распознавания изображений документов в видеопотоке при слабо контролируемых условиях съемки и ограниченных вычислительных ресурсах.

Исследование выполнено при частичной финансовой поддержке РФФИ в рамках научных проектов № 17-29-03370 офи_м, № 18-07-01387 а.

СПИСОК ЛИТЕРАТУРЫ

Арлазаров В.В., Арлазарова А.Р., Арлазаров Н.В., Николаев Д., Славин О., Усилин С., Шешкус А. *Система доступа к дистанционному получению банковских услуг.* Патент на полезную модель РФ. № 161478. 2016.

Арлазаров В.В., Булатов К.Б., Усков А.В. Модель системы распознавания объектов в видеопотоке мобильного устройства. *Труды ИСА РАН*. Спецвыпуск. 2018а. С. 73–82. DOI: 10.14357/20790279180508.

Арлазаров В. В., Жуковский А., Кривцов В., Николаев Д., Полевой Д. Анализ особенностей использования стационарных и мобильных малоразмерных цифровых видеокамер для распознавания документов. *Информационные технологии и вычислительные системы*. 2014. № 3. С. 71–78.

Арлазаров В.В., Маталов Д.П., Усилин С.А. Локализация образа печати на документе, удостоверяющем личность, методом машинного обучения. *Труды ИСА РАН*. Спецвыпуск. 2018б. С. 158–166. DOI: 10.14357/20790279180518

Арлазаров В.В., Николаев Д.П., Скорюкина Н.С., Чернов Т.С. *Способ детектирования голографических элементов в видеопотоке.* Патент РФ. № 2644513. 2018в.

Безматерных П.В., Плискин Е.Л., Фарсобина В.В. Вычислительный комплекс для контроля качества распознавания структурированных документов. *Информационные технологии и вычислительные системы*. 2018. № 2. С. 94–102. DOI: 10.14357/20718632180208

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

Блохинов Ю.Б., Горбачев В.А. Анализ подлинности образцов защищенной печатной продукции с использованием смартфона. *Вестник компьютерных и информационных технологий*. 2016. № 4. С. 23–29. DOI: 10.14489/vkit.2016.04.pp.023-029.

Булатов К. Выбор оптимальной стратегии комбинирования покадровых результатов распознавания символа в видеопотоке. *Информационные технологии и вычислительные системы*. 2017. № 3. С. 45–55.

Булатов К.Б., Ильин Д.А., Полевой Д.В., Чернышова Ю.С. Проблемы распознавания машиночитаемых зон с использованием малоформатных цифровых камер мобильных устройств. *Труды ИСА РАН*. 2015. Т. 65. № 3. С. 85–93.

Вашкевич Н.А., Рубис А.С. *Средства защиты и способы подделки машиносчитываемых проездных документов: учебное пособие*.Минск. Право и экономика, 2017. 91 с.

Гайер А.В., Чернышова Ю.С., Шешкус А.В. Генерация искусственной обучающей выборки для задачи распознавания символов полей паспорта РФ. *Сенсорные системы*. 2018а. Т. 32. № 3. С. 230–235. DOI: 10.1134/S023500921803006X

Гайер А.В., Шешкус А.В., Чернышова Ю.С. Аугментация обучающей выборки “на лету” для обучения нейронных сетей. *Труды ИСА РАН*. Спецвыпуск. 2018б. С. 150–157. DOI: 10.14357/20790279180517

Герасимов А. *Цифровое мошенничество: риски и ущерб*. URL: https://bosfera.ru/bo/cifrovoe-moshennichestvo-riski-i-ushcherb (дата обращения: 20.10.2018).

ГОСТ Р 54109-2010. *Защитные технологии. Продукция полиграфическая защищенная. Общие технические требования*. М. Стандартинформ, 2011. 18 с.

Емельянов С.О., Иванова А.А., Швец Е.А., Николаев Д.П. Методы аугментации обучающих выборок в задачах классификации изображений. *Сенсорные системы*. 2018. Т. 32. № 3. С. 236–245. DOI: 10.1134/S0235009218030058

Жуковский А.Е. Методы межкадровой интеграции результатов обнаружения документов в видеопотоке мобильного устройства. *Труды ИСА РАН*. Спецвыпуск. 2018. С. 15–22. DOI: 10.14357/20790279180502.

Иьин Д.А. Быстрая локализация текстовых полей на изображения документов низкого качества. *Труды ИСА РАН*. Спецвыпуск. 2018. С. 192–198. DOI: 10.14357/20790279180522

КонсультантПлюс. *Справочная информация: “Документы, удостоверяющие личность”*. URL: http://www.consul-

tant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=149244 (дата обращения: 20.10.2018).

Лынченко А.Е., Шешкус А.В., Арлазаров В.Л. Алгоритм классификации документов, удостоверяющих личность, на проективно-искаженных изображениях на основе обучаемой метрики подобия. *Труды ИСА РАН*. Спецвыпуск. 2018. С. 167–173. DOI: 10.14357/20790279180519

НБКИ. *В 2015 году было зафиксировано 596 тысяч кредитов с признаками мошенничества. Это на 12.6% больше, чем в 2014 году*. URL: https://www.nbki.ru/company/news/?id=12161&sphrase_id=116239 (дата обращения: 20.10.2018).

Одиноков С.Б. *Методы и оптико-электронные приборы для автоматического контроля подлинности защитных голограмм*. М. Техносфера, 2013. 175 с.

Петрова О.О., Булатов К.Б. Методы пост-обработки результатов распознавания машиночитаемой зоны документов. *Труды ИСА РАН*. Спецвыпуск. 2018. С. 43–50. DOI: 10.14357/20790279180505.

Полевой Д., Булатов К., Скорюкина Н., Чернов Т., Арлазаров В.В., Шешкус А. Ключевые аспекты распознавания документов с использованием малоразмерных цифровых камер. *Вестник РФФИ*. 2016. № 4. С. 97-108. DOI: 10.22204/2410-4639-2016-092-04-97-108

Тропин Д.В., Николаев Д.П., Слугин Д.Г. Метод совмещения изображений на основе максимизации резкости. *Труды ИСА РАН*. Спецвыпуск. 2018. С. 134–141. DOI: 10.14357/20790279180515

Усилин С.А., Николаев Д.П., Шоломов Д.Л., Арлазаров В.В. Распознавание гильоширных элементов: определение страниц паспорта РФ. *Труды ИСА РАН*. 2013. Т. 63. № 3. С. 106–110.

ЦБ РФ. *Основные направления развития финансовых технологий на период 2018–2020 гг.* URL: https://www.cbr.ru/content/document/file/35816/on_fintex_2017.pdf (дата обращения: 20.10.2018).

Шемякина Ю.А., Жуковский А.Е., Коноваленко И.А., Николаев Д.П. Алгоритм автоматического кадрирования цифровых изображений при проективном преобразовании. *Труды ИСАРАН*. Спецвыпуск. 2018. С. 142–149. DOI: 10.14357/20790279180516

Arlazarov V. V., Bulatov K., Manzhikov T., Slavin O., Yanishevskiy I. Method of determining the necessary number of observations for video stream documents recognition.*Proc. SPIE 10696, Tenth International Conference on Machine Vision (ICMV 2017)*. 2018. V. 106961X. P. 1–6. DOI: 10.1117/12.2310132.

Arlazarov V.V., Bulatov K., Chernov T., Arlazarov V.L. *MIDV-500: A Dataset for Identity Documents*. URL: https://arxiv.org/pdf/1807.05786.pdf (дата обращения: 20.10.2018).

Artaud C., Sidère N., Doucet A., Ogier J.-M., Poulain V. Find it! Fraud Detection Contest Report. *24th International Conference on Pattern Recognition (ICPR 2018)*. 2018.

Awal A.-M., Ghanmi N., Sicre R., Furon T. Complex Document Classification and Localization Application on Identity Document Images.*14th IAPR International Conference on Document Analysis and Recognition (ICDAR 2017)*. 2017. P. 426–431. DOI: 10.1109/ICDAR.2017.77.10.1109/ICDAR.2017.77

Baluja S. *Learning typographic style*.URL: https://arxiv.org/pdf/1603.04000 (датаобращения 20.10.2018).

Berenguel A., Terrades O.R., Llados J., Canero C. Banknote Counterfeit Detection through Background Texture Printing Analysis. *12th IAPR Workshop on Document Analysis Systems (DAS)*. 2016. P. 66–71. DOI: 10.1109/das.2016.34.

Bertrand R., Terrades O. R., Gomez-Kramer P., Franco P., Ogier J.-M. A conditional random field model for font forgery detection.*13th International Conference on Document Analysis and Recognition (ICDAR 2015)*. 2015. V. 576–580.

Bezmaternykh P. V., Nikolaev D. P., Arlazarov V. L. Textual Blocks Rectification Method Based on Fast Hough Transform Analysis in Identity Documents Recognition. *Proc. SPIE 10696, Tenth International Conference on Machine Vision (ICMV 2017)*. 2018. V. 1069606. P. 1–6. DOI: 10.1117/12.2310162.

Boulkenafet Z., Akhtar Z., Feng X., Hadid A. Face Antispoofing in Biometric Systems.*Biometric Security and Privacy*. Ed. Jiang R. Springer. 2017. P. 299–321. DOI: 10.1007/978-3-319-47301-7_13

Bulatov K., Arlazarov V.V., Chernov T., Slavin O., Nikolaev D. Smart IDReader: Document Recognition in Video Stream. *14th IAPR International Conference on Document Analysis and Recognition (ICDAR 2017)*. 2017. P. 39–44. DOI: 10.1109/ICDAR.2017.347.

Burie J.C., Chazalon J., Coustaty M., Eskenazi S., Luqman M.M., Mehri M., Nayef N., Ogier J.M., Prum S., Rusinol M. ICDAR 2015 competition on smartphone document capture and OCR (SmartDoc). *Proc. of the Intl. Conf. on Document Analysis and Recognition (ICDAR 2015)*. 2015. P. 1161–1165.

Chazalon J., Gomez-Kramer P., Burie J.-C., Coustaty M., Eskenazi S., Luqman M., Nayef N., Rusinol M., Sidere N., Ogier J.-M. SmartDoc 2017 Video Capture: Mobile Document Acquisition in Video Mode. *Proc. of the Conf. on Document Analysis and Recognition (ICDAR 2017)*.2017. DOI: 10.1109/icdar.2017.306.

Chen G., Yang J., Jin H., Brandt J., Shechtman E., Agarwala A., Han T. X., Large-scale visual font recognition. *Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2014)*. 2014. P. 3598–3605. DOI: 10.1109/CVPR.2014.460.

Chernov T.S., Nikolaev D.P., Kliatskine V.M. A Method of Periodic Pattern Localization on Document Images.*Proceedings SPIE 9875, Eighth International Conference on Machine Vision (ICMV 2015)*.2015. V. 987504. P. 1–7. DOI: 10.1117/12.2228600.10.1117/12.2228600

Chernov T.S., Kolmakov S.I., Nikolaev D.P. An algorithm for detection and phase estimation of protective elements periodic lattice on document image. *Pattern Recognition and Image Analysis*. 2017. V. 27. № 1. P. 53–65 DOI: 10.1134/S1054661817010023

Chernov T.S., Razumnuy N.P., Kozharinov A.S., Nikolaev D.P., Arlazarov V.V. Image quality assessment for video stream recognition systems. *Proc. SPIE 10696, Tenth International Conference on Machine Vision (ICMV 2017)*. 2018. V. 106961U. P. 1–8. DOI: 10.1117/12.2309628.

Chernyshova Y.S., Gayer A.V., Sheshkus A.V. Generation method of synthetic training data for mobile OCR system. *Proc. SPIE 10696, Tenth International Conference on Machine Vision (ICMV 2017)*. 106962G. 2018. P. 1–7. DOI: 10.1117/12.2310119.

Chernyshova Y.S., Aliev M.A., Sheshkus A.V. *Optical font recognition in images captured with smartphones, and its applicability for detecting forgery of identity documents*. URL: https://arxiv.org/abs/1810.08016 (дата обращения: 20.10.2018).

Cook S. Selfie banking: is it a reality? *Biometric Technology Today*. 2017. V. 3. P. 9–11.

Dewaele T., Diephuis M., Holotyak T., Voloshynovskiy S. Forensic authentication of banknotes on mobile phones. *Electronic Imaging*. 2016. V. 8. P. 1–8. DOI: 10.2352/issn.2470-1173.2016.8.mwsf-083

Dittimi T.V., Suen C.Y. Mobile App for Detection of Counterfeit Banknotes. *Lecture Notes in Computer Science*. 2018. V. 10832. P. 156–168. DOI: 10.1007/978-3-319-89656-4_13

Folego G., Angeloni M. A., Stuchi J. A., Godoy A., Rocha A. Cross-domain face verification: Matching ID document and self-portrait photographs.*XII Workshop de VisãoComputacional*. 2016. P. 311–316.

Gaia K., Qiua M., Suna X. A survey on fintech.*Journal of Network and Computer Applications*. 2018. V. 103. P. 262–273.

Hartl A., Arth C., Grubert J., Schmalstieg D. Efficient Verification of Holograms Using Mobile Augmented Reality. *Transactions on Visualization and Computer Graphics*. 2016. V. 22. № 7. P. 1843–1851.

Hartl A., Arth C., Schmalstieg D. AR-Based Hologram Detection on Security Documents Using a Mobile Phone. *Lecture Notes in Computer Science*. 2015. V. 8888. P. 335–346. DOI: 10.1007/978-3-319-14364-4_32

Hartl A., Grubert J., Schmalstieg D., Reitmayr G. Mobile interactive hologram verification. *Proceedings of the IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*. 2013. P. 75–82.

Ilin D., Limonova E., Arlazarov V., Nikolaev D. Fast Integer Approximations In Convolutional Neural Networks Using Layer-By-Layer Training. *Proceedings SPIE 10341, Ninth International Conference on Machine Vision (ICMV 2016)*. 2017. V. 103410Q. P. 1–5. DOI: 10.1117/12.2268722.

Kumar J., Ye P., Doermann D. A dataset for quality assessment of camera captured document images. *Proc. of the International Workshop on Camera-Based Document Analysis and Recognition (CBDAR 2013)*. 2013. P. 113–125.

Kwon Y.-B., Kim J.-H. Recognition based verification for the machine readable travel documents. *International Workshop on Graphics Recognition (GREC 2007)*. 2007.

Limonova E.E., Bezmaternykh P., Nikolaev D., Arlazarov V. Slant Rectification in Russian Passport OCR System Using Fast Hough Transform. *Proceedings SPIE 10341, Ninth International Conference on Machine Vision (ICMV 2016)*.2017. V. 10341. № 103410P. P. 1–5. DOI: 10.1117/12.2268725.

Nayef N., Luqman M., Prum S., Eskenazi S., Chazalon J., Ogier J.-M. SmartDoc-QA: A dataset for quality assessment of smartphone captured document imagessingle and multiple distortions. *Proc. of the Conf. on Document Analysis and Recognition (ICDAR 2015)*. 2015. P. 1231–1235.

Ngoc M.O., Fabrizio J., Geraud T. Saliency-Based Detection of Identy Documents Captured by Smartphones. *13th IAPR International Workshop on Document Analysis Systems (DAS 2018)*. 2018. DOI: 10.1109/das.2018.17.

Oliveira J. S., Souza G. B., de Rezende R. A., de Deus F. E., Marana A. N. *Cross-domain deep face matching for real banking security systems*. URL: https://arxiv.org/abs/1806.07644 (дата обращения: 20.10.2018).

Puybareau E., Geraud T. Real-Time Document Detection in Smartphone Videos. *25th IEEE International Conference on Image Processing (ICIP 2018)*. 2018. DOI: 10.1109/icip.2018.8451533.

Rahman U., Sargano A., Bajwa U. Android-Based Verification System for Banknotes. *Journal of Imaging*. 2017. V. 3. № 54.DOI: 10.3390/jimaging3040054

Satkhozhina A., Ahmadullin I., Allebach J. P. Optical font recognition using conditional random field. *Proceedings of the 2013 ACM Symposium on Document Engineering (DocEng '13)*. 2013. P. 119–122. DOI: 10.1145/2494266.2494307.

Simon M., Rodner E., Denzler J. Fine-grained classification of identity document types with only one example. *14th IAPR International Conference on Machine Vision Applications (MVA 2015)*. 2015. P. 126–129. DOI: 10.1109/MVA.2015.7153149.

Shemyakina J., Zhukovskiy A., Nikolaev D. The Method for Homogrpahy Estimation between Two Planes Based on Lines and Points. *Proc. SPIE 10696, Tenth International Conference on Machine Vision (ICMV 2017)*. 2018. V. 106961G. P. 1–20. DOI: 10.1117/12.2310111.

Sheshkus A., Limonova E., Nikolaev D., Krivtsov V. Combining Convolutional Neural Networks and Hough Transform for Classification of Images Containing Lines. *Proceedings SPIE 10341, Ninth International Conference on Machine Vision (ICMV 2016)*. 2017. V. 103411C. P. 1–5. DOI: 10.1117/12.2268717.

Sicre R., MontaserAwal A., Furon T. Identity documents classification as an image classification problem.*19th International Conference on Image Analysis and Processing (ICIAP 2017)*. 2017. P. 602–613. DOI: 10.1007/978-3-319-68548-9_55

Sidere N., Cruz F., Coustaty M., Ogier J.-M. A dataset for forgery detection and spotting in document images. *Proc. of the Seventh International Conference on Emerging Security Technologies (EST 2017)*. 2017. P. 26–31. DOI: 10.1109/est.2017.8090394

Skoryukina N., Nikolaev D.P., Sheshkus A., Polevoy D. Real time rectangular document detection on mobile devices. *Proc. SPIE 9445, Seventh International Conference on Machine Vision (ICMV 2014)*. 2015. V. 94452A. P. 1–6.

Skoryukina N., Shemyakina J., Arlazarov V. L., Faradzhev I. Document localization algorithms based on feature points and straight lines. *Proc. SPIE 10696, Tenth International Conference on Machine Vision (ICMV*

2017). 2018. V. 106961H. P. 1–8. DOI: 10.1117/12.2311478.

Usilin S., Nikolaev D., Postnikov V., Schaefer G. Visual appearance based document image classification. *Proc. of the IEEE International Conference on Image Processing*. 2010. P. 2133–2136.DOI: 10.1109/ICIP.2010.5652024.

Vironit. *A Real-time Document Recognition SDK Comparison*.URL: https://vironit.com/a-real-time-document-recognition-sdk-comparison (дата обращения: 20.10.2018).

Wang X. Bissacco A., Berntson G., Nazif M., Scheiner J., Shih S., Snyder M., Talavera D. *Client side filtering of card OCR images*. Patent US. № 8,903,136. 2014.

Wang Z., Yang J., Jin H., Shechtman E., Agarwala A., Brandt J., Huang T. S. DeepFont, Identify your font from an image. *In Proceedings of the 23rd ACM International Conference on Multimedia*. 2015. P. 451–459.

Wang Z. Deep Learning for Font Recognition and Retrieval. *Applied Cloud Deep Semantic Recognition Advanced Anomaly Detection*. 2018. Auerbach Publications. P. 109–130.

Williem C. Simon S. Cho and I. K. Park. Fast and Robust Perspective Rectification of Document Images on a Smartphone. *Proc. IEEE (CVPRW 2014)*. 2014. P. 197–198.

Winarski T.Y. *Selfie financial security transaction system*. Patent US. No. US20160071101A1. 2016.

Xu Y., Carlinet E., Géraud T., Najman L. Hierarchical Segmentation Using Tree-Based Shape Spaces. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2017. V. 39. № 3. P. 457–469.

Zhukovsky A., Nikolaev D., Arlazarov V., Postnikov V., Polevoy D., Skoryukina N., Chernov T., Shemiakina J., Mukovozov A., Konovalenko I., Povolotsky M. Segments Graph-Based Approach for Document Capture in a Smartphone Video Stream. *Proceedings of the International Conference on Document Analysis and Recognition (ICDAR)*. 2017. V. 1. P. 337–342. DOI: 10.1109/ICDAR.2017.63

Zramdini A., Ingold R. Optical font recognition using typographical features. *IEEE Trans. Pattern Anal. Mach. Intell.* 1998. V. 20. P. 877–882.

Identity documents forgery detection with mobile devices

D. V. Polevoy[a,b,c,#]

[a] *Federal Research Center "Computer Science and Control" of RAS, 19333 Moscow, Vavilova avenue, 44-2, Russia*

[b] *National University of Science and Technology "MISIS", 119991 Moscow, Leninsky prospect, 4, Russia*

[c] *Smart Engines Ltd., 117312 Moscow, 60-letiya Oktyabryaavenue, 9, Russia*

[#] *E-mail: dvpsun@gmail.com*

There is a growing interest in using of identity documents images for users registration and identification in mobile and fintech services. At the same time, these technologies increase the risks of losses from fraud. This paper reviews approaches and methods for solving the actual problem of document fraud detection on mobile devices.

Key words: identity documents fraud detection, document image recognition, image processing, mobile device, smartphone, identification

REFERENCES

Arlazarov V.V., Arlazarova A.R., Arlazarov N.V., Nikolaev D., Slavin O., Usilin S., Sheshkus A. Sistema dostupa k distancionnomu polucheniju bankovskih uslug [The system of access to remote banking services]. Patent for a useful model RF. № 161478. 2016.

Arlazarov V.V., Bulatov K.B., Uskov A.V. Model' sistemy raspoznavanija ob#ektov v videopotoke mobil'nogo ustrojstva [A model of object recognition system in video stream of a mobile device]. Trudy ISA RAN[Proceedings of ISA RAS]. Special issue. 2018. P. 73–82. DOI: 10.14357/20790279180508 (in Russian).

Arlazarov V.V., Zhukovskiy A., Krivtsov V., Nikolaev D., Polevoy D. Analiz osobennostey ispolzovaniya statsionarnykh i mobilnykh malorazmernykh tsifrovykh video kamer dlya raspoznavaniya dokumentov [Analysis of the features of using stationary and mobile small-sized digital video cameras for document recognition]. *Informatsionnye tekhnologii i vychislitelnye sistemy* [Information technology and computing systems]. 2014. № 3. P. 71–78 (in Russian).

Arlazarov V.V., Matalov D.P., Usilin S.A. Lokalizacija obraza pechati na dokumente, udostoverjajushhem lichnost', metodom mashinnogo obuchenija [Localization of the seal on the identity document image using machine learning approach]. Trudy ISA RAN [Proceedings of ISA RAS]. *Special issue*. 2018. P. 158–166. DOI: 10.14357/20790279180518 (in Russian).

Arlazarov V.V., Nikolaev D.P.,Skoryukina N.S., Chernov T.S. Sposob detektirovanija gologra ficheskihj elementov v videopotoke [Method for detecting holographic elements in a video stream]. Patent RF. № 2644513. 2018.

Bezmaternyh P.V., Pliskin E.L., Farsobina V.V. Vychislitel'ny jkompleks dlja kontrolja kachestva raspoznavanija strukturirovannyh dokumentov [Information system for structured documents OCR quality control]. *Informatsionnye tekhnologii I vychislitelnye sistemy* [Information technology and computing systems]. 2018. № 2. P. 94–102. DOI: 10.14357/20718632180208 (in Russian).

Blokhinov Yu.B., Bondarenko A.V., Gorbachev V.A., Zheltov S.Yu., Rakutin Yu.O. Opredelenie podlinnosti banknot na osnove analiza izobrazhenij dlja smartfona

[Counterfeit bill detection by image analysis for smartphones]. *Komp'juternaja optika* [Computer Optics]. 2017. V. 41. № 2. P. 237–244. DOI: 10.18287/2412-6179-2017-41-2-237-244 (in Russian).

Blokhinov Yu.B., Gorbachev V.A. Analiz podlinnosti obrazcov zashhishhjonnoj pechatnoj produkcii s ispol'zovaniem smartfona [The authenticity analysis of samples of the protected printed materials with use of the smartphone]. *Vestnik kompiuternykhin formatsion nykhtekhnologii* [Herald of computer and information technologies]. 2016. V. 4. P. 23–29. DOI: 10.14489/vkit.2016.04 (in Russian).

Bulatov K. Vybor optimal'noj strategii kombinirovanija pokadrovyh rezul'tatov raspoznavanija simvola v videopotoke [Choosing the optimal strategy for combining frame-by-frame character recognition results in a video stream]. *Informatsionnye tekhnologii ivychislitelnye sistemy* [Information technology and computing systems.] 2017. № 3. P. 45–55 (in Russian).

Bulatov K.B., Ilin D.A., Polevoy D.V., Chernyshova Y.S. Problemy raspoznavanija mashinochitaemyh zon s ispol'zovaniem maloformatnyh cifrovyh kamer mobil'nyh ustrojstv [Problems of recognition of machine-readable zones using small-format digital cameras of mobile devices].*Trudy ISA RAN* [Proceedings of ISA RAS]. 2015. V. 65 (3). P. 85–93 (in Russian).

Vashkevich N.A., Rubis A.S. Sredstva zashhity i sposoby poddelki mashinoschityvaemyh proezdnyh dokumentov: uchebnoe posobie [Remedies and ways of machine readable travel documents forgeries: a tutorial]. Minsk. *Law and Economics*. 2017. 91 p. (in Russian).

Gayer A.V., Chernyshova Y.S., Sheshkus A.V. Generacija iskusstvennoj obuchajushhej vyborki dlja zadachi raspoznavanija simvolov polej pasporta RF [Artificial training data generation for the task of character recognition of fields of russian passport]. *Sensornye sistemy* [Sensory systems]. 2018. V. 32 (3). P. 230–235. DOI: 10.1134/S023500921803006X (in Russian).

Gayer A.V., Sheshkus A.V., Chernyshova Y.S. Augmentacija obuchajushhej vyborki "naletu" dlja obuchenija nejronnyh setej [Augmentation on the fly for the neural networks learning]. *Trudy ISA RAN* [Proceedings of ISA RAS]. Special issue. 2018. P. 150–157. DOI: 10.14357/20790279180517 (in Russian).

Gerasimov A. Cifrovoe moshennichestvo: riski i ushherb [Digital fraud: risks and damages]. URL: https://bosfera.ru/bo/cifrovoe-moshennichestvo-riski-i-ushcherb (accessed: 20.10.2018) (in Russian).

GOST R 54109-2010 Zashhitnye tehnologii. Produkcija poligraficheskaja zashhishhennaja. Obshhie tehnicheskie trebovanija [State Standard R 54109-2010. Protective technology. Printing products protected. General technical requirements]. Moscow, Standartinform Publ., 2011. 18 p (in Russian).

Emelyanov S.O., Ivanova A.A., Shvets E.A., Nikolaev D.P. Metody augmentacii obuchajushhih vyborok v zadachah klassifikaciii zobrazhenij [Methods of training data augmentation in the task of image classification]. *Sensornye sistemy* [Sensory systems]. 2018. V. 32 (3). P. 236–245. DOI: 10.1134/S0235009218030058 (in Russian).

Zhukovsky A.E. Metody mezhkadrovoj integracii rezul'tatov obnaruzhenija dokumentov v videopotoke mobil'nogo ustrojstva [Methods for interframe integration of document detection results in a video stream of a mobile device]. *Trudy ISA RAN* [Proceedings of ISA RAS]. Special issue. 2018. P. 15–22. DOI: 10.14357/20790279180502 (in Russian).

Ilin D.A. Bystraja lokalizacija tekstovyh polej na izobrazhenija dokumentov nizkogo kachestva [Fast words boundaries localization in text fields for low quality document images]. *Trudy ISA RAN* [Proceedings of ISA RAS]. Special issue. 2018. P. 192–198. DOI: 10.14357/20790279180522 (in Russian).

Consultant Plus. Spravochnaja informacija: "Dokumenty, udostoverjajushhie lichnost" [Reference information: "Identity documents"]. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=149244 (accessed: 20.10.2018) (in Russian).

Lynchenko A.E., Sheshkus A.V., Arlazarov V.L. Algoritm klassifikacii dokumentov na proektivno-iskazhennyh izobrazhenijah na osnove obuchaemoj metriki podobija [Identity document classifiaction algorithm based on similarity metric robust to projective distortions]. *Trudy ISA RAN* [Proceedings of ISA RAS]. Special issue. 2018. P. 167–173. DOI: 10.14357/20790279180519 (in-Russian).

NBKI.V 2015 godu bylo zafiksirovano 596 tysjach kreditov s priznakami moshennichestva. Jetona 12.6% bol'she, chem v 2014 godu [In 2015, 596 thousand loans with signs of fraud were recorded. This is 12.6% more than in 2014]. URL: https://www.nbki.ru/company/news/?id=12161&sphrase_id=116239 (accessed: 20.10.2018) (in Russian).

Odinokov S.B. Metody I optiko-jelektronnye pribory dlja avtomaticheskogo kontrolja podlinnosti zashhitnyh gologramm [Methods and optoelectronic devices for automatic control of the authenticity of security holograms]. M. Teshnosphera, 2013. 175 p. (in Russian).

Petrova O.O., Bulatov K.B. Metody post-obrabotki rezul'tatov raspoznavanija mashinochitaemoj zony dokumentov [Methods of machine-readable zone recognition results post-processing]. *Trudy ISA RAN* [Proceedings of ISA RAS]. Special issue. 2018. P. 43–50. DOI: 10.14357/20790279180505 (in Russian).

Polevoy D., Bulatov K., Skoryukina N., Chernov T., Arlazarov V.V., Sheshkus A. Kljuchevye aspekty raspoznavanija dokumentov s ispol'zovaniem malorazmernyh cifrovyh kamer [Key Aspects of Document Recognition Using Small Digital Cameras]. *Vestnik RFFI* [Herald of the RFBR]. 2016. V. 4. P. 97–108. DOI: 10.22204/2410-4639-2016-092-04-97-108 (in Russian).

Tropin D.V., Nikolaev D.P., Slugin D.G. Metod sovmeshhenija izobrazhenij na osnove maksimizacii rezkosti [The method of image alignment based on sharpness maximization]. *Trudy ISA RAN* [Proceedings of ISA RAS]. Special issue. 2018. P. 134–141. DOI: 10.14357/20790279180515 (in Russian).

Usilin S.A., Nikolaev D.P., Sholomov D.L., Arlazarov V.V. Raspoznavanie gil'oshirnyh jelementov: opredelenie stranic pasporta RF [Guilloche Elements Recognition Applied to Passport Page Processing]. *Trudy ISA RAN* [Proceedings of ISA RAS]. 2013. V. 63 (3). P. 106–110 (in Russian).

CB RF. Osnovnye napravlenija razvitija finansovyh tehnologij na period 2018–2020 gg. [The main directions of development of financial technologies for the period 2018–2020 yy.] URL: https://www.cbr.ru/con-

tent/document/file/35816/on_fintex_2017.pdf (accessed: 20.10.2018) (in Russian).

Shemiakina J.A., Zhukovsky A.E., Konovalenko I.A., Nikolaev D.P. Algoritm avtomaticheskogo kadrirovanija cifrovyh izobrazhenij pri proektivnom preobrazovanii [Algorithm for automatic framing of digital images under projective transformation]. *Trudy ISA RAN* [Proceedings of ISA RAS]. Special issue. 2018. P. 142–149. DOI: 10.14357/20790279180516 (in Russian).

Arlazarov V.V., Bulatov K., Manzhikov T., Slavin O., Yanishevskiy I. Method of determining the necessary number of observations for video stream documents recognition.Proc. SPIE 10696, *Tenth International Conference on Machine Vision* (ICMV 2017). 2018. V. 106961X. P. 1–6. DOI: 10.1117/12.2310132.

Arlazarov V.V., Bulatov K., Chernov T., Arlazarov V.L. MIDV-500: A Dataset for Identity Documents. URL: https://arxiv.org/pdf/1807.05786.pdf (дата обращения: 20.10.2018).

Artaud C., Sidère N., Doucet A., Ogier J.-M., Poulain V. Find it! Fraud Detection Contest Report. 24th International Conference on Pattern Recognition (ICPR 2018). 2018.

Awal A.-M., Ghanmi N., Sicre R., Furon T. Complex Document Classification and Localization Application on Identity Document Images. 14th IAPR International Conference on Document Analysis and Recognition (ICDAR 2017). 2017. P. 426–431. DOI: 10.1109/ICDAR.2017.77.

Baluja S. Learning typographic style.URL: https://arxiv.org/pdf/1603.04000 (дата обращения 20.10.2018).

Berenguel A., Terrades O.R., Llados J., Canero C. Banknote Counterfeit Detection through Background Texture Printing Analysis. 12th IAPR Workshop on Document Analysis Systems (DAS). 2016. P. 66–71. DOI: 10.1109/das.2016.34.

Bertrand R., Terrades O.R., Gomez-Kramer P., Franco P., Ogier J.-M. A conditional random field model for font forgery detection.13th International Conference on Document Analysis and Recognition (ICDAR 2015). 2015. V. 576–580.

Bezmaternykh P.V., Nikolaev D.P., Arlazarov V.L. Textual Blocks Rectification Method Based on Fast Hough Transform Analysis in Identity Documents Recognition. Proc. SPIE 10696, *Tenth International Conference on Machine Vision* (ICMV 2017). 2018. V. 1069606. P. 1–6. DOI: 10.1117/12.2310162.

Boulkenafet Z., Akhtar Z., Feng X., Hadid A. Face Antispoofing in Biometric Systems.Biometric Security and Privacy. Ed. Jiang R. Springer. 2017. P. 299–321. DOI: 10.1007/978-3-319-47301-7_13.

Bulatov K., Arlazarov V.V., Chernov T., Slavin O., Nikolaev D. Smart IDReader: Document Recognition in Video Stream. 14th IAPR International Conference on Document Analysis and Recognition (ICDAR 2017). 2017. P. 39–44. DOI: 10.1109/ICDAR.2017.347.

Burie J.C., Chazalon J., Coustaty M., Eskenazi S., Luqman M.M., Mehri M., Nayef N., Ogier J.M., Prum S., Rusinol M. ICDAR 2015 competition on smartphone document capture and OCR (SmartDoc). Proc. of the Intl. Conf. on Document Analysis and Recognition (ICDAR 2015). 2015. P. 1161–1165.

Chazalon J., Gomez-Kramer P., Burie J.-C.,Coustaty M., Eskenazi S., Luqman M., Nayef N., Rusinol M., Sidere N., Ogier J.-M. SmartDoc 2017 Video Capture: Mobile Document Acquisition in Video Mode.Proc. of the Conf. on Document Analysis and Recognition (ICDAR 2017). 2017. DOI:10.1109/icdar.2017.306.

Chen G., Yang J., Jin H., Brandt J., Shechtman E., Agarwala A., Han T.X., Large-scale visual font recognition. Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2014).2014. P. 3598–3605. DOI: 10.1109/CVPR.2014.460.

Chernov T.S., Nikolaev D.P., Kliatskine V.M. A Method of Periodic Pattern Localization on Document Images.Proceedings SPIE 9875, Eighth International Conference on Machine Vision (ICMV 2015). 2015. V. 987504. P. 1–7. DOI: 10.1117/12.2228600.

Chernov T.S., Kolmakov S.I., Nikolaev D.P. An algorithm for detection and phase estimation of protective elements periodic lattice on document image. Pattern Recognition and Image Analysis. 2017. V. 27. № 1. P. 53–65. DOI: 10.1134/S1054661817010023.

Chernov T.S., Razumnuy N.P. Kozharinov A.S. Nikolaev D.P. Arlazarov V.V. Image quality assessment for video stream recognition systems.Proc. SPIE 10696, Tenth International Conference on Machine Vision (ICMV 2017). 2018. V. 106961U. P. 1–8. DOI: 10.1117/12.2309628.

Chernyshova Y.S., Gayer A.V., Sheshkus A.V. Generation method of synthetic training data for mobile OCR system. Proc. SPIE 10696, Tenth International Conference on Machine Vision (ICMV 2017). 106962G. P. 1–7. 2018. DOI: 10.1117/12.2310119.

Chernyshova Y.S., Aliev M.A., Sheshkus A.V. Optical font recognition in images captured with smartphones, and its applicability for detecting forgery of identity documents. URL: https://arxiv.org/abs/1810.08016 (дата обращения: 20.10.2018).

Cook S. Selfie banking: is it a reality? Biometric Technology Today. 2017. V. 3. P. 9–11.

Dewaele T., Diephuis M., Holotyak T., Voloshynovskiy S. Forensic authentication of banknotes on mobile phones. Electronic Imaging. 2016. V. 8. P. 1–8. DOI: 10.2352/issn.2470-1173.2016.8.mwsf-083.

Dittimi T.V., Suen C.Y. Mobile App for Detection of Counterfeit Banknotes. Lecture Notes in Computer Science. 2018. V. 10832. P. 156–168. DOI: 10.1007/978-3-319-89656-4_13.

Folego G., Angeloni M.A., Stuchi J.A., Godoy A., Rocha A. Cross-domain face verification: Matching ID document and self-portrait photographs.XII Workshop de Visão Computacional. 2016. P. 311–316.

Gaia K., Qiua M., Suna X. A survey on fintech.Journal of Network and Computer Applications. 2018. V. 103. P. 262–273.

Hartl A., Arth C., Grubert J., Schmalstieg D. Efficient Verification of Holograms Using Mobile Augmented Reality. Transactions on Visualization and Computer Graphics.2016. V. 22. № 7. P. 1843–1851.

Hartl A., Arth C., Schmalstieg D. AR-Based Hologram Detection on Security Documents Using a Mobile Phone. Lecture Notes in Computer Science. 2015. V. 8888. P. 335–346. DOI: 10.1007/978-3-319-14364-4_32.

Hartl A., Grubert J., Schmalstieg D., Reitmayr G. Mobile interactive hologram verification. Proceedings of the IEEE International Symposium on Mixed and Augmented Reality (ISMAR). 2013. P. 75–82.

Ilin D., Limonova E., Arlazarov V., Nikolaev D. Fast Integer Approximations In Convolutional Neural Networks Using Layer-By-Layer Training. Proceedings SPIE 10341, Ninth International Conference on Machine Vision (ICMV 2016). 2017. V. 103410Q. P. 1–5. DOI: 10.1117/12.2268722.

Kumar J., Ye P., Doermann D. A dataset for quality assessment of camera captured document images. Proc. of the International Workshop on Camera-Based Document Analysis and Recognition (CBDAR 2013). 2013. P. 113–125.

Kwon Y.-B., Kim J.-H. Recognition based verification for the machine readable travel documents. International Workshop on Graphics Recognition (GREC 2007). 2007.

Limonova E.E., Bezmaternykh P., Nikolaev D., Arlazarov V. Slant Rectification in Russian Passport OCR System Using Fast Hough Transform. Proceedings SPIE 10341, Ninth International Conference on Machine Vision (ICMV 2016). 2017. V. 10341. № 103410P. P. 1–5. DOI: 10.1117/12.2268725.

Nayef N., Luqman M., Prum S., Eskenazi S., Chazalon J., Ogier J.-M. SmartDoc-QA: A dataset for quality assessment of smartphone captured document imagessingle and multiple distortions. Proc. of the Conf. on Document Analysis and Recognition (ICDAR 2015). 2015. P. 1231–1235.

Ngoc M.O., Fabrizio J., Geraud T. Saliency-Based Detection of Identy Documents Captured by Smartphones. 13th IAPR International Workshop on Document Analysis Systems (DAS 2018). 2018. DOI: 10.1109/das.2018.17.

Oliveira J.S., Souza G.B., de Rezende R.A., de Deus F.E., Marana A.N. Cross-domain deep face matching for real banking security systems. URL: https://arxiv.org/abs/1806.07644 (дата обращения: 20.10.2018).

Puybareau E., Geraud T. Real-Time Document Detection in Smartphone Videos. 25th IEEE International Conference on Image Processing (ICIP 2018). 2018. DOI: 10.1109/icip.2018.8451533.

Rahman U., Sargano A., Bajwa U. Android-Based Verification System for Banknotes. Journal of Imaging. 2017. V. 3. № 54. DOI: 10.3390/jimaging3040054.

Satkhozhina A., Ahmadullin I., Allebach J. P. Optical font recognition using conditional random field. Proceedings of the 2013 ACM Symposium on Document Engineering (DocEng'13). 2013. P. 119–122. DOI: 10.1145/2494266.2494307.

Simon M., Rodner E., Denzler J. Fine-grained classification of identity document types with only one example. 14th IAPR International Conference on Machine Vision Applications (MVA 2015). 2015. P. 126–129. DOI: 10.1109/MVA.2015.7153149.

Shemyakina J., Zhukovskiy A., Nikolaev D. The Method for Homogrpahy Estimation between Two Planes Based on Lines and Points.Proc. SPIE 10696, Tenth International Conference on Machine Vision (ICMV 2017). 2018. V. 106961G. P. 1–20. DOI: 10.1117/12.2310111.

Sheshkus A., Limonova E., Nikolaev D., Krivtsov V. Combining Convolutional Neural Networks and Hough Transform for Classification of Images Containing Lines. Proceedings SPIE 10341, Ninth International Conference on Machine Vision (ICMV 2016).2017. V. 103411C. P. 1–5. DOI: 10.1117/12.2268717.

Sicre R., MontaserAwal A., Furon T. Identity documents classification as an image classification problem.19th International Conference on Image Analysis and Processing, (ICIAP 2017). 2017. P. 602–613. DOI: 10.1007/978-3-319-68548-9_55

Sidere N., Cruz F., Coustaty M., Ogier J.-M. A dataset for forgery detection and spotting in document images.Proc. of the Seventh International Conference on Emerging Security Technologies (EST 2017). 2017. P. 26–31. DOI: 10.1109/est.2017.8090394

Skoryukina N., Nikolaev D.P., Sheshkus A., Polevoy D. Real time rectangular document detection on mobile devices. Proc. SPIE 9445, Seventh International Conference on Machine Vision (ICMV 2014). 2015. V. 94452A. P. 1–6.

Skoryukina N., Shemyakina J., Arlazarov V.L., Faradzhev I. Document localization algorithms based on feature points and straight lines. Proc. SPIE 10696, Tenth International Conference on Machine Vision (ICMV 2017). 2018. V. 106961H. P. 1–8. DOI: 10.1117/12.2311478.

Usilin S., Nikolaev D., Postnikov V., Schaefer G. Visual appearance based document image classification. Proc. of the IEEE International Conference on Image Processing. 2010. P. 2133–2136. DOI: 10.1109/ICIP.2010.5652024.

Vironit. A Real-time Document Recognition SDK Comparison.URL: https://vironit.com/a-real-time-document-recognition-sdk-comparison (дата обращения: 20.10.2018).

Wang X. Bissacco A., Berntson G., Nazif M., Scheiner J., Shih S., Snyder M., Talavera D. Client side filtering of card OCR images. Patent US. № 8,903,136. 2014.

Wang Z., Yang J., Jin H., Shechtman E., Agarwala A., Brandt J., Huang T.S. DeepFont, Identify your font from an image. In Proceedings of the 23rd ACM International Conference on Multimedia. 2015. P. 451–459.

Wang Z. Deep Learning for Font Recognition and Retrieval.Applied Cloud Deep Semantic Recognition Advanced Anomaly Detection. 2018. Auerbach Publications. P. 109–130.

Williem C. Simon, Cho S., Park I. K. Fast and Robust Perspective Rectification of Document Images on a Smartphone. Proc. IEEE (CVPRW 2014). 2014. P. 197–198.

Winarski T.Y. Selfie financial security transaction system. Patent US. No. US20160071101A1. 2016.

Xu Y., Carlinet E., Géraud T., Najman L. Hierarchical Segmentation Using Tree-Based Shape Spaces. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2017. V. 39. № 3. P. 457–469.

Zhukovsky A., Nikolaev D., Arlazarov V., Postnikov V., Polevoy D., Skoryukina N., Chernov T., Shemiakina J., Mukovozov A., Konovalenko I., Povolotsky M. Segments Graph-Based Approach for Document Capture in a Smartphone Video Stream. Proceedings of the International Conference on Document Analysis and Recognition (ICDAR). 2017. V. 1. P. 337–342. DOI: 10.1109/ICDAR.2017.63.

Zramdini A., Ingold R. Optical font recognition using typographical features. IEEE Trans. Pattern Anal. Mach. Intell. 1998. V. 20. P. 877–882.