НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
июль–август 2017 Том 17 № 4 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
July–August 2017 Vol. 17 No 4 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.932.2

ПРИМЕНЕНИЕ СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ПРОТИВОДЕЙСТВИЯ АТАКЕ СПУФИНГА В СИСТЕМАХ ЛИЦЕВОЙ БИОМЕТРИИ

С.С. Волкова[a], Ю.Н. Матвеев[b,c]

[a] ООО «Простые решения», Москва, 105318, Российская Федерация
[b] ООО «ЦРТ-инновации», Санкт-Петербург, 196084, Российская Федерация
[c] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: malysheva.svetlana.s@gmail.com

Информация о статье
Поступила в редакцию 05.05.17, принята к печати 07.06.17
doi: 10.17586/2226-1494-2017-17-4-702-710
Язык статьи – русский

Ссылка для цитирования: Волкова С.С., Матвеев Ю.Н. Применение сверточных нейронных сетей для решения задачи противодействия атаке спуфинга в системах лицевой биометрии // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 4. С. 702–710. doi: 10.17586/2226-1494-2017-17-4-702-710

Аннотация

Предмет исследования. Предложен метод обнаружения ситуации, в которой при лицевой аутентификации один человек маскируется под другого путем подмены его лица фотографией или отображаемым видеороликом. **Метод.** Задача решается в два последовательных этапа. На первом этапе проводится выделение вектора лицевых признаков. На втором этапе проводится классификация и определение, насколько получаемый кадр (или группа кадров) похож на то, что перед камерой находится человек, а не его фотография или видео. Вектор лицевых признаков извлекается с помощью сверточной нейронной сети. Классификация реализуется путем использования машины опорных векторов. На вход методу можно подавать как один, так и группу кадров. **Основные результаты.** Предложенное в работе решение задачи противодействия атаке спуфинга дает возможность работать как с реальными лицами, полученными с низким качеством, так и с поддельными лицами, отображаемыми на дисплеях высокой четкости, что подтверждено экспериментами на двух общедоступных тестовых базах. Проведенные эксперименты показали, что среднее значение ошибок первого и второго рода на тестовых данных не превышает 9%, а точность достигает более 91%. Результаты классификации сопоставимы с лучшими результатами, показанными при использовании других известных методов обнаружения атак спуфинга на этих же тестовых базах. **Практическая значимость.** Предложенный метод может быть применен для повышения качества аутентификации лицевыми биометрическими системами, а также для разработки мультимодальных биометрических систем.

Ключевые слова
атака спуфинга, биометрия, безопасность, лицо, нейронная сеть

CONVOLUTIONAL NEURAL NETWORKS FOR FACE ANTI-SPOOFING

S.S. Volkova[a], Yu.N. Matveev [b,c]

[a] Smilart UG, Moscow, 105318, Russian Federation
[b] "STC-Innovations" Ltd., Saint Petersburg, 196084, Russian Federation
[c] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: malysheva.svetlana.s@gmail.com

Article info
Received 05.05.17, accepted 07.06.17
doi: 10.17586/2226-1494-2017-17-4-702-710
Article in Russian

For citation: Volkova S.S., Matveev Yu.N. Convolutional neural networks for face anti-spoofing. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, vol. 17, no. 4, pp. 702–710 (in Russian). doi: 10.17586/2226-1494-2017-17-4-702-710

Abstract

Subject of Research. We propose the method for detecting an incident at face authentication when imposter tries to disguise himself as a real client. He tries to falsify the client's face by photo or video. **Method.** The face anti-spoofing method involves two successive steps. Obtaining facial features takes place at the first stage. Classification is performed at the second stage for making a decision if the real person or an imposter is in front of the camera. Facial features are extracted with the use of deep convolutional neural network. Classification is realized by support vector machine. One frame or a group of

frames can become the input data for the method. **Main Results.** The proposed method for anti-spoofing gives the possibility to work with both real faces obtained with low quality and with fake faces displayed on high-resolution displays. It is confirmed by experiments on two available test datasets. Experiments show that the average value of the first and second kind errors on the test data does not exceed 9%, and the accuracy reaches values over 91%. Classification results are comparable with the best results shown when applying the other known techniques for detecting spoofing attacks on the same test bases. **Practical Relevance.** The proposed method can be applied to improve the quality of face authentication systems, as well as for the development of multimodal biometric systems.

Keywords
spoofing attack, biometrics, security, face, neural network

Введение

Биометрические технологии распознавания людей в последнее время активно развиваются и находят применение в системах контроля и управления доступом, в системах анализа человеческого трафика, системах поиска злоумышленников в местах большого скопления людей. Биометрические системы распознавания людей позволяют идентифицировать личность по уникальным физическим характеристикам, таким как отпечатки пальцев, изображение лица, голос [1]. Биометрические системы используются там, где требуется высокий уровень безопасности, благодаря своим преимуществам по сравнению с обычными методами контроля: паспорт, специальные пластиковые карты и жетоны, PIN-коды и т.д. [2]. Особенно привлекательны технологии, основанные на изображении лица. По сравнению с другими методами биометрического контроля технологии, основанные на распознавании лица, не требуют непосредственного контакта с оборудованием.

Несмотря на то, что многие исследователи [3–7] работали над проблемой распознавания лиц в течение многих лет, существует еще ряд проблем, которые необходимо решить. Одна из таких проблем – противодействие атаке спуфинга, т.е. попытке подмены биометрической характеристики, обмана биометрической системы путем представления сенсору поддельного объекта идентификации [8]. Неавторизованные клиенты (злоумышленники) могут попытаться обмануть систему распознавания лиц (Face Recognition System, FaReS) путем подмены «живого» изображения лица авторизованного клиента его фотографией или видео. Несмотря на простоту, такие атаки, как правило, довольно успешны, и до сих пор нет эффективных алгоритмов, способных противодействовать этим атакам. Однако положительной тенденцией является то, что в настоящее время исследователи начинают фокусироваться на данном вопросе [9–12].

Для решения задачи противодействия атаке спуфинга в работах [13, 14] рассматривались методы, использующие дополнительные датчики или трехмерные сканеры. Несмотря на достигнутые высокие показатели эффективности, применение этих методов затрудняется необходимостью использования специального оборудования. Методы без дополнительных устройств и участия человека предпочтительнее, поскольку они могут быть легко интегрированы в существующую систему распознавания лиц, которая, как правило, оборудована только камерой. В подобных (неинвазивных) методах обычно используются характеристики движения, действий и текстуры [15].

При анализе движения используют тот факт, что движение плоских 2D-объектов существенно отличается от движения реального человеческого лица, которое является 3D-объектом. В работе [16] были проанализированы различия в свойствах оптического потока, генерируемого трехмерными объектами и двумерными плоскостями. В работе [17] авторы оценивают траекторию движения отдельных частей лица, используя небольшую последовательность изображений и упрощенный анализ оптического потока. Основная идея метода основывается на предположении, что центральная часть лица движется иначе, чем периферийная его часть (например, в районе уха). Следует отметить, что подход, основанный на анализе движения, может не дать должного качества в случае, когда информации о движении недостаточно. Например, ошибка может возникать при анализе зашумленных изображений и изображений с низким разрешением.

Признаки действия, в зависимости от способа взаимодействия с пользователем, можно условно разделить на два типа: требующие обратной связи (например, выполнить распоряжение «открыть рот в определенный момент», так сказать, предъявить «пароль движения») и не требующие от него определенной активности, т.е. базирующиеся на действиях, не зависящих от внешних указаний (например, самопроизвольное моргание). Так, в [18] был предложен метод, основанный на анализе моргания. В [19] авторы проанализировали движения глаз и обучили модель движения с использованием машины опорных векторов. В работе [20] предложен метод, в котором витальность лица определяется по губам. Витальность в применении к биометрическим системам означает, что с системой контактирует «живой» человек. Признаки действия очень сложно подделать с помощью фотографии или трехмерной скульптуры головы человека. Тем не менее, этот подход может потребовать взаимодействия с пользователем и в значительной степени зависит от качества обнаружения черт лица. Методы, основанные на анализе движения и анализе действий без обратной связи, также могут быть неэффективны в случае использования видеозаписи объекта идентификации.

Подходы, основанные на анализе текстуры, позволяют обнаружить особенности текстуры, не характерные для «живого» человека, которые могут возникнуть, например, в случае сбоев при печати или из-за общей размытости фотографии. Так, в работе [21] информация о текстуре была вычислена с помощью локальных бинарных шаблонов. В отличие от предыдущих двух подходов, анализ текстуры не требует взаимодействия с пользователем и прост в реализации. Этот подход работает на предположении, что поддельные изображения лица печатаются на бумаге, а процесс печати и структура бумаги порождают изменения в текстуре, что позволяет отличать напечатанные изображения от реальных лиц [22].

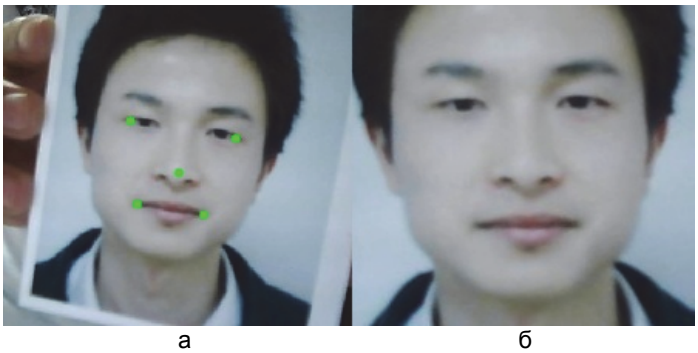
Тем не менее, эти предположения могут не быть истинными в некоторых случаях. Например, с развитием дисплеев сверхвысокой четкости вероятность того, что воспроизведение интенсивности цветов на дисплее близко к реальным значениям цветов, растет. Иначе говоря, атака может быть выполнена с помощью снимка, отображаемого на экране, а не на бумаге, что приведет к трудностям в различении текстур изображения живого человека и подделки. Таким образом, атака спуфинга с использованием видеозаписи лица, воспроизведенной на дисплее высокой четкости, будет становиться все более распространенным явлением. Следовательно, при разработке и тестировании методов определения витальности лиц следует обратить более пристальное внимание на эту схему спуфинга.

С учетом всего вышеизложенного в работе предлагается новый метод противодействия атаке спуфинга. Метод основывается на анализе текстуры и не требует анализа нескольких кадров. Решение может быть принято по одному изображению лица. Подход базируется на обучении сверточной нейронной сети для извлечения вектора лицевых признаков и дальнейшей классификации с использованием машины опорных векторов, что позволяет с высокой точностью разделять истинные и поддельные изображения лиц.

Предлагаемый метод

В предложенном методе противодействия атаке спуфинга определяется, насколько получаемый кадр (или группа кадров) похож на то, что перед камерой находится человек, а не его фотография или видео. Если на вход методу подается несколько изображений, то итоговое значение вероятности вычисляется как среднее значение по всем изображениям. Предлагаемый в работе метод основывается на использовании сверточной нейронной сети для получения вектора признаков и машины опорных векторов для классификации.

Исходные данные, подаваемые на вход сети, представляют собой изображения лица размером 224×224 пикселя. Все изображения лиц проходят блок геометрической нормализации в соответствии с координатами контрольных точек.



а б

Рис. 1. Выравнивание изображения лица: результат поиска контрольных точек (а); результат нормализации изображения лица (б)

Пять контрольных точек, используемых для нормировки, изображены на рис. 1, а, их находим с использованием метода, описанного в работе [23]. Затем изображение нормализуем таким образом, чтобы линия между точками глаз была горизонтальна. Значение расстояния между линией глаза и линией губ фиксируется равной 70 пикселям. Нормализованное изображение лица показано на рис. 1, б.

В качестве нейросетевой архитектуры для получения вектора признаков предложена сверточная нейронная сеть модели AlexNet [24], содержащая 5 сверточных слоев и 3 полносвязных слоя. AlexNet первоначально была разработана для классификации по базе ImageNet [25], которая, в свою очередь, предназначена для классификации изображений с большим числом категорий. Предложенная архитектура отличается от архитектуры AlexNet параметрами слоев. В табл. 1 представлены параметры предложенной архитектуры нейронной сети и архитектуры сети AlexNet. Предложенная архитектура нейронной сети представлена на рис. 2. Выходом данной модели является вектор $[\mathbf{p}_0, \mathbf{p}_1]$, элементы которого характеризуют вероятность попадания исходного изображения в соответствующий класс – «живое» лицо или поддельное.

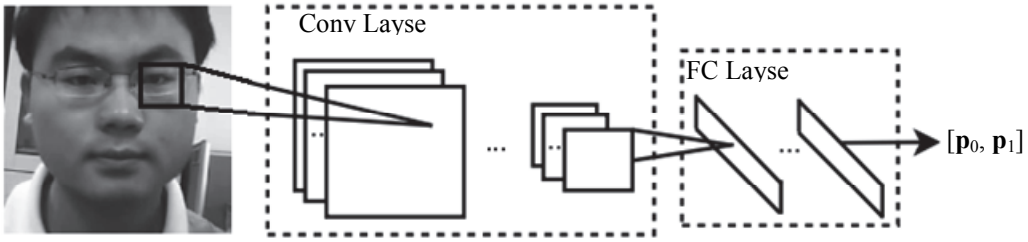


Рис. 2. Архитектура предложенной нейронной сети

Тип слоя, имя	**Предложенная сеть**		**AlexNet**	
	Размер ядра / шаг, пикс	**Выходной размер**, (ширина, пикс) × (высота, пикс) × (количество)	**Размер ядра/ шаг**, пикс	**Выходной размер,** (ширина, пикс) × (высота, пикс) × количество
Input	–	224×224×3	–	227×227×3
Conv-1 ReLU-1 LRN	7×7/2 – –	109×109×96 109×109×96 109×109×96	11×11/4 – –	55×55×96 55×55×96 55×55×96
Pool-1	3×3/3	37×37×96	3×3/3	27×27×96
Conv-2 ReLU-2 LRN2	5×5/2 – не используется	37×37×256 37×37×256 не используется	5×5/2 – –	27×27×256 27×27×256 27×27×256
Pool - 2	2×2/2	19×19×256	2×2/2	13×13×256
Conv-3 ReLU-3	3×3/1 –	19×19×512 19×19×512	3×3/1 –	13×13×384 13×13×384
Conv-4 ReLU-4	3×3/1 –	19×19×512 19×19×512	3×3/1 –	13×13×384 13×13×384
Conv-5 ReLU-5	3×3/1 –	19×19×512 19×19×512	3×3/1 –	13×13×256 13×13×256
Pool-5	3×3/3	7×7×512	3×3/2	6×6×256
FC-6 ReLU-6 Drop-6	– – –	1×1×4048 1×1×4048 1×1×4048	– – –	1×1×4096 1×1×4096 1×1×4096
FC-7 ReLU-7 Drop-7	– – –	1×1×4048 1×1×4048 1×1×4048	– – –	1×1×4096 1×1×4096 1×1×4096
FC-8	–	1×1×2	–	1×1×2

Таблица 1. Параметры архитектур предложенной сети и сети AlexNet

В табл. 1 приняты следующие обозначения:

- Conv – convolutional layer – сверточный слой;
- PeLU – Rectified-Linear Unit – блок линейной ректификации, функция активации, имеющая вид $f(x) = \max(0, x)$;
- LRN – Local Response Normalization – слой локальной нормализации;
- Pool – pooling layer – слой пространственного объединения;
- FC – fully connected layer – полносвязный слой;
- Drop – dropout-регуляризации, прореживание сети путем отключения нейронов сети с заданной вероятностью.

Для обучения сети выбран алгоритм стохастического градиентного спуска [26]. Обучение сети проводилось с использованием баз лиц CASIA [27], OULU [28] и собственной базы данных. Собственная

база данных включает 6635 поддельных лиц и 7047 истинных лиц. Истинные лица собственной базы выбраны из базы CASIA-WebFace [29], предназначенной для обучения систем идентификации лиц, фотографии поддельных лиц получены с использованием камер двух мобильных устройств (iPhone5, Xiaomi RedMe 3S). Образцы поддельных лиц были взяты из напечатанных журналов и отображаемых на экране монитора фильмов. Всего обучающая выборка содержит 10811 изображений лиц, валидационная – 994 изображений лиц. Для обучения модели используется Caffe [30] – библиотека с открытым исходным кодом, разрабатывается командой Berkeley Vision and Learning Center и предназначенная для научных разработок в сфере компьютерного зрения. Входной слой принимает цветное изображение размером 224×224 пикселей. Для повышения качества сети использовалась аугментация (augmentation, «раздутие») – добавление искаженных изображений в выборку с целью увеличения разнообразия данных. Было задействовано такое преобразование, как отражение. Подобная процедура позволяет улучшить обобщающую способность сверточной нейронной сети, а также предотвратить переобучение [24]. Коэффициент скорости обучения сначала устанавливается в 10^{-4} и постепенно уменьшается до 10^{-5}.

В процессе обучения нейронная сеть настраивает веса таким образом, чтобы минимизировать эмпирический риск – функционал качества, характеризующий среднюю ошибку алгоритма a на обучающей (валидационной) выборке, который определяется по следующей формуле:

$$Q\left(a, X^m\right) = \frac{1}{m}\sum_{i=1}^{m} \Im\left(y_i, y^*\left(x_i\right)\right),$$

где $y^*: X \to Y$ – отображение множества описаний объектов X в множество допустимых ответов Y, неизвестная целевая зависимость, значения которой известны только на объектах конечной обучающей выборке $X^m = \{(x_1, y_1), ..., (x_m, y_m)\}$ размерности m, $\Im\left(y_i, \hat{y}\right)$ – функция потерь, характеризующая величину отклонения ответа $y = a(x)$ от верного ответа $\hat{y} = y^*\left(x\right)$, для произвольного объекта $x \in X$.

В качестве функции потерь используем перекрестную энтропию, которая имеет вид $\Im\left(y_i, \hat{y}\right) = -\sum_{j=1}^{K} y_{ij}^* \log(y_{ij})$. Графики изменения значения средней ошибки на обучающей и валидационной выборках представлены на рис. 3.

После обучения сети вектор лицевых признаков извлекается из первого полносвязного слоя. Для классификации полученного вектора признаков используем машину опорных векторов. Для обучения классификатора необходимо определить тип функции ядра $k(x, x')$, значение параметров ядра и значение параметра регуляризации C, позволяющего найти компромисс между максимизацией ширины полосы, разделяющей классы, и минимизацией суммарной ошибки.

Параметры обучения модели машины опорных векторов выбраны следующие:

– ядро на основе радиальных базисных функций (RBF): $k(x, x') = \exp(-\gamma \left\| x - x' \right\|^2)$;

– значение параметра гамма: $\gamma = \frac{1}{n\_feature} = 2{,}47 \cdot 10^{-4}$;

– значение параметра регуляризации: $C = 1$.

Обучение классификатора осуществляется с использованием второй части базы OULU [28].

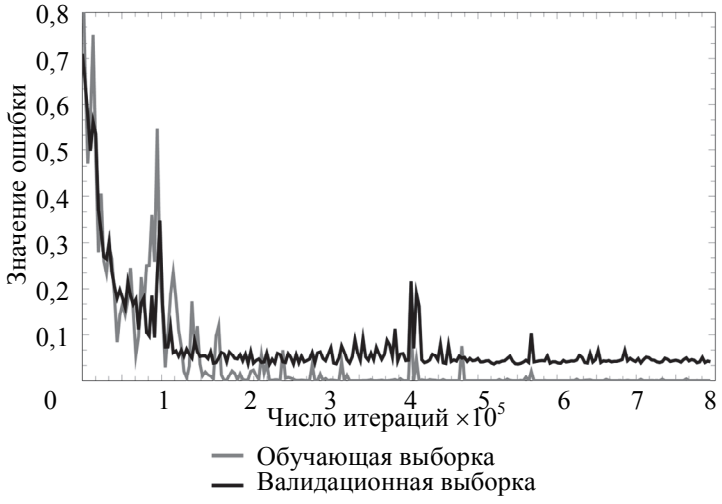


Рис. 3. Изменение значения средней ошибки на обучающей и валидационной выборках в зависимости от числа итераций

Результаты экспериментов

В настоящей работе эксперименты реализованы на двух наборах данных: NUAA PI DB [31] и CASIA [27]. В этих наборах данных моделируются различные типы атак спуфинга.

База данных CASIA содержит изображения лиц 50 человек. Для каждого человека были получены изображения лица с низким, средним и высоким качеством. Поддельные лица имитируют три вида атак: деформированное фото (злоумышленник предъявляет камере напечатанную фотографию, намеренно ее искажая, пытаясь симулировать движение лица), частично вырезанное фото (из фотографии вырезаются глаза, злоумышленник прячется за фотографией и имитирует моргание) и с использованием видео (камере предъявляется iPad, на котором транслируется видео высокого качества). В результате для каждого человека имеется 12 видеопоследовательностей (3 истинных лица и 9 поддельных). Общее число последовательностей в базе – 600, из них 240 используются для обучения, 360 – для тестирования.

База данных NUAA PI DB содержит изображения 15 человек и разделена на три сессии согласно различным условиям освещения. Объем данных между сессиями не сбалансирован, так как не все люди принимали участие во всех трех сессиях. При съемке участнику было предложено смотреть фронтально на веб-камеру, имея нейтральное выражение лица, избегая движения головы или моргания, что позволяет быть максимально похожим на фотографию. Камера записывает ролик длительностью 25 секунд со скоростью 20 кадров в секунду (FPS). Для скачивания доступна не исходная последовательность видео, а изображения, выбранные из нее. Изображения для атаки спуфинга были собраны для тех же участников. Человек фотографировался с использованием камеры Canon таким образом, чтобы его лицо занимало 1/3 изображения. Затем фотографии были напечатаны и предъявлены камере с перемещением во время захвата кадра.

По результатам выполненных экспериментов были построены DET-кривые, представленные на рис. 4. Оценивалось 2 типа ошибок:

1. ошибка ложного принятия фотографии (видео), установленной перед экраном, за живого пользователя FA (False Accept);
2. ошибка ложного принятия живого пользователя за его изображение (видео) FR (False Reject).

Среднее значение ошибок первого и второго рода (Half Total Error Rate, HTER) и точность (Accuracy, доля входных данных, отнесенных к правильному классу) для предложенного метода противодействия атаке спуфинга, а также сравнение предложенного метода с существующими подходами представлены в табл. 2 и 3.

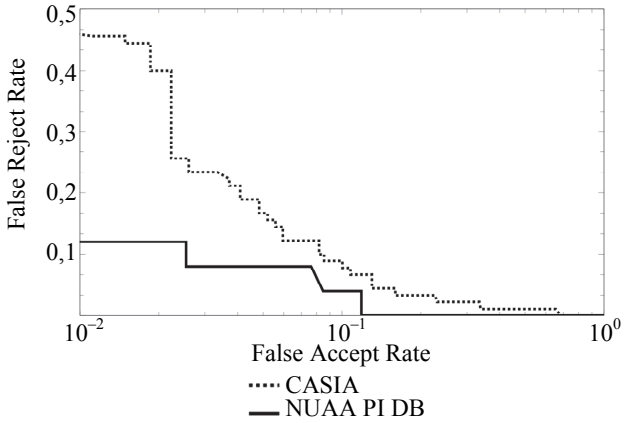


Рис. 4. DET-кривые для метода противодействия атаке спуфинга
На базах NUAA PI DB и CASIA

Метод	**Оценки эффективности**	
	HTER, %	**Accuracy**, %
Sparse logistic regression + DoG filter	–	87,5 [31]; 93 [32]
LBP + SVM [33]	19,03	–
LBP + DoG filter [34]	11,97	–
LBP + Linear discriminant analysis [35]	18,32	–
Предложенный метод	5,27	96,5

Таблица 2. Сравнение эффективности методов противодействия атаке спуфинга на базе NUAA PI DB

Метод	Оценки эффективности	
	HTER, %	**Accuracy**, %
LBP + Linear discriminant analysis [35]	21,01	–
LBP + SVM [33]	18,17	–
LBP [35]	18,21	–
LBP-TOP	10	–
Предложенный метод	8,71	91,39

Таблица 3. Сравнение эффективности методов противодействия атаке спуфинга на базе CASIA

В результате можно сделать вывод, что предложенная архитектура сверточной сети, а также выбранные обучающие данные позволяют с высокой точностью определять попытки атак спуфинга по изображению лица.

Заключение

В работе рассмотрена задача противодействия атаке спуфинга в системах лицевой биометрии. Рассмотрены существующие способы подмены биометрических характеристик, а также методы, направленные на противодействие спуфингу в лицевых биометрических системах, выявлены их недостатки. На основании анализа этих недостатков предложен метод, результаты работы которого сопоставимы с лучшими результатами, показанными при использовании других известных методов обнаружения атак спуфинга.

Предложенное решение задачи противодействия атаке спуфинга заключается в последовательном выполнении двух этапов анализа – этапа выделения лицевых признаков и этапа классификации для определения, насколько предъявляемый кадр (или группа кадров) похож на то, что перед нами находится реальный человек, а не его фотография или видео.

В рамках решения первой подзадачи, связанной с выделением лицевых признаков, в работе было предложено использование сверточной нейронной сети, содержащей 5 сверточных и 3 полносвязных слоя. Описан алгоритм ее обучения, а также используемые для обучения и валидации данные. В рамках решения второй подзадачи, связанной с принятием решения об отнесении полученного вектора признаков к одному из классов, в работе предлагается использовать машину опорных векторов с ядром на основе радиальных базисных функций.

Программная реализация, полученная в рамках решения основной задачи исследования, позволяет использовать предложенное решение как при анализе одного кадра, так и при анализе группы кадров.

Проведенные эксперименты показали, что среднее значение ошибок первого и второго рода на тестовых данных не превышает 9%, а точность достигает значения более 91%.

Дальнейшее развитие нейросетевого метода для решения противодействия атаке спуфинга возможно за счет использования рекуррентных нейронных сетей для дополнительного анализа связей между несколькими кадрами.

Литература

1. Матвеев Ю.Н. Технологии биометрической идентификации личности по голосу и другим модальностям // Инженерный журнал: наука и инновации. 2012. №3. С. 46–61.
2. Physical access control biometrics [Электронный ресурс]. Режим доступа: http://www.findbiometrics.com/physical-access/, свободный. Яз. англ. (дата обращения 05.05.2017).
3. Кухарев Г.А., Каменская Е.И., Матвеев Ю.Н., Щеголева Н.Л. Методы обработки и распознавания изображений лиц в задачах биометрии / Под ред. М.В. Хитрова. СПб: Политехника, 2013. 388 с.
4. Li S.Z., Jain A.K. Handbook of Face Recognition. London: Springer-Verlag, 2011. 724 p. doi: 10.1007/978-0-85729-932-1
5. De Marsico M., Nappi M., Tistarelli M. Face Recognition in Adverse Conditions. IGI Global, 2014. 480 p. doi: 10.4018/978-1-4666-5966-7
6. Bourlai T. Face Recognition Across the Imaging Spectrum. Springer, 2016. 383 p. doi: 10.1007/978-3-319-28501-6
7. Datta A.K., Datta M., Banerjee P.K. Face Detection and Recognition: Theory and Practice. Chapman and Hall/CRC, 2015. 326 p. doi: 10.1201/b19349
8. Ojala T., Pietikainen M., Maenpaa T. Multiresolution gray-scale and rotation invariant texture classification with local binary

References

1. Matveev Y.N. Technologies of biometric identification of a person by voice and other modalities. *Engineering Journal: Science and Innovation*, 2012, no. 3, p. 46–61. (In Russian)
2. *Physical access control biometrics*. Available at: http://www.findbiometrics.com/physical-access (accessed 05.05.2017).
3. Kukharev G.A., Kamenskaya E.I., Matveev Y.N., Shchegoleva N.L. *Methods for Face Image Processing and Recognition in Biometric Applications* / Ed. M.V. Khitrov. St. Petersburg, Politekhnika Publ., 2013, 388 p.
4. Li S.Z., Jain A.K. *Handbook of Face Recognition*. London, Springer-Verlag, 2011, 724 p. doi: 10.1007/978-0-85729-932-1
5. De Marsico M., Nappi M., Tistarelli M. *Face Recognition in Adverse Conditions*. IGI Global, 2014, 480 p. doi: 10.4018/978-1-4666-5966-7
6. Bourlai T. *Face Recognition Across the Imaging Spectrum*. Springer, 2016, 383 p. doi: 10.1007/978-3-319-28501-6
7. Datta A.K., Datta M., Banerjee P.K. *Face Detection and Recognition: Theory and Practice*. Chapman and Hall/CRC, 2015, 326 p. doi: 10.1201/b19349
8. Ojala T., Pietikainen M., Maenpaa T. Multiresolution gray-scale and rotation invariant texture classification with local

patterns // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2002. V. 24. N 7. P. 971–987. doi: 10.1109/TPAMI.2002.1017623
9. Shyama V.S., Mary Linda P.A. A survey on facial spoofing detection // International Journal of Science, Engineering and Technology Research. 2016. V. 5. N 1. P. 49–53.
10. Marcel S., Nixon M.S., Li S.Z. Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks. Springer, 2014. 281 p. doi: 10.1007/978-1-4471-6524-8
11. Galbally J., Marcel S., Fierrez J. Biometric antispoofing methods: a survey in face recognition // IEEE Access. 2014. V. 2. P. 1530–1552. doi: 10.1109/ACCESS.2014.2381273
12. Parveen S., Syed Ahmad, S.M., Hanafi M., Wan Adnan W.A. Face anti-spoofing methods // Current Science. 2015. V. 108. N 8. P. 1491–1500. doi: 10.18520/cs/v108/i8/1491-1500
13. Костылев Н.М., Горевой А.В. Модуль определения витальности лица по спектральным характеристикам отражения кожи человека // Инженерный журнал: наука и инновации. 2013. № 9 (21). С. 47–60. doi: 10.18698/2308-6033-2013-9-925
14. Lagorio A., Tisterelli M., Cadoni M. et. al. Liveness detection based on 3D face shape analysis // Proc. International Workshop on Biometrics and Forensics, IWBF. Lisbon, Portugal, 2013. Art. 657310. doi: 10.1109/IWBF.2013.6547310
15. Chakarborty S., Das D. An overview of face liveness detection // International Journal on Information Theory. 2014. V. 3. N 2. P. 11–25.
16. Bao W., Li H., Li n., Jiang W. A liveness detection method for face recognition based on optical flow field // Proc. Int. Conf. of Image Analysis and Signal Processing. Tiazhou, China, 2009. P. 233–236. doi: 10.1109/IASP.2009.5054589.
17. Kollreider K., Fronthaler M., Bigun J. Evaluating liveness by face images and structure tensor // Proc. 4th IEEE Workshop on Automatic Identification Advanced Technologies. Washington, USA, 2005. P. 75–80. doi: 10.1109/AUTOID.2005.20
18. Jee H.-K., Jung S.-U., Yoo J.-H. Liveness detection for embedded face recognition system // International Journal of Biomedical Sciences. 2006. V. 1. N 4. P. 235.
19. Deng G., Coo B., Miao J. et al. Liveness check algorithm based on eye movement model using SVM // Journal of Computer Aided Design and Computer Graphics. 2003. V. 15. N 7. P. 853–857.
20. Kollreider K., Fronthaler M., Faraj M.I., Bigun J. Real-time face detection and motion analysis with application in liveness assessment // IEEE Transactions on Information Forensics and Security. 2007. V. 2. N 3. P. 548–558. doi: 10.1109/TIFS.2007.902037
21. Kim G., Eum S., Suhr J.K. et al. Face liveness detection based on texture and frequency analyses // Proc. 5th IAPR Int. Conf. on Biometrics (ICB). New Deli, India, 2012. P. 67–72. doi: 10.1109/ICB.2012.6199760
22. Yang J., Lei Z., Liao S., Li S.Z. Face liveness detection with component dependent descriptor // Proc. Int. Conf. on Biometrics (ICB). Madrid, Spain, 2013. doi: 10.1109/ICB.2013.6612955
23. Xiong X., De la Torre F. Supervised descent method and its applications to face alignment // Proc. 26th IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Portland, USA, 2013. P. 532–539. doi: 10.1109/CVPR.2013.75
24. Krizhevsky A., Sutskever I., Hinton G.E. ImageNet classification with deep convolutional neural networks // Advances in Neural Information Processing Systems. 2012. V. 2. P. 1097–1105.
25. Deng J., Dong W., Socher R., Li L., Li K., Fei-Fei L. ImageNet: a large-scale hierarchical image database // Proc. IEEE Conference on Computer Vision and Pattern Recognition. Miami, USA, 2009. doi: 10.1109/cvprw.2009.5206848
26. LeCun Y., Bottou L., Orr G.B., Muller K.R. Efficient BackProp // Lecture Notes in Computer Science. 1998. V. 1524. P. 9–50. doi: 10.1007/3-540-49430-8_2.
27. Zhang Z., Yan J., Liu S., Lei Z., Yi D., Li S.Z. A face antispoofing database with diverse attacks // Proc. 5th IAPR Int. Conf. on Biometrics (ICB). New Delhi, India, 2012. P. 26–31. doi: 10.1109/ICB.2012.6199754.
28. Zinelabidine B., Jukka K., Li L., Feng X., Hadid A. OULU-NPU: a mobile face presentation attack database with real-world variations // Proc. IEEE Int. Conf. on Identity, Security and

binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2002, vol. 24, no. 7, pp. 971–987. doi: 10.1109/TPAMI.2002.1017623
9. Shyama V.S., Mary Linda P.A. A survey on facial spoofing detection. *International Journal of Science, Engineering and Technology Research*, 2016, vol. 5, no. 1, pp. 49–53.
10. Marcel S., Nixon M.S., Li S.Z. *Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks*. Springer, 2014, 281 p. doi: 10.1007/978-1-4471-6524-8
11. Galbally J., Marcel S., Fierrez J. Biometric antispoofing methods: a survey in face recognition. *IEEE Access*, 2014, vol. 2, pp. 1530–1552. doi: 10.1109/ACCESS.2014.2381273
12. Parveen S., Syed Ahmad, S.M., Hanafi M., Wan Adnan W.A. Face anti-spoofing methods. *Current Science*, 2015, vol. 108, no. 8, pp. 1491–1500. doi: 10.18520/cs/v108/i8/1491-1500
13. Kostylev N.M., Gorevoy A.V. The liveness detection module based on spectral reflection characteristics of facial skin. *Engineering Journal: Science and Innovation*, 2013, no. 9, pp. 47–60. (In Russian) doi: 10.18698/2308-6033-2013-9-925
14. Lagorio A., Tisterelli M., Cadoni M. et. al. Liveness detection based on 3D face shape analysis. *Proc. International Workshop on Biometrics and Forensics, IWBF*. Lisbon, Portugal, 2013, art. 657310. doi: 10.1109/IWBF.2013.6547310
15. Chakarborty S., Das D. An overview of face liveness detection. *International Journal on Information Theory*, 2014, vol. 3, no. 2, pp. 11–25.
16. Bao W., Li H., Li n., Jiang W. A liveness detection method for face recognition based on optical flow field. *Proc. Int. Conf. of Image Analysis and Signal Processing*. Tiazhou, China, 2009, pp. 233–236. doi: 10.1109/IASP.2009.5054589.
17. Kollreider K., Fronthaler M., Bigun J. Evaluating liveness by face images and structure tensor. *Proc. 4th IEEE Workshop on Automatic Identification Advanced Technologies*. Washington, USA, 2005, pp. 75–80. doi: 10.1109/AUTOID.2005.20
18. Jee H.-K., Jung S.-U., Yoo J.-H. Liveness detection for embedded face recognition system. *International Journal of Biomedical Sciences*, 2006, vol. 1, no. 4, pp. 235.
19. Deng G., Coo B., Miao J. et al. Liveness check algorithm based on eye movement model using SVM. *Journal of Computer Aided Design and Computer Graphics*, 2003, vol. 15, no. 7, pp. 853–857.
20. Kollreider K., Fronthaler M., Faraj M.I., Bigun J. Real-time face detection and motion analysis with application in liveness assessment. *IEEE Transactions on Information Forensics and Security*, 2007, vol. 2, no. 3, pp. 548–558. doi: 10.1109/TIFS.2007.902037
21. Kim G., Eum S., Suhr J.K. et al. Face liveness detection based on texture and frequency analyses. *Proc. 5th IAPR Int. Conf. on Biometrics, ICB*. New Deli, India, 2012, pp. 67–72. doi: 10.1109/ICB.2012.6199760
22. Yang J., Lei Z., Liao S., Li S.Z. Face liveness detection with component dependent descriptor. *Proc. Int. Conf. on Biometrics, ICB*. Madrid, Spain, 2013. doi: 10.1109/ICB.2013.6612955
23. Xiong X., De la Torre F. Supervised descent method and its applications to face alignment. *Proc. 26th IEEE Conference on Computer Vision and Pattern Recognition, CVPR*. Portland, USA, 2013, pp. 532–539. doi: 10.1109/CVPR.2013.75
24. Krizhevsky A., Sutskever I., Hinton G.E. ImageNet classification with deep convolutional neural networks. *Advances in Neural Information Processing Systems*, 2012, vol. 2, pp. 1097–1105.
25. Deng J., Dong W., Socher R., Li L., Li K., Fei-Fei L. ImageNet: a large-scale hierarchical image database. *Proc. IEEE Conference on Computer Vision and Pattern Recognition*. Miami, USA, 2009. doi: 10.1109/cvprw.2009.5206848
26. LeCun Y., Bottou L., Orr G.B., Muller K.R. Efficient BackProp. *Lecture Notes in Computer Science*, 1998, vol. 1524, pp. 9–50. doi: 10.1007/3-540-49430-8_2.
27. Zhang Z., Yan J., Liu S., Lei Z., Yi D., Li S.Z. A face antispoofing database with diverse attacks. *Proc. 5th IAPR Int. Conf. on Biometrics, ICB*. New Delhi, India, 2012, pp. 26–31. doi: 10.1109/ICB.2012.6199754.
28. Zinelabidine B., Jukka K., Li L., Feng X., Hadid A. OULU-NPU: a mobile face presentation attack database with real-world

Behavior Analysis (ISBA). New Delhi, India, 2017. P. 1–7.
29. Yi D., Lei Z., Liao S., Li S.Z. Learning Face Representation from Scratch // arXiv preprint arXiv:1411.7923. 2014. 9 p.
30. Jia Y., Shelhamer E., Donahue J., Karayev S., Long J., Girshick R., Guadarrama S., Darrel T. Caffe: convolutional architecture for fast feature embedding // Proc. ACM Conference on Multimedia. Orlando, USA, 2014. P. 675–678.
31. Tan X., Li Y., Liu J., Jiang L. Face liveness detection from a single image with sparse low rank bilinear discriminative model // Lecture Notes in Computer Science. 2010. V. 6316. P. 504–517. doi: 10.1007/978-3-642-15567-3_37
32. Peixoto B., Michelassi C., Rocha A. Face liveness detection under bad illumination conditions // Proc. IEEE 18th Int. Conf. of Image Processing (ICIP). Brussels, Belgium, 2011. P. 3557–3560. doi: 10.1109/ICIP.2011.6116484
33. Maatta J., Hadid A., Pietik M. Face spoofing detection from single images using micro-texture analysis // Proc. 2011 Int. Joint Conference on Biometrics (IJCB). Washington, USA, 2011. doi: 10.1109/IJCB.2011.6117510.
34. Kose N., Dugelay J.L. Classification of captured and recaptured images to detect photograph spoofing // Proc. Int. Conf. on Informatics, Electronics and Vision. Dhaka, India, 2012. P. 1027–1032. doi: 10.1109/ICIEV.2012.6317336
35. Chingovska I., Anjos A., Marcel S. On the effectiveness of local binary patterns in face anti-spoofing // Proc. Int. Conf. on Biometrics Special Interest Group (BIOSIG). Darmstadt, Germany, 2012.

variations. *Proc. IEEE Int. Conf. on Identity, Security and Behavior Analysis, ISBA*. New Delhi, India, 2017, pp. 1–7.
29. Yi D., Lei Z., Liao S., Li S.Z. Learning Face Representation from Scratch. *arXiv preprint*, arXiv:1411.7923, 2014, 9 p.
30. Jia Y., Shelhamer E., Donahue J., Karayev S., Long J., Girshick R., Guadarrama S., Darrel T. Caffe: convolutional architecture for fast feature embedding. *Proc. ACM Conference on Multimedia*. Orlando, USA, 2014, pp. 675–678.
31. Tan X., Li Y., Liu J., Jiang L. Face liveness detection from a single image with sparse low rank bilinear discriminative model. *Lecture Notes in Computer Science*, 2010, vol. 6316, pp. 504–517. doi: 10.1007/978-3-642-15567-3_37
32. Peixoto B., Michelassi C., Rocha A. Face liveness detection under bad illumination conditions. *Proc. IEEE 18th Int. Conf. of Image Processing, ICIP*. Brussels, Belgium, 2011, pp. 3557–3560 doi: 10.1109/ICIP.2011.6116484
33. Maatta J., Hadid A., Pietik M. Face spoofing detection from single images using micro-texture analysis. *Proc. 2011 Int. Joint Conference on Biometrics, IJCB*. Washington, USA, 2011. doi: 10.1109/IJCB.2011.6117510.
34. Kose N., Dugelay J.L. Classification of captured and recaptured images to detect photograph spoofing. *Proc. Int. Conf. on Informatics, Electronics and Vision*. Dhaka, India, 2012, pp. 1027–1032. doi: 10.1109/ICIEV.2012.6317336
35. Chingovska I., Anjos A., Marcel S. On the effectiveness of local binary patterns in face anti-spoofing. *Proc. Int. Conf. on Biometrics Special Interest Group, BIOSIG*. Darmstadt, Germany, 2012.

Авторы

Волкова Светлана Сергеевна – программист, ООО «Простые решения», Москва, 105318, Российская Федерация, malysheva.svetlana.s@gmail.com

Матвеев Юрий Николаевич – доктор технических наук, главный научный сотрудник, ООО «ЦРТ-инновации», Санкт-Петербург, 196084, Российская Федерация; заведующий кафедрой, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, matveev@speechpro.com

Authors

Svetlana S. Volkova – Software developer, Smilart UG, Moscow, 105318, Russian Federation, malysheva.svetlana.s@gmail.com

Yuri N. Matveev – D.Sc., Chief Scientific Officer, “STC-Innovations” Ltd., Saint Petersburg, 196084, Russian Federation; Head of Chair, ITMO University, Saint Petersburg, 197101, Russian Federation, matveev@speechpro.com