УДК 004.93'11

МОДЕЛЬ АТАК И МЕТОД ПОДТВЕРЖДЕНИЯ ПОДЛИННОСТИ ОБЪЕКТОВ В СИСТЕМАХ КОНТРОЛЯ ДОСТУПА ПО ИЗОБРАЖЕНИЮ ЛИЦА[1]

Ефимов И.Н., *аспирант, ФГБОУ ВО «СамГТУ», e-mail: Mr.Efimov.IN@gmail.com;*
Косолапов А.М., *д.т.н., профессор, в.н.с., ФГБОУ ВО «СамГТУ»;*
Ефимов Н.А., *к.т.н., доцент, ФГБОУ ВО «СамГУПС».*

METHOD AND SYSTEM FOR SPOOFING DETECTION AND APPARATUS OF VIDEO IMAGE

Efimov I.N., Kosolapov A.M., Efimov N.A.

A description, advantages and disadvantages of the original method of authentication recognizable object, based on the evaluation of repeated dispersal of brightness conjugate pixels of the object image. The model of attacks on a person's biometric identification system. Possible action by malicious deception systems by spoofing.

Key words: method of authentication recognizable, dispersal of brightness, model of attacks, person's biometric identification system.

Ключевые слова: компьютерное зрение, методы подтверждения подлинности распознаваемого объекта, распознавание образов, системы контроля доступа, спуфинг атаки.

Приводятся описание, достоинства и недостатки оригинального метода подтверждения подлинности распознаваемого объекта, на основе многократной оценки рассеивания яркостей сопряжённых пикселей изображений объекта. Представлена модель атак на биометрическую систему распознавания человека по изображению лица. Рассмотрены возможные действия злоумышленников по обману систем распознавания с помощью подмены распознаваемого объекта (атаки спуфинга). Описаны требования к системе, способной предотвратить подмену распознаваемого объекта.

Введение

Большинство систем биометрического распознавания не устойчиво к атакам спуфинга. Системы контроля в большей степени нацелены на распознавание лица человека и не защищают от подмены распознаваемого объекта. В [11] авторы продемонстрировали, успешный взлом коммерческих систем распознавания лиц, используя фотографию или видеозапись зарегистрированного пользователя. Системы биометрического распознавания нуждаются во внедрении эффективных методов подтверждения подлинности распознаваемого объекта.

В следующих публикациях [4, 5, 9, 10, 12-14] описан ряд подходов, используемых исследователями для подтверждения подлинности распознаваемого объекта. Однако их существенными недостатками являются высокая вычислительная сложность, неудобство для конечного пользователя, использование специализированного оборудования или отсутствие защиты перед использованием злоумышленниками фотографий, видеозаписей или фотомасок лица зарегистрированного пользователя.

В работе описаны математическая модель, метод и алгоритм подтверждения подлинности распознаваемого объекта. Метод подтверждения подлинности объекта относится к классам, использующим воздействие на пользователя (классификация представлена в [2]). Предложенное решение не использует специализированное оборудование, что является преимуществом по сравнению с аналогами из данного класса, удобнее для конечного пользователя и может быть легко интегрирован в существующие системы распознавания лиц. Метод, математическая модель и алгоритм найдут применение в системах распознавания изображений лиц человека в качестве самостоятельного решения или в виде дополнительного средства предотвращения спуфинг атак. Результаты исследования защищены патентом РФ [8].

Модель атак на биометрическую систему

При разработке методов защиты биометрических систем необходимо определить все возможные виды угроз и описать модель атак. На данный момент уже составлены модели атак на различные биометрические системы [7, 16]. В данном пункте описана модель атак на системы распознавания по изображению лица. Определены девять наиболее уязвимых мест для атак злоумышленников в общей схеме биометрической системы, представленной на рис.1.

Для осуществления успешных атак на системы биометрического распознавания, злоумышленник должен обладать навыками в различных специализированных областях, а также иметь информацию о изъянах в оборудовании и аппаратной реализации, структуре и способе организации базы данных, методах расчёта и сопо-

[1] Работа поддержана грантом фонда содействия развитию малых форм предприятий («У.М.Н.И.К.» I полугодие, Самара, 2014).

ставления информативных признаков, о подсистеме взаимодействия с базой данных и о других моделях и методах, заложенных в реализованную систему биометрического распознавания [7]. Возможными целями злоумышленника могут являться:

– нелегальный доступ одного или нескольких незарегистрированных пользователей к охраняемой информации или на объекты предприятия;

– запрет в доступе зарегистрированному пользователю;

– полный отказ в работе всей системы биометрического распознавания.

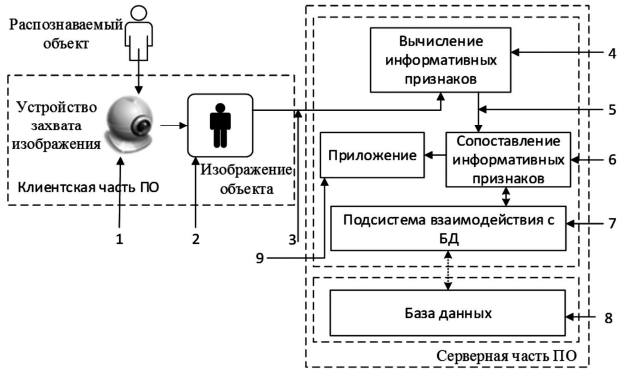


Рис. 1. Общая схема биометрической системы распознавания пользователей с обозначенными атаками

На рис. 1 приведены места для возможных атак на систему распознавания по изображению лица, которые также могут быть применены и для других существующих биометрических систем. Цифры на рис. 1 соответствуют пунктам в следующем списке:

1. *Устройство захвата изображения*. Представление устройству захвата изображения поддельных биометрических данных. Для различных систем биометрического распознавания используют такие объекты, как искусственный палец, копия подписи, маска лица и т.д.

2. *Канал связи между устройством захвата изображения и клиентской частью биометрической системы*. Замена сигнала, полученного с устройства захвата изображения, и передача для дальнейшей обработки в клиентскую часть биометрической системы.

3. *Канал связи между клиентской и серверной частями системы биометрического распознавания*. Для совершения атаки поддельная версия сигнала, подготовленная злоумышленником, передаётся в систему биометрического распознавания, минуя устройство захвата изображения и клиентскую часть программного обеспечения.

4. *Модуль вычисления информативных признаков*. Атака производится на модуль вычисления информативных признаков, таким образом, чтобы модуль генерировал информативные признаки, предварительно выбранные злоумышленником.

5. *Канал передачи информативных признаков*. Результат работы модуля вычисления информативных признаков подменяются злоумышленником (предполагается, что метод вычисления признаков известен злоумышленнику). Данный вид атаки актуален в случае если информативный признак передаётся удалённо.

6. *Модуль сопоставления информативных признаков*. Модуль сопоставления информативных признаков повреждается таким образом, чтобы формировать заранее выбранные злоумышленником оценки соответствия.

7. *Канал связи и подсистема взаимодействия с БД*. Целью данной атаки является перехват и модификация информативных признаков, полученных от БД через канал связи и подсистему взаимодействия.

8. *Элемент базы данных, содержащий информативные признаки*. Злоумышленником модифицируется один или несколько элементов в базе данных. Подобная модификация может привести либо к ошибочной выдаче доступа к системе злоумышленнику, либо к отказу в доступе зарегистрированному пользователю.

9. *Приложение*. Производится подмена окончательного решения о выдаче доступа пользователю к системе. Это означает, что система распознавания была полностью отключена, даже если база информативных признаков и система распознавания образов находятся в работоспособном состоянии.

Все выше перечисленные атаки, кроме атаки на устройство захвата изображения, являются общими для всех биометрических систем. Для защиты систем биометрического распознавания от подобных атак необходимо использовать методы шифрования и цифрового кодирования. Наибольшую угрозу для биометрических систем, использующих изображение лица в роли объекта распознавания, представляют атаки на устройство захвата изображений (спуфинг атаки). Злоумышленник имеет непосредственный доступ к видеокамере, а использовать методы цифрового кодирования и шифрования не представляется возможным. По этой причине необходимо более подробно остановиться на спуфинг атаках. Далее представлены возможные виды атак на устройство захвата изображения.

Постановка задачи подтверждения подлинности распознаваемого объекта

В отличие от систем, где требуется дополнительное оборудование (распознавание по пальцу, сетчатке глаза, кровеносным сосудам и др.), при распознавании человека по изображению лица очень легко создать копию распознаваемого объекта. Все, что необходимо, это фотография человека, которую легко можно обнаружить в интернете или сфотографировать объект на расстоянии. Одной из задач исследования является детектирование подмены представленного видеокамере объекта. Данная задача является не всегда лёгкой даже для человека. Решение должно обладать низкой вычислительной сложностью и высокой вероятностью верного обнаружения подмены распознаваемого объекта, без использования дополнительного специализированного оборудования. В зависимости от направленности биометрической системы, спуфинг атаки могут иметь различные уровни сложности. В таблице 1 рассмотрены возможные виды угроз и меры защиты от подмены распознаваемого объекта. В данном исследовании не рассматриваются такие виды атак, как грим или силиконовая маска. В соответствии с приведёнными в табл. 1 угрозами и представленными мерами защиты, решение задачи подтверждения подлинности распознаваемого объекта должно содержать следующие действия:

Таблица 1. Виды угроз и меры защиты от подмены объекта

Угроза	Описания	Мера защиты
Фото	Злоумышленник предъявляет видеокамере распечатанные фотографии высокого разрешения, либо цифровые фотографии с экрана какого-либо устройства.	Человеческое лицо это 3D объект, поэтому различным регионам поверхности лица присущи различные коэффициенты отражения, рассеяния, преломления и поглощения. Бумага и экран устройства указанным свойством не обладают. Необходимо анализировать изображения объекта с различной интенсивностью освещения.
Видеозапись	Системе распознавания предъявляется видеозапись объекта, подготовленная в реальной жизни, либо серия искусственно сформированных изображений.	Необходимо сформировать серию изображений объекта с различной интенсивностью освещения в случайные моменты времени, чтобы избежать возможного совпадения.
Устройство с экраном + ПО	Изображение объекта, изменённое специализированной программой, предъявляется системе распознавания. Программа способна изменять заранее подготовленное изображение объекта, имитируя моргание глаз, падение света как на 3D объект (подсвечиваются соответствующие регионы) и т.д.	Следует производить анализ изображений после формирования серии изображений, чтобы сократить время формирования решения о подмене. Тем самым предотвратить возможность предъявления сенсору подложных изображений.
Фото маска	Видеокамере предъявляется распечатанное изображение лица человека с прорезями для глаз и губ.	Для предотвращения атаки необходимо анализировать изображения с различной интенсивностью освещения объекта.
3D муляж	Сенсору предъявляют 3D муляж лица человека.	Следует анализировать биометрическую активность объекта.
Грим/ Силиконовая маска	Изменение внешности злоумышленника с целью обмана системы защиты.	Необходимо использовать дополнительное дорогостоящее оборудование.

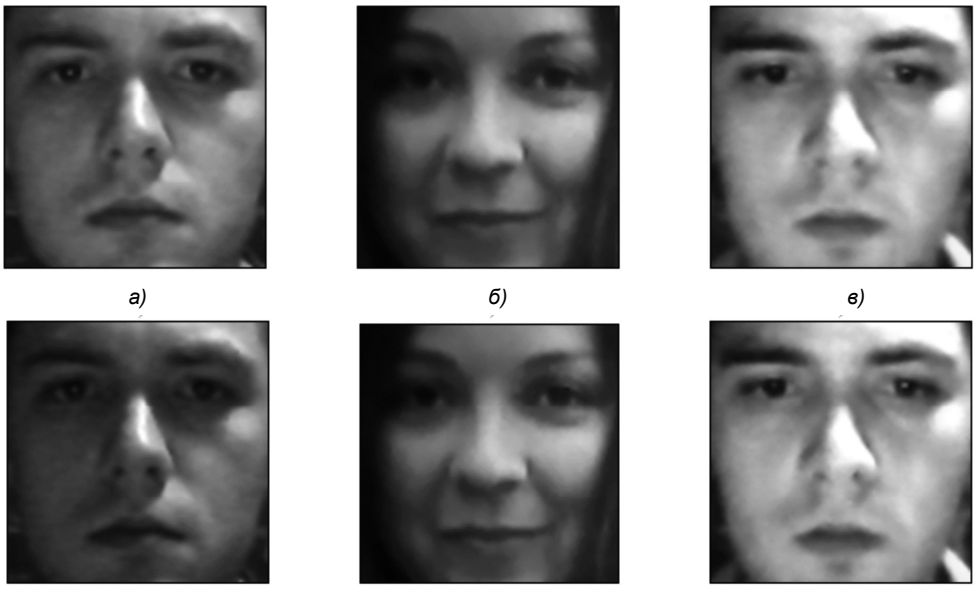


Рис. 2. Примеры изображений с различной интенсивностью освещения: а), г) реальный человек; б), д) фотография; в), е) экран телефона

– формирование серии изображений объекта с различной интенсивностью освещения объекта в случайные моменты времени;

– анализ изображений распознаваемого объекта с различной интенсивностью освещения. Анализ следует производить после проведения всех подготовительных операций по подготовке серии изображений, чтобы сократить время формирования решения о подмене. Тем самым предотвратить возможность предъявления сенсору подложных объектов;

– оценка биометрической активности объекта, для обнаружения случаев предъявления 3D муляжа лица зарегистрированного человека.

Метод подтверждения подлинности распознаваемого объекта

Ниже приведены оригинальные метод, математическая модель и алгоритм подтверждения подлинности распознаваемого объекта, не требующие специализированного оборудования, и, как следствие, внедрение не повлечёт за собой существенного удорожания системы контроля доступа. Одним из способов всестороннего изучения и оптимизации параметров объекта, явления или процесса называют математическое моделирование. Математическая модель, представленная в данном подразделе, является совокупностью частных моделей, описывающих процесс подтверждения подлинности объекта.

Визуальный осмотр изображений реального человека и подложного объекта демонстрирует, что изображения могут быть очень похожи, даже человеческому глазу тяжело определить подмену. Ниже представлены изображения реального человека (рис. 2а, г), фотографии на бумажном носителе (рис. 2б, д) и экрана телефона (рис. 2в, е) с различной интенсивностью освещения.

Тем не менее, некоторые различия между изображениями лица человека и подложным объектом могут стать очевидней, если образы перевести в надлежащее пространство признаков. Человеческое лицо это 3D объект, поэтому различным регионам поверхности лица присущи различные коэффициенты отражения, рассеяния, преломления и поглощения. Бумага и экран устройства указанным свойством не обладают. Есть основание предполагать, что текстурные свойства изображений лица реального человека и подложного объекта будут отличаться при различной интенсивности освещения (рис. 2). При изменении интенсивности освещения появятся текстурные артефакты и неравномерно изменится освещённость регионов распознаваемого объекта. Текстурные артефакты будут хорошо заметны в местах однородных областей, например, на лбу или щеках, а неравномерное изменение освещённости в областях глаз и рта. Описанные изменения освещённости будут отчётливо видны при анализе отношений яркости пикселей изображений объекта до подсветки и после (рис. 2):

$$q_i(x,y) = \frac{q_{0,i}(x,y)}{q_{1,i}(x,y)+1}, \quad (1)$$

где i – номер текущей проверки подлинности предъявляемого объекта; $q_{b,i}(x,y)$ – значение яркости пикселя массива $I_{b,i}$; соответствующего изображению лица пользователя; b – идентификатор массива пикселей, обозначающий режим подсветки, при котором производилась подготовка массива, $b = \overline{0,1}$; x и y координаты рассматриваемого пикселя, $x = \overline{0,W-1}, \quad y = \overline{0,H-1};$ W и H – количество пикселей, соответствующих ширине и высоте массива $I_{b,i}$.

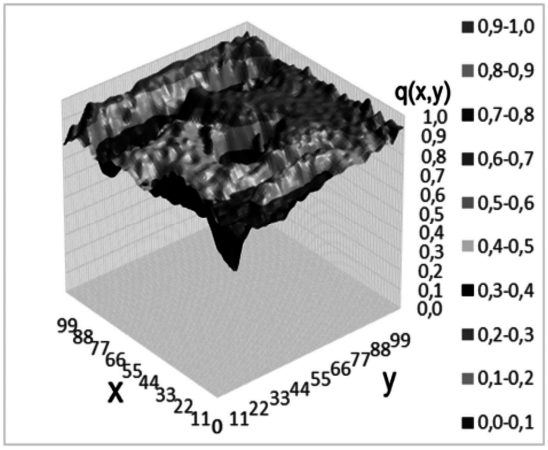
Следует оценить меру рассеивания всех значений $q_i(x,y)$. Для оценки степени рассеивания относительно среднего значения (математического ожидания), вычисляют дисперсию:

$$D(I_{0,i}, I_{1,i}) = \frac{1}{WH}\sum_{x=0}^{W-1}\sum_{y=0}^{H-1}(q_i(x,y)-\overline{q_i})^2, \quad (2)$$

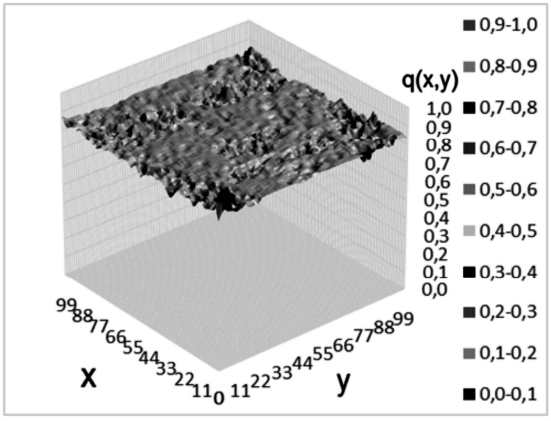
где $\overline{q_i}$ – среднее значение или математическое ожидание дискретной случайной величины $q_i(x,y)$ вычисляется по формуле:

$$\overline{q_i} = \frac{1}{WH}\sum_{x=0}^{W-1}\sum_{y=0}^{H-1} q_i(x,y). \quad (3)$$

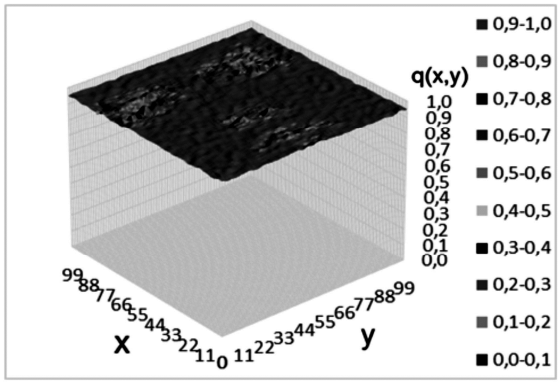
Чем больше дисперсия, тем больше рассеяны значения и соответственно, тем более рельефную поверхность имеет распознаваемый объект. На рис. 3 приведены трёхмерные графики, построенные на основе значений $q_i(x,y)$, для оценки поверхностей различных объектов (реального лица пользователя, фотографии, фото маски и экрана устройства).



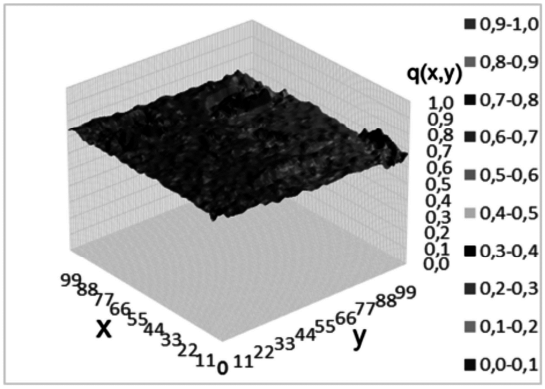
а) поверхность реального объекта D = 0,003564



б) поверхность фотографии на бумажном носителе D = 0,000174



в) поверхность экрана устройства D = 0,000039



г) поверхность фотомаски D = 0,000732

Рис. 3. Графики поверхностей

Оценка меры рассеивания величины $q_i(x,y)$ способствует уменьшению вероятности взлома системы защиты с помощью плоского объекта (фотографии, фото маски, экрана устройства). Но остаётся опасность взлома подбором, т.е. случайного совпадения вспышки и изменения изображения на экране устройства с помощью соответствующего программного обеспечения. Чтобы исключить подобную возможность, необходимо производить подтверждение подлинности распознаваемого объекта многократно и в различные моменты времени:

$$F = \sum_{i=1}^{Q} | X(I_{0,i}, I_{1,i}) - Y_i |, \quad (4)$$

где i – номер текущего проверки подлинности предъявляемого объекта; Y_i – значение последовательности случайных чисел Y; Q – количество проверок подлинности предъявляемого объекта; $\sum_{i=1}^{Q} | X(I_{0,i}, I_{1,i})$ – значение оценки рельефности распознаваемого объекта имеет вид:

$$X(I_{0,i}, I_{1,i}) = \begin{cases} 1, D(I_{0,i}, I_{1,i}) \le \tau_{ROC}; \\ 0, D(I_{0,i}, I_{1,i}) > \tau_{ROC}, \end{cases} \quad (5)$$

где τ_{ROC} – пороговое значение, при котором разница значений $(TPR - FPR)$ максимальна; TPR – процент правильного распознавания случаев представления реального лица видеокамере (True Positives Rate); FPR – процент пропуска подмены распознаваемого объекта (False Positives Rate). Учитывая вероятность ошибки в расчёте $X(I_{0,i}, I_{1,i})$, необходимо ввести пороговое значение τ_{spf}. Значение τ_{spf} варьируется в зависимости от требуемой степени безопасности системы контроля доступа. Выполнение неравенства, представленного ниже, означает, что на вход системы подано объёмное лицо человека, иначе алгоритм детектирует наличие подмены:

$$F \le \tau_{spf}, \quad (6)$$

$X(I_{0,i}, I_{1,i})$ и Y_i могут принимать значения только из множества $\{0,1\}$, где $Y_i = 0$ соответствует изображению с выключенной подсветкой, а $Y_i = 1$ – с включенной. Для модели (4) воспользуемся операцией сложения по модулю 2 (XOR). Ниже представлено преобразованное выражение (4):

$$\sum_{i=1}^{Q} X(I_{0,i}, I_{1,i}) \oplus Y_i \le \tau_{spf}, \quad (7)$$

В соответствии с методом подтверждения подлинности, разработан алгоритм, состоящий из следующей последовательности действий:

Шаг 1. Создаётся последовательность случайных чисел Y.

Шаг 2. Формируется массив пикселей $I_{0,i}$ без подсветки.

Шаг 3. Формируется массив пикселей $I_{1,i}$, при этом, если следующее значение в последовательности $Y_i = 1$, то массив формируется при включённой подсветке, а если $Y_i = 0$, то при выключенной.

Шаг 4. Принимается решение с учётом шага 3, если i-ая цифра в последовательности Y не последняя, то следует перейти к шагу 2, иначе к шагу 5.

Шаг 5. Формируется совокупность значений оценки рельефности распознаваемого объекта $X(I_{0,i}, I_{1,i})$.

Шаг 6. Проводится сравнительный анализ последовательности Y и совокупности значений $X(I_{0,i}, I_{1,i})$.

Шаг 7. Принимается решение о подлинности объекта.

Представленный алгоритм можно модифицировать: добавлять новые блоки или заменять старые блоки, с условием сохранения основной идеи исследования. Вместо блока подсветки возможно использование лампы накаливания или компьютерного монитора. Для данного алгоритма приемлемы небольшие изменения интенсивности освещения и как следствие снижается воздействие на пользователя.

Характеристики технических устройств, используемых для подтверждения подлинности объекта

В соответствии с методом подтверждения подлинности имеем: объект, ориентированный нормально к видеокамере, с коэффициентом отражения ρ, освещаемый световым потоком Φ_b и источник света, сопряжённым с видеокамерой. Известны параметры ПЗС-матрицы, параметры оптики видеокамеры и параметры источника света.

Для расчёта яркости источника освещения B_b, взаимного расположения источника освещения и распознаваемого объекта воспользуемся законом аддитивности освещённостей [1]. При воздействии на объект несколькими источниками света, его освещённость равна сумме освещённостей от каждого источника света. Если распознаваемый объект до включения подсветки имеет освещённость E_n, то закон аддитивности освещённости для случая с пониженным уровнем освещения примет вид:

$$E_{c0} = E_0 + E_n, \quad (8)$$

для случая с повышенным уровнем освещения:

$$E_{c1} = E_1 + E_n, \quad (9)$$

где E_{c0} и E_{c1} – общая энергетическая освещённость объекта, E_0 и E_1 – энергетическая освещенность от источника света системы. Вычтем (8) из (9):

$$E_{c1} - E_{c0} = E_1 - E_0. \quad (10)$$

Соотношения для силы света J_b и энергетической освещённости объекта от точечного источника будет иметь вид [6]:

$$E_b = \frac{\Phi_b}{S_0} = \frac{\Omega \cdot J_b}{S_0} = \frac{J_b \cdot \cos\alpha}{L^2}, \quad (11)$$

$$\Omega = \frac{S_0 \cdot \cos\alpha}{L^2}, \quad (12)$$

где Φ_b – световой поток, исходящий в пределах телесного угла Ω; S_0 – площадь поверхности распознаваемого объекта; L – расстояние от источника света до объекта; α – угол между направлением источника и перпендикуляром к освещаемой поверхности.

В случае протяжённого источника света, следует говорить о силе света каждого элемента источника и площади его поверхности. Тогда под Φ_b следует понимать световой поток, излучаемый каждым элементом поверхности источника. В частности, можно разделить всю поверхность источника света на отдельные Z участков существенно меньших расстояния до облучаемого объекта и принять их за точечные источники света. Каждый участок источника освещения имеет свою площадь S_z, яркость B_{bz}, угол между направлением источника и перпендикуляром к освещаемой поверхности α_z и расстояние до объекта L_z. Полная освещённость объекта от всех отдельных участков протяжённого источника света может быть вычислена следующим образом [3]:

$$E_b = \sum_{z=1}^{Z} \frac{B_{bz} \cdot S_z \cdot \cos_z}{L_z^2}, \quad (13)$$

где z – рассматриваемый номер участка.

Угол обзора источника освещения θ_z – угол, при котором сохраняется удовлетворительный уровень яркости. Яркость B_{bz} от каждого региона источника освещения будет одинакова, если α_z не превышает θ_z, а линейные размеры источника освещения не превышают значения $2tg(\theta_z) \cdot L$. При условии, что яркость B_{bz} всей поверхности источника освещения одинакова, целесообразно использовать следующую формулу для полной освещённости объекта [3]:

$$E_b = \frac{B_b \cdot S \cdot \cos\alpha}{L^2}, \quad (14)$$

где B_b – яркость поверхности источника освещения; S – площадь светящейся поверхности протяжённого источника освещения. Откуда правая часть соотношения (10) равна:

$$E_1 - E_0 = \frac{(B_1 - B_0) \cdot S \cdot \cos\alpha}{L^2} = E_{c1} \quad (15)$$

Выражение для расчёта яркости источника освещения B_b, взаимного расположения источника освещения и распознаваемого объекта следующее:

$$L = \sqrt{\frac{(B_1 - B_0) \cdot S \cdot \cos\alpha}{E_{c1} - E_{c0}}}. \quad (16)$$

Световое излучения от распознаваемого объекта попадает через объектив на светочувствительный слой ПЗС-матрицы видеокамеры и создаёт на нем оптическое изображение распознаваемого объекта с эквивалентной освещённостью E_{sb}. Эквивалентная освещённость E_{sb} показывает степень уменьшения реальной освещённости объекта E_{cb} при прохождении света через объектив камеры (коэффициент пропускания объектива видеокамеры K_a), с учетом спектральной чувствительности видеокамеры K_λ, а также с учетом светосилы объектива и коэффициента диффузного отражения распознаваемого объекта ρ:

$$E_{sb} = E_{cb} K_\lambda K_a \rho \frac{1}{4F^2}, \quad (16)$$

где F – отношение фокусного расстояния объектива к диафрагме видеокамеры (F-число). Выражение для реальной освещённости объекта E_{sb} с учётом эквивалентной E_{sb} имеет вид:

$$E_{cb} = \frac{E_{sb} 4F^2}{K_\lambda K_a \rho}. \quad (18)$$

Эквивалентную освещённость оптического изображения объекта E_{sb} возможно рассчитать, используя массив яркостей оптического изображения объекта $I_{b,i}$ согласно рекомендациям, описанным в стандарте федеральной комиссии связи (FCC) [15]:

$$E_{sb} = K_c \overline{g_b}, \quad (19)$$

$$\overline{g_b} = \frac{1}{WH} \sum_{x=0}^{W-1} \sum_{y=0}^{H-1} g_b(x,y), \quad (20)$$

где K_c – коэффициент расчёта энергетической освещённости объекта; $\overline{g_b}$ – средняя освещенность распознаваемого объекта в плоскости оптического изображения; x, y – координаты текущего пикселя; $X \cdot Y$ – размеры изображения; $g_b(x,y)$ – яркость пикселя, значение рассчитывается с помощью (21). Выражение для яркости пикселя, в соответствии с рекомендациями стандарта Федеральной комиссии связи (FCC) [15], имеет вид:

$$g(x,y) = 0,3 \cdot R_{x,y} + 0,59 \cdot G_{x,y} + 0,11 \cdot B_{x,y}, \quad (21)$$

где $R_{x,y}$, $G_{x,y}$ и $B_{x,y}$ – цветовые составляющие пикселя.

Коэффициент K_c используется для пересчёта освещённости оптического изображения объекта $\overline{g_b}$ в эквивалентную освещённость объекта E_{sb}. Для расчёта $\overline{g_b}$ выбрана область в центре лба, неприкрытая волосами и головным убором. Данная область наиболее плоская и равномерно отражающая свет. Выбор данного региона обусловлен минимизацией погрешности, связанной с неравномерностью распределения освещённости при подсветке трёхмерных объектов. Подставим в выражение (16) соотношения (18) и (19). Итоговое выражение для расчёта яркости источника освещения B_b и взаимного расположения источника освещения и распознаваемого объекта примет вид:

$$L = \frac{(B_1 - B_0) \cdot S \cdot \cos\alpha \cdot K_\lambda \cdot K_a \cdot \rho}{(\overline{g_1} - \overline{g_0} + 0,001) \cdot 4F^2 \cdot K_c}. \quad (22)$$

Соотношение (22) необходимо использовать при калибровке системы подтверждения подлинности распознаваемого объекта. Для вычисления коэффициента K_c, следует на заданном расстоянии L сформировать два изображения распознаваемого объекта с заданными яркостями источника освещения B_0 и B_1. Выражение для расчёта K_c представлено ниже:

$$K_c = \frac{(B_1 - B_0) \cdot S \cdot \cos\alpha \cdot K_\lambda \cdot K_a \cdot \rho}{(\overline{g_1} - \overline{g_0} + 0,001) \cdot (2FL)^2}. \quad (23)$$

При следующих значениях: яркости источника $(B_1 - B_0) = 17$ кд/м^2, площади светящейся поверхности протяжённого источника освещения $S = 0,0825$ м^2, спек-

тральной чувствительности видеокамеры $K_\lambda = 0,6,$ коэффициента пропускания объектива видеокамеры $K_a = 0,8$, коэффициента диффузного отражения кожи лица $\rho = 0,3$, средней освещённости распознаваемого объекта в плоскости изображения $(\overline{g_1} - \overline{g_0}) = 4,5$ лм/м^2, отношения фокусного расстояния объектива к диафрагме видеокамеры (F-число) $F = 0,25$, расстояние от источника света до объекта $L = 0,5$ м, значение коэффициента расчёта энергетической освещённости равно $K_c = 0,72$.

Для уменьшения воздействия на пользователя, при сохранении эффективности предложенного метода, производится расчёт максимально допустимого уровня вариации освещённости от E_0 до E_1, в соответствии с коэффициентом пульсации. Коэффициент пульсации освещённости K_p – критерий оценки относительной глубины колебаний освещённости объекта источником света. Выражение для расчёта K_p имеет вид:

$$K_p = \frac{E_1 - E_0}{2E_m} 100\% \quad (24)$$

где E_1 и E_0 – максимальное и минимальное значения освещённости соответственно, E_m – среднее значение освещённости за период колебания.

В соответствии с условиями, налагаемыми на устройство освещения в «Гигиенические требования к естественному, искусственному и совмещённому освещению жилых и общественных зданий», $K_p = 20\%$. Примем $E_m = E_0$. Откуда значение освещённости E_1 не должно превышать $1,4 \cdot E_0$.

Для обеспечения устойчивости выделяемых признаков к изменениям внешней обстановки и параметров регистрирующих устройств необходимо проводить калибровку системы по объекту с известной спектральной характеристикой коэффициентом отражения и на заданном расстоянии между устройством освещения и объектом. С учётом коэффициента K_c, расстояния между устройством освещения и объектом L, характеристиками видеокамеры, а также ограничения $E_1 < 1,4 \cdot E_0$, необходимо в ручном или автоматическом режиме подобрать значения освещённостей E_0 и E_1 для источника света.

Общее и текущее время работы системы определяются соотношениями:

$$T = t \cdot N. \quad (25)$$

$$t_i = t \cdot i, \quad (26)$$

где t – время, затрачиваемое на обработку одного разряда.

$$t = t_{под} + 2 \cdot t_{кам} + t_{пад}, \quad (27)$$

$$t_{отк} = t_{под} + t_{пад}, \quad (28)$$

где $t_{под}$ – время «подъема», за которое устройство освещения переходит в режим повышенной яркости, $t_{кам}$ – время восприятия изображения видеокамерой, $t_{пад}$ – время «падения», за которое устройство освещения переходит в режим пониженной яркости, $t_{отк}$ – время отклика (black-white-black), за которое устройство освещения изменит режим яркости от минимального значения до максимального значения и обратно. Перечисленные временные рамки зависят от технических характеристик устройства освещения и видеокамеры. Тесты системы подтверждения подлинности производились на компьютере с процессором Intel Core i3 тактовая частота – 2,40ГГц и ОЗУ 4,00ГБ, видеокамерой SCB-0350M – 0,3 Мп при скорости работы 11 кадров/с, откуда $t_{кам} = 91$ мс. Устройством освещения выбран ЖК-дисплей со следующими характеристиками: диагональю 17.3", значением яркости при максимальном режиме 224 кд/м², а при минимальном режиме – 1,34 кд/м² и $t_{отк} = 17$ мс. Время для обработки одной проверки $t = 17 + 182 = 199$ мс. Примем $t = 0,2$ с. С увеличением количества проверок – Q увеличивается время работы T (формула 25) и уменьшается вероятность подбора последовательности Y. Минимальным значением Q выбрано 20, откуда общее время $T = 4$ с.

Экспериментальные исследования

Для проведения опытов была подготовлена экспериментальная БД (табл. 2). В обучающей выборке находятся 160 случаев предоставления видеокамере лиц реальных людей, а также 400 случаев предоставления видеокамере фотографий, видеозаписей, экранов устройств и фотомасок. В тестовой выборке содержаться 320 случаев предоставления видеокамере лиц реальных людей, а также 700 случаев предоставления видеокамере фотографий, видеозаписей и фотомасок. Каждый случай предоставления объекта видеокамере дублировался при повышенной интенсивности освещения для реализации алгоритмов подтверждения подлинности.

Таблица 2. Экспериментальная БД изображений лиц

	Тестовая выборка	Обучающая выборка
Реальные лица	320 изображений, 40 человек	160 изображений, 40 человек
Попытка обмана	700 изображений различных лиц	400 изображений, 40 человек

Примеры изображений представлены на рис. 2. Существуют различные БД для экспериментальной проверки систем подтверждения подлинности [9, 17], но они не подходят в виду специфики используемого метода подтверждения (необходимо, чтобы каждый случай предоставления объекта видеокамере дублировался при повышенной интенсивности освещения). В БД содержатся изображения лиц людей с различным возрастом, мимикой и ракурсом. Изображения подготавливались в четырёх различных условиях освещения. Распознаваемый объект предъявлялся системе подтверждения подлинности в двух режимах:

Фотографию или экран устройства фиксируют на неподвижной опоре, чтобы избежать движения во время попытки обмана.

Пользователь, используя свои собственные руки, предъявляет сенсору фотографию или экран устройства.

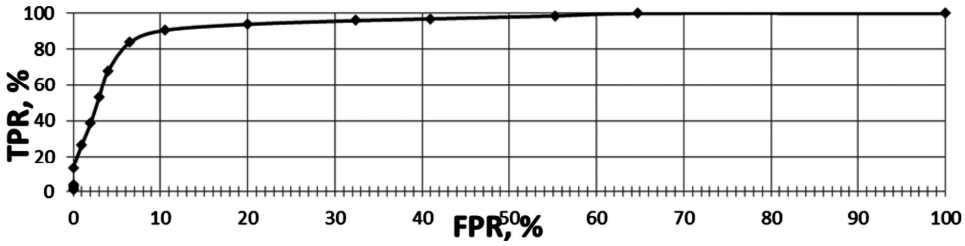


Рис. 4. График экспериментальной зависимости частоты правильного обнаружения подмены объекта от частоты ложных тревог

В данном случае, небольшое движение объекта относительно камеры может внести шум на изображения.

На рис. 4 представлены результаты экспериментальных исследований разработанной системы подтверждения подлинности на основе ROC-анализа (Receiver Operator Characteristic). На графике 4 по оси ординат указан процент правильного распознавания случаев представления реального лица видеокамере (True Positives Rate), а по оси абсцисс указан процент пропуска подмены распознаваемого объекта (False Positives Rate). Для рис. 4 значение площади под криво AUC (Area Under Curve) – 0,944. Значение порога в точке отсечения τ_{ROC} (при котором разница значений $(TPR - FPR)$ максимальна) равно 0,001557. При указанном значении процент правильного распознавания случаев представления реального лица видеокамере не менее 91%, а процент пропуска подмены распознаваемого объекта не более 10%.

Заключение

Представленное решение найдёт применение в небольших информационных средах для обнаружения подмены распознаваемого объекта, например, в дистанционном обучении, при сдаче экзаменов. Для внедрения описанного решения в существующие системы контроля доступа не требуется дорогостоящее специализированное оборудование. Необходимо и достаточно устройства освещения, в роли которого возможно использование источника дневного или инфракрасного света.

Литература

1. Борн М. Основы оптики / М. Борн, Э. Вольф // М: Наука. – 1973.– 720с

2. Ефимов И.Н. Классификация способов подтверждения подлинности распознаваемого объекта / И.Н. Ефимов, А.М. Косолапов // Сборник материалов международной научно-технической конференции «Перспективные информационные технологии». – Самара: СГАУ. – 2016. – С.109-112.

3. Иванов В.П. Трехмерная компьютерная графика / В.П. Иванов, А.С. Батраков, Г.М. Полищук // М.: Радио и связь. – 1995.– 224с.

4. Костылев Н.М. Модуль обнаружения витальности лица по спектральным характеристикам отражения кожи человека / Н. М. Костылев, А. В. Горевой // Инженерный журнал наука и инновации. – 2013. – № 9 – С.13.

5. Костылев Н.М. Обнаружение витальности человека по спектральным характеристикам кожи лица / Н.М. Костылев, Ф. А. Трушкин, В. Я. Колючкин // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение». – 2012. – № 2 – С. 75-85.

6. Пустынский И.Н. К расчету освещенности изображения и числа сигнальных электронов в телевизионном датчике на ПЗС-матрице / И.Н. Пустынский, Е.В. Зайцева // Доклады ТУСУРа. – 2009. – № 2 – С. 5-10.

7. Ручай А.Н. Модель атак и защиты биометрических систем распознавания диктора / А.Н. Ручай // Доклады ТУСУРа. – 2011. – № 1 – С. 96-100.

8. Способ и устройство распознавания рельефности изображения лица: пат. 2518939 Рос. Федерация: МПК A 61 B 3/10 / И.Н. Ефимов, А.М. Косолапов; заявитель и патентообладатель ФГБОУ ВПО «Самарский государственный университет путей сообщения». – № 2013109943 ; заявл. 05.03.2013 ; опубл. 11.04.2014.

9. Chingovska I. On the Effectiveness of Local Binary Patterns in Face Anti-spoofing / I. Chingovska, A. Anjos, S. Marcel // Biometrics Special Interest Group, 2012 BIOSIG - Proceedings of the International Conference of the.– 2012.

10. Chingovska I. Anti-spoofing in action: Joint operation with a verification system / I. Chingovska, M. Switzerland, A. Anjos, S.Marcel // Computer Vision and Pattern Recognition Workshops (CVPRW) . – 2013. – C. 98-104.

11. Duc N.M. Your face is not your password / N.M. Duc // Black Hat Conference. – 2009. – C. 1-16.

12. Freitas P.T. LBP- TOP Based Countermeasure against Face Spoofing Attacks / F. Pereira, T. Anjos, A. Martino, J. Mario, M. Sébastien // International Workshop on Computer Vision With Local Binary Pattern Variants – ACCV. – 2013. – C. 121-132.

13. Housam K.B. Face spoofing detection based on improved local graph structure/ K.B. Housam // IEEE Computer Society. – 2014.

14. Maatta J. Face spoofing detection from single images using micro-texture analysis / J. Maatta, A. Hadid, M. Pietikainen // Biometrics (IJCB), International Joint Conference on Biometrics Compendium, IEEE. – 2011.

15. Plataniotis, K.N. Color image processing and applications/K.N. Plataniotis, A.N. Venetsanopoulos – Engineering Monograph: Springer Science & Business Media. – 2000. – 65 с.

16. Ratha N.K. Enhancing security and privacy in biometrics-based authentication systems / N.K. Ratha, J.H. Connell, R.M. Bolle // IBM Syst. J. – 2001. – Т. 40 – № 3 – С. 614-634.

17. Zhang, Z. A face antispoofing database with diverse attacks / J. Yan, S. Liu, Z. Lei // Biometrics Compendium, IEEE. – 2012. – C. 26-31.