УДК 004.02 DOI 10.18522/2311-3103-2025-5-36-52

И.В. Калиберда

МЕТОД ВЫЧИСЛЕНИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ ИЗ БИОМЕТРИЧЕСКИХ ДАННЫХ ЛИЦА НА ОСНОВЕ УСТОЙЧИВЫХ ПРЕОБРАЗОВАНИЙ

Рассматривается задача преобразования биометрических данных лица в криптографические ключи, обеспечивающие высокий уровень защищённости. Биометрические данные, хотя и уникальные, не обладают достаточной случайностью для создания сильных криптографических ключей. Кроме того, возникают вопросы хранения ключей: злоумышленник может похитить их шаблон, а при малейшем изменении входных данных (другое освещение, мимика) создаётся риск несоответствия, что приводит к высокому уровню частоты ложных отбраковок. В качестве решения предлагается метод генерации криптографических ключей, объединяющий несколько ключевых технологий для обеспечения эффективности и безопасности процесса создания ключей. Дано описание основных этапов метода, включающих получение изображения лица, обработку изображения, анализ изображения с извлечением необходимых признаков с помощью сверточной нейронной сети, преобразование изображения (вектора признаков) в двоичную строку, устойчивые преобразования. Устойчивые преобразования призваны в качестве методик, направленных на защиту биометрических данных: использование корректирующих кодов Reed-Solomon, генерацию биометрически зависимого ключа, с последующим распределением его на части по классической схеме Шамира, шифрование. Проведено теоретическое обоснование преимущества такого подхода в контексте уменьшения вероятности ложных допусков и ложных отклонений. Представлены результаты экспериментов на базе публичных наборов данных. Показано, что по сравнению с классическими методами и некоторыми существующими схемами без коррекции ошибок предлагаемое решение даёт более высокую точность. Представленный метод дает существенные преимущества в области безопасности, делая криптографические системы более подходящими для приложений с высоким уровнем безопасности.

Биометрические системы; генерация ключей; устойчивые преобразования; корректирующие коды; хеш-функции; схема Шамира; распознавание лиц.

I.V. Kaliberda

A METHOD FOR CALCULATING CRYPTOGRAPHIC KEYS FROM A PERSON'S BIOMETRIC DATA BASED ON STABLE TRANSFORMATIONS

This article discusses the task of converting a person's biometric data into cryptographic keys that provide a high level of security. Biometric data, although unique, does not have sufficient randomness to create strong cryptographic keys. In addition, key storage issues arise: an attacker can steal the template, and the slightest change in the input data (different lighting, facial expressions) creates a risk of inconsistency, which leads to a high frequency of false rejections. As a solution, a cryptographic key generation method is proposed that combines several key technologies to ensure the efficiency and security of the key creation process. The main stages of the method are described, including obtaining a face image, image processing, image analysis with the extraction of necessary features using a convolutional neural network, image transformation (feature vector) into a binary string, and stable transformations. Sustainable transformations are called upon as techniques that are aimed at protecting biometric data: the use of Reed-Solomon correction codes, the generation of a biometrically dependent key, followed by its distribution into parts according to the classical Shamir scheme, encryption. The advantages of this approach have been theoretically justified in the context of reducing the likelihood of false tolerances and false deviations. The results of experiments based on public datasets are presented. It is shown that compared with classical methods simple sampling and some existing schemes (Bio-Hashing without error correction), the proposed solution provides higher accuracy. The presented method provides significant security advantages, making cryptographic systems more suitable for high-security applications.

Biometric systems; key generation; tokenized conversion; sustainable transformations; hash functions; Shamir scheme; facial recognition.

Введение. В современном цифровом мире вопрос безопасного хранения и передачи конфиденциальных данных стал одним из важнейших приоритетов. С ростом числа онлайн-сервисов, таких как банковские приложения, электронная коммерция и социальные сети, увеличилось и количество кибератак, направленных на кражу личных данных и идентификационной информации, что вызвало необходимость в надежной защите идентификационных данных пользователей. Развитие технологий, таких как биометрия и многофакторная аутентификация, открывает новые возможности для повышения безопасности удаленной идентификации. Требования о защите информации с использованием криптографических средств для таких случаев указаны в нормативной документации [1].

Защита от атак на инфраструктуру системы удаленной идентификации может быть эффективно осуществлена с помощью шифрования. Предлагается решение, в котором биометрические данные лица пользователя (биометрический шаблон), предназначенные для передачи на сервер аутентификации в зашифрованном виде, используются и для генерации криптографического ключа этой же системы шифрования.

Для обеспечения возможности успешного применения биометрических данных для генерации криптографического ключа, необходимо учитывать их особенности, а также преимущества и недостатки. При формировании идентифицирующего изображения лица принимается во внимание шумность данных (качество сенсоров, освещение, вариации позы головы и выражения лица), необходимое качество изображения как на этапе создания эталона для базы лиц, так и на этапе аутентификации пользователя [2]. На эффективность работы системы существенно будут влиять настройки параметров алгоритма распознавания лиц и ошибки трансформации непрерывно значимых собственных проекций лица в строки битов. Длина и сложность криптографического ключа напрямую влияют на его стойкость к атакам. С учетом обеспечения необходимого уровня безопасности, сопоставимого с AES-256, и при этом адаптированного под российские стандарты и сертификации ФСТЭК и ФСБ, решено использовать шифрование дескриптора с помощью симметричного алгоритма блочного шифрования ГОСТ "Кузнечик" [3]. В алгоритме (128-битный блок, 256-битный ключ) предлагается использовать режим CBC, с IV (инициализирующим вектором). Процесс генерации ключа не должен замедлять работу системы, особенно в реальных приложениях, таких как мобильные устройства или сетевые сервисы. Для гарантии безопасности стоит учитывать фактор секретности ключа, заключающийся в том, что ключ должен оставаться скрытым от неавторизованных лиц. Генерация и управление криптографическими ключами должны быть частью стратегии безопасности, включая механизмы хранения, передачи и распределения ключей.

При генерации криптографических ключей на основе биометрических признаков остаются несколько нерешённых задач, которые могут затруднить использование таких методов в реальных системах. Вот основные из них:

- обеспечение необратимости биометрических данных, то есть исключают возможность восстановления оригинального изображения из ключа;
- безопасность передачи биометрических данных, отсутствие которой при использовании небезопасных каналов, может привести к её утечке;
- проблемы с производительностью: алгоритмы для извлечения и обработки биометрических признаков могут требовать значительных вычислительных ресурсов, что может затруднить их использование в реальном времени, особенно на устройствах с ограниченными ресурсами.

В качестве решения необходим метод, объединяющий несколько ключевых технологий для обеспечения эффективности и безопасности процесса создания ключей по биометрическим параметрам лица. Новизна предложенного метода заключается в интеграции современных нейросетевых технологий и криптографии для создания биометрически зависимого ключа с высокой степенью безопасности.

Постановка решаемой задачи. Задача вычисления криптографических ключей из биометрических данных лица обладает высокой важностью как для науки, так и для общества, и практической деятельности. Этот подход позволит объединить биометрические

данные (изображение лица) с классическими криптографическими алгоритмами. Генерация биометрически зависимого ключа позволит решить проблемы, связанные с уязвимостью традиционных методов аутентификации. Научные исследования в этой области в дальнейшем, могут способствовать разработке новых методов обработки биометрических данных, улучшению алгоритмов распознавания и повышению стойкости криптографических ключей к атакам. Биометрически зависимые ключи могут быть внедрены в современные системы безопасности, такие как мобильные платежи, системы контроля доступа, медицинские системы и государственные учреждения. Эти системы требуют высокой степени защиты и удобства, что делает использование биометрии эффективным решением.

Главная цель исследования заключается в разработке метода, реализующего процесс извлечения биометрических признаков, подходящих для криптографической защиты данных при передаче по не защищенным каналам связи. Под подходящими для криптографической защиты признаками следует понимать такие биометрические данные, которые:

- обладают достаточной энтропией (случайностью), сравнимой с криптографическими ключами длиной 256 бит;
- устойчивы к малым вариациям входных данных (освещение, мимика, поворот головы);
- необратимы, то есть исключают возможность восстановления оригинального изображения из ключа;
- совместимы с криптографическими протоколами хранения, шифрования и передачи;
- допускают отзыв и регенерацию ключа в случае компрометации вспомогательных параметров (токенов, масок и т. д.).

Такие признаки позволяют интегрировать биометрию в защищённые системы с гарантированной стойкостью к анализу и подделке.

Анализ известных решений. В области биометрических криптосистем имеются несколько направлений исследований. Ниже дана краткая характеристика основных известных решений, их особенности и где требуются дополнения.

Первоначально возникла идея «прямого» использования биометрии в качестве ключа, известная как классический Biometric Encryption [4,5]. Однако если без преобразований записать биометрические данные (проекции лица) прямо в ключ, возникает несколько проблем:

- прямое хранение шаблона: злоумышленник может похитить шаблон, а пользователь не может «отозвать» собственное лицо.
- при малейшем изменении входных данных (другое освещение, мимика) создаётся риск несоответствия, что приводит к высокому уровню FRR.

Следующие разработчики Bio-Hashing и FaceHashing [6,7] предлагают идею «необратимого» преобразования биометрии. Суть заключается в следующем, биометрические данные смешиваются с псевдослучайной информацией (токен). Получается выход, из которого нельзя получить исходный шаблон. Если токен скомпрометирован, его меняют и формируют новый биометрический хэш. Преимущество данного метода – гибкость и «обратимость» в смысле обновления схемы. Недостаток заключается в обеспечении реальной необратимости (при определённых условиях злоумышленник может попытаться вычислить разницу между исходной биометрией и зашумлённой версией).

Существуют решения, предлагающие использование кодов коррекции ошибок:

- в работе [8] биометрический вектор связывается (commitment) с некоторым случайным ключом, зашифрованным кодом (например, Рид-Соломона). Если при проверке биометрия достаточно близка к исходной, систему удаётся «раскрыть» и восстановить ключ;
- в работе [9] похожая идея, но используется создание множества точек (поддельных и настоящих), из которых только владелец биометрии может выделить истинную кривую.

Плюсы: высокая точность в отсутствии сильного шума, формальное описание через коды коррекции. Минусы: потенциально сложная реализация, нужны аккуратные схемы распределения ключа.

В исследовании, приведенном в работе [10] предлагается метод извлечения признаков с использованием вейвлетов, где дискретное вейвлет-преобразование используется для создания изображений признаков из отдельных вейвлет-полос, а сокращённый вектор признаков используется для дальнейшей классификации с помощью классификатора евклидова расстояния и классификатора нейронных сетей:

- анализ главных компонент (PCA) сокращает размерность, выделяя наиболее значимые характеристики лиц;
- дискретное косинусное преобразование (DCT) выделяет блоки основных частот в изображении, устойчив к небольшим вариациям;
- вейвлет-преобразование: многомасштабное разложение сигнала, позволяет эффективно представлять данные с минимумом потерь;
- CNN-эмбеддинги (FaceNet, ArcFace, MobileNet+ArcFace, InsightFace): эффективно извлекают признаки из данных (края, текстуры и формы в изображениях). На сегодняшний день самые точные, устойчивые к значительным вариациям.

Недостаток классических методов (PCA, DCT) в том, что они не столь хорошо работают при сильных изменениях ракурса, освещения; CNN-методы обеспечивают более высокую точность, но сложнее в реализации (требуют обучения на большом датасете).

Ниже представлена сводная табл. 1, отражающая ключевые плюсы и минусы рассмотренных решений.

Таблица 1

Преимущества и недостатки основных подходов биометрических криптосистем

Подход	Преимущества	Недостатки
Biometric Encryption	Простое понятие, прямое использование биометрии	Хранение шаблона небезопасно, сложность «отзыва»
Cancelable Biometrics	Возможность «перегенерации» в случае компрометации	Нужно доказать необратимость, сложная настройка параметров
Fuzzy Commitment/Vault	Строгая математическая модель с кодами коррекции	Ресурсоёмко, требует аккуратной реализации, может быть сложен в эксплуатации
PCA/DCT/Wavelet	Простые и быстрые вычисления, многолетние исследования	Не всегда достаточно точно при сильных вариациях (под разными углами)
CNN-эмбеддинги	Высокая точность, хорошая устойчивость к шумам	Необходима мощная модель, сложность развертывания, обучение на большом датасете

Прямое сохранение биометрических данных небезопасно и непрактично. Нужно разработать метод, позволяющий учесть шумность биометрии (наличие посторонних шумов) в виде коррекции ошибок; исключить возможность восстановления исходных биометрических признаков (необратимое преобразование); обеспечить отзыв ключа при компрометации вспомогательных параметров.

Разработка метода. Метод генерирования защищенного криптографического ключа на основе биометрии лица (назовем его SBC-KG (Secure Biometric Crypto Key Generation)), представляет собой улучшенный вариант схемы, объединяющей идеи Bio-Hashing, коррекции ошибок (BCH/RS) и разделения ключа (Шамира). Реализация метода достигается выполнением последующих операций:

1. Получение изображения лица человека.
2. Предобработка изображения (масштабирование, фильтрация, выравнивание гистограммы).
3. Анализ изображения с извлечением необходимых идентификационных признаков (обнаружение лица на изображении, определение 68 ключевых точек лица, преобразование ключевых точек в вектор эмбеддингов).

4. Устойчивые преобразования (дискретизация, коррекция ошибок, генерирование криптографического ключа, распределение ключа на части).

Рассмотрим этапы метода SBC-KG более подробно.

Захват изображения с видеокамеры

Вначале необходимо получить изображение идентифицируемого лица. Для этого в составе системы идентификации используется потоковый сервер (WCS) с разработанным и установленным ПО и IP-видеокамера, поддерживающая протокол потоковой передачи в реальном времени (RTSP). Для того, чтобы захватить видеопоток с IP-видеокамеры организовано Ethernet-соединение источника видеосигнала с WCS. Для возможности воспроизведения в программе видеопоток камеры передается в поддерживаемых кодеках (рис. 1).

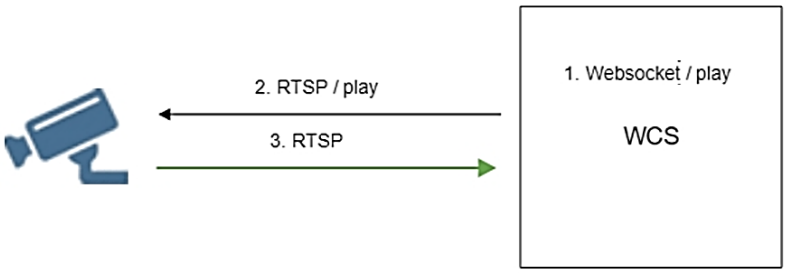

Рис. 1. Схема захвата изображения с IP-видеокамеры

Схема содержит следующие шаги:

1. ПО соединяется с сервером по протоколу Websocket и отправляет команду «playStream».
2. Сервер соединяется с RTSP-источником и отправляет команду «PLAY».
3. RTSP-источник передает на сервер RTSP-поток. Сервер отдает поток ПО. По умолчанию, RTSP потоки захватываются по TCP.

Предобработка изображения

На этапе предобработки изображения используется фильтрация Гаусса. Данное размытие удаляет шум, не затрагивая крупных деталей. Аддитивный гауссов шум характеризуется добавлением к каждому пикселю изображения значений с нормальным распределением и с нулевым средним значением. Формула (1) Гауссова фильтра для плоского изображения имеет вид:

$$I_{filtered}(x,y) = \frac{1}{2\pi\sigma^2}\sum_{i=-k}^{k}\sum_{j=-k}^{k} I(x+i, y+j)\cdot e^{-\frac{x^2+y^2}{2\sigma^2}}, \quad (1)$$

где

$I(x, y)$ – интенсивность пикселя в точке с координатами (x, y);

σ – стандартное отклонение;

$k = \lfloor 3\sigma \rfloor$ – радиус ядра, в пределах которого происходит фильтрация;

$\frac{1}{2\pi\sigma^2}$ – нормализующий коэффициент, который обеспечивает, чтобы сумма всех значений ядра равнялась 1.

Ядро Гаусса $e^{-\frac{x^2+y^2}{2\sigma^2}}$ задаёт вес для каждого пикселя, при этом чем дальше пиксель от центра, тем меньший вес он имеет.

Внешние суммы $\sum_{i=-k}^{k}\sum_{j=-k}^{k}$ означают, что фильтрация учитывает все пиксели в области вокруг точки (x, y), которая имеет размер $(2k+1)\times(2k+1)$, где k зависит от значения σ.

Значение стандартного отклонения (σ) выбирается в зависимости от размера изображения и желаемой степени размытия. Для изображения размером 240×192 пикселей, выбор значения σ лежит в диапазоне от 1 до 3 пикселей [13]:

- при σ = 1 – ядро имеет размер 5×5 пикселей;
- при σ = 1.5 – ядро увеличивается, и более агрессивно размывает изображение, сохраняя менее выраженные детали.

В нашем случае выбрано значение σ = 1, достаточное для умеренного размытия (рис. 2). Ядро размером 5×5 выглядеть как матрица (G):

$$G = \begin{bmatrix} 0.003 & 0.013 & 0.021 & 0.013 & 0.003 \\ 0.013 & 0.059 & 0.096 & 0.059 & 0.013 \\ 0.021 & 0.096 & 0.159 & 0.096 & 0.021 \\ 0.013 & 0.059 & 0.096 & 0.059 & 0.013 \\ 0.003 & 0.013 & 0.021 & 0.013 & 0.003 \end{bmatrix}.$$

Это ядро применяется к изображению, где каждому пикселю присвоено весовое значение из представленной матрицы.

Рис. 2. Результат обработки изображения с различными значениями σ

Гауссов фильтр является удобным инструментом на этапе предобработки изображения лица. Он эффективно удаляет шум и оставляет глобальные черты лица нетронутыми.

Обнаружение лица

Для обнаружения изображения лица с видеокамеры используется сверточная нейронную сеть (CNN), которая использует алгоритм TinyFaceDetector [11]. Это одно из удачных решений, используемых в задачах обнаружения лиц в условиях сложных фонов и разнообразных углов зрения. Алгоритм TinyFaceDetector улучшает точность распознавания, минимизируя ошибку классификации, при этом обеспечивая максимальное разделение между лицами и фоном. В результате, на выходе алгоритм TinyFaceDetector выдает координаты прямоугольной области, в которой находится лицо. Эти координаты определяют верхний левый угол прямоугольника, а также его ширину и высоту.

Изображение лица представляется как массив с использованием ndarray из библиотеки NumPy, где каждый элемент этого массива является кортежем, содержащим три значения: красный (R), зелёный (G) и синий (B) компоненты цвета пикселя. Каждый кортеж представляет собой цвет пикселя на изображении.

Приведение изображения лица к стандартному размеру

После того как алгоритм TinyFaceDetector успешно обнаружил лицо, следующим шагом является приведение изображения лица к стандартному размеру [12], включающий шаги:

- извлечение области лица: изображение лица извлекается из полного кадра, используя координаты, полученные на этапе обнаружения лица. Эта область будет прямоугольной и ограничена размерами, указанными в выходных данных MMOD;
- масштабирование изображение лица до нужного размера — 320x240 пикселей. Масштабирование выполняется через изменение размера изображения, при этом важно сохранить пропорции и качество изображения, чтобы минимизировать искажения.
- определение внутренней области для изображения лица с горизонтальным размером 240 пикселей: высота области определяется пропорциями лица. Чтобы сохранить стандартизированный размер изображения, примем значение высоты в 192 пикселя.

Внутренняя область изображения лица всегда должна содержать важные элементы лица (глаза, нос, рот). Это достигнуто с использованием алгоритмов компьютерного зрения.

Извлечение признаков (CNN)

Для изображения лица, представляющего собой 2D-матрицу пикселей, с последующим анализом с использованием нейронной сети, создается массив, где каждая точка представляет координаты одной из 68 ключевых точек, полученных с использованием модели FaceLandmark68TinyNet. Эти точки описывают важные характеристики лица, такие как глаза, нос, рот и контуры лица [14]. Наглядное представление работы метода выделения лица человека и ключевых точек после обработки входного изображения для задачи распознавания ключевых точек лица представлено на рис. 3.

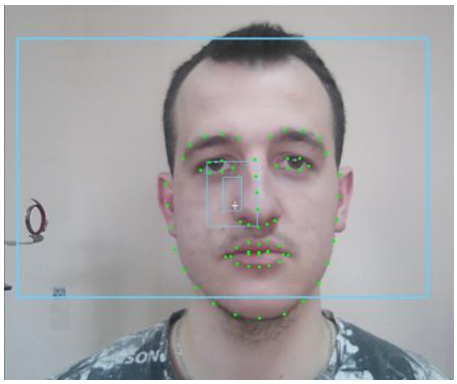

Рис. 3. Размещение ключевых точек на оптическом изображении лица пользователя

Нейронная сеть генерирует массив из 68-и ключевых точек. Массив (P) из 68 точек с координатами x и y представляется следующим образом:

$$P = [(x_1, y_1), (x_2,y_2), \ldots, (x_{14}, y_6)], \quad (2)$$

где

x_i – это горизонтальная координата i-й ключевой точки;

y_i – координата вертикальной i-й ключевой точки.

Пример массива из 68 ключевых точек лица, координаты которых варьируются в пределах размера 240x192, показан на рис. 4.


```
Позиции лицевых точек:
[{"_x":112.73252106583368,"_y":112.33436777356994},{"_x":113.4645
7085883867,"_y":119.5592535949124},{"_x":114.79015515125047,"_y":
126.63003250125777},{"_x":116.17014513290178,"_y":133.16832467082
87},{"_x":118.6357192633177,"_y":140.11767848495376},{"_x":122.91
331791258108,"_y":144.53519865039718},{"_x":127.09912388897192,"_
y":147.10619791511428},{"_x":132.66619788980734,"_y":149.02155800
823104},{"_x":141.63867616033804,"_y":150.26584132675063},{"_x":1
50.2685839471842,"_y":148.9533154583348},{"_x":156.15358167267095
,"_y":146.89166112903487},{"_x":160.4742169318224,"_y":144.218790
37383925},{"_x":164.6597901520754,"_y":138.9609180307759},{"_x":1
67.0543852982546,"_y":132.08887322906386},{"_x":168.0916185913111
,"_y":125.5599604463948},{"_x":169.40535348034155,"_y":118.297978
48228347},{"_x":170.14501863098394,"_y":111.16128101114165},{"_x"
:118.99019310748827,"_y":101.25738798741233},{"_x":122.0114555892
9693,"_y":97.59233622912299},{"_x":126.28311895704519,"_y":95.813
49148515594},{"_x":130.4846486685301,"_y":95.23921161059272},{"_x
":134.2985061047102,"_y":96.04203059438598},{"_x":148.26024972772
848,"_y":95.41064201954734},{"_x":151.9637003479029,"_y":94.54156
129721534},{"_x":156.17632406330358,"_y":94.48006122473609},{"_x"
:160.52889346456777,"_y":96.17365493539702},{"_x":164.02352374172
46,"_y":99.61163102749717},{"_x":140.99308680868398,"_y":103.5149
9035123717},{"_x":141.01071279621374,"_y":107.54655166629684},{"_
x":140.7070929942156,"_y":111.158262333907},{"_x":140.58521764850
866,"_y":114.8789729094876},{"_x":135.84305679178487,"_y":120.471
91842559707},{"_x":138.1226534781481,"_y":120.70861025813949},{"_
x":140.75865905857336,"_y":121.05303569797408},{"_x":143.69111555
195104,"_y":120.64522012237441},{"_x":146.02656947946798,"_y":120
.43915941480529},{"_x":124.47305487966787,"_y":106.54029323820006
```


Рис. 4. Пример массива из 68-и ключевых точек с координатами (x, y)

Ключевые точки лица, полученные нейросетью при распознавании лица, содержат не только координаты точек (*x*, *y*), но и дополнительные признаки, такие как:

- значение яркости пикселя;
- среднее значение в окрестности пикселя.

Параметр яркости пикселя необходим для улучшения распознавания в условиях различного освещения. Использование параметра среднего значения пикселей в окрестности ключевой точки помогает улучшить точность распознавания в тех случаях, когда изображение может быть шумным или размытым. Это позволяет нейросети учитывать не только положение самой точки, но и информацию о ближайших пикселях, что делает систему более устойчивой к шуму и вариациям изображения.

Формирование эмбеддинга

Для распознавания лиц и анализа изображений используется модель ResNet. Она преобразовывает лицевые точки в вектор признаков (эмбеддинг), отражающего уникальные характеристики структуры лица. В разных версиях ResNet используется разное количество свёрточных слоёв: в ResNet-18 – их 18, в ResNet-34 – 34, в ResNet-50 – 50 слоев,в ResNet-101 – 101 слоев, в ResNet-152 – 152 слоев. В конечном итоге это отражается на выходном размере признаков. Выбор размерности эмбеддинга обусловлен необходимостью соблюдения баланса между несколькими факторами:

- точность биометрической идентификации;
- вычислительная эффективность при обработке и сравнении шаблонов;
- объём передаваемой и хранимой информации.

Модель ResNet-18 оптимальна с учетом точности идентификации и скорости обработки шаблонов. Изображения, содержащие выровненные лица, подаются на вход модели ResNet-18. Сеть проходит через 18 сверточных слоев, которые извлекают признаки. На выходе модели ResNet получается эмбеддинг фиксированной длины (128 элементов), который представляет лицо. Каждый элемент вектора кодирует абстрактную особенность изображения, извлечённую внутренними представлениями нейросети. Эти признаки не поддаются прямой интерпретации человеком, однако в совокупности формируют устойчивое и воспроизводимое описание биометрического объекта. Размерность в 128 признаков рекомендуется как промышленный стандарт в задачах идентификации по лицу. Эта конфигурация подтверждена экспериментально в ряде исследований, включая работу FaceNet (Google) [16], и демонстрирует высокую точность при умеренных требованиях к вычислительным ресурсам.

С математической точки зрения, полученный эмбеддинг может быть представлен как точка на поверхности 128-мерной гиперсферы. Похожие лица формируют плотные кластеры, в то время как векторы, соответствующие разным людям, стремятся к равномерному распределению на поверхности сферы. Пусть $z \in R^{128}$ – эмбеддинг, полученный от модели ResNet-18.

Нормализуем его по L2-расстоянию (евклидово расстояние):

$$\hat{z} = \frac{z}{||z||_2}, \text{ где } ||z||_2 = \sqrt{\sum_{i=1}^{128} z_i^2}, \quad (3)$$

После нормализации:

$$||\hat{z}||_2 = 1.$$

Это означает, что $\hat{z}$ лежит на единичной 128-мерной гиперсфере:

$$S^{127} = \{x \in R^{128} | \, ||x||_2 = 1\}, \quad (4)$$

3D проекция 100 эмбеддингов на гиперсфере (PCA) показана на рис. 5.

На рис. 5 показаны:

- PCA1 (первая главная компонента) – это направление в исходном 128-мерном пространстве, по которому максимальная дисперсия данных. PCA1 указывает ось, вдоль которой векторы эмбеддингов различаются наиболее сильно;

♦ PCA2 (вторая главная компонента) – ортогональна PCA1 и указывает второе по значимости направление дисперсии. PCA2 фиксирует второстепенные различия между эмбеддингами, которые не объясняются первой компонентой;

♦ PCA3 (третья главная компонента) – ортогональна как PCA1, так и PCA2. PCA3 охватывает дополнительную вариативность, менее значимую, но важную для пространственного разделения точек.

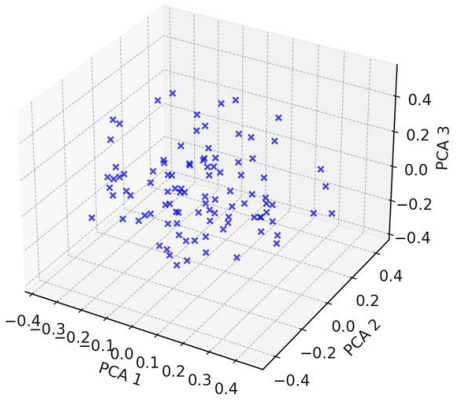

Рис. 5. 3D проекция 100 эмбеддингов на гиперсфере (PCA)

Компоненты PCA1, PCA2 и PCA3 формируют новое ортонормированное базисное пространство, в котором 128-мерные эмбеддинги отображаются как 3D-векторы. Это позволяет визуально оценить степень различия и группировку векторов для идентификации.

Идентификация личности

Эмбеддинги, полученные для разных лиц, располагаются в многомерном признаковом пространстве таким образом, что векторы, соответствующие одному и тому же лицу или похожим лицам, находятся на малом расстоянии друг от друга. Для измерения степени близости применяется метрика косинусного расстояния, позволяющая эффективно сравнивать ориентацию векторов на единичной гиперсфере. Для оценки степени сходства между биометрическими векторами-эмбеддингами применяем метрику косинусного расстояния (cosine distance). Пусть заданы два вектора эмбеддингов:

$$z_1, z_2 \in R^d,$$

где d – размерность признакового пространства *(d=128).*

Косинусное сходство вычисляется по формуле:

$$\cos(\theta) = \frac{\langle z_1, z_2 \rangle}{||z_1|| \cdot ||z_2||}, \quad (5)$$

где

$\langle \cdot, \cdot \rangle$ – скалярное произведение,

$\|\cdot\|$ – евклидова норма (длина вектора),

θ – угол между векторами.

Результат принимает значения от –1 до 1, где:

1 – полное совпадение направления (векторы идентичны),

0 – ортогональные (несвязанные),

−1 – противоположные (в реальной биометрии почти не встречается).

Косинусное расстояние интерпретируется как мера расхождения:

$$dist_{cos}(z_1, z_2) = 1 - \cos(\theta), \quad (6)$$

Значения ближе к нулю указывают на высокую степень схожести. При регистрации: эмбеддинг нормализуется и сохраняется как эталон. При идентификации: сравниваются текущий и эталонный векторы по косинусной метрике. При превышении установленного порога схожести, cos(θ)>0,75, считается, что пользователь успешно распознан.

Адаптивная бинаризация

Процедура адаптивной бинаризации необходима для преобразования вектора признаков в двоичную строку. В отличие от обычной бинаризации, при которой используется один фиксированный порог для всех пикселей, адаптивная бинаризация учитывает локальные характеристики. В нашем случае имеется вектор признаков $f = [f_1, f_2, f_3, \ldots, f_n]$, полученный из изображения лица. Адаптивная бинаризация осуществляется следующим образом:

1. Для каждого элемента f_i вектора признаков вычисляется локальный порог t_i, который зависит от ближайших значений признаков.
2. Сравнивается значение каждого элемента f_i с локальным порогом для присвоения ему значения 0 или 1. Таким образом, для вектора признаков f получаем двоичный вектор b:

$$b = [b_1, b_2, b_3, \ldots, b_{128}], \tag{7}$$

где $b_i = \begin{cases} 1, & \text{если } f_i > t_i \\ 0, & \text{иначе} \end{cases}$

Кодирование ошибок (RS)

Блоковые коды Рида-Соломона (Reed-Solomon (RS)) обеспечивают коррекцию ошибок с помощью добавления избыточности в исходные данные. Эта функция поможет в восстановлении исходной информации при её потере.

Разберем принцип работы кодов RS. Двоичный вектор (7), состоящий из 128 бит, можно представить как полином:

$$P(x) = b_1 + b_2x + b_3x^2 +, \ldots, + b_{128}x^{127}, \tag{8}$$

где

b_i – это коэффициенты полинома, которые соответствуют битам двоичного вектора b;

x – переменная для определения значений полинома в разных точках.

В кодировании полином используется для определенных значений x при восстановления исходных данных. Например, для значений двоичного вектора b, полученных в выражении (3) – это биты данных, полином $P(x)$ используется для создания закодированных данных, и x представляет переменную, через которую эти данные могут быть восстановлены в дальнейшем.

Структура кодов RS следующая: если у нас есть исходное сообщение длиной k символов, код Рида-Соломона может добавить $n - k$ символов избыточности. В результате длина закодированного сообщения будет равна n, где n – это максимальная длина закодированного сообщения [17].

Так как у нас есть кодированный вектор b_{RS}, и получен вектор b'_{RS}, который отличается от b_{RS} в пределах допустимой погрешности (порог t), то декодер сможет восстановить исходный вектор b с помощью алгоритма Рида-Соломона:

$$P(x) = Interp(b'_{RS}, t), \tag{9}$$

где *Interp* – это процесс интерполяции, который восстанавливает полином, исходя из исправленных значений вектора b'_{RS}.

Если количество ошибок в b'_{RS} не превышает порога t, то процесс интерполяции позволяет восстановить исходный вектор b_{RS} следующим образом:

$$b_{RS} = Decod(b'_{RS}, t), \tag{10}$$

где *Decode* – это процесс восстановления исходного вектора, который использует методы коррекции ошибок, такие как полиномы Рида-Соломона.

Таким образом, коды Рида-Соломона обеспечивают надежность, позволяя исправлять ошибки в полученных данных.

Преимущества использования кодов RS:

♦ устойчивость к ошибкам: кодирование с помощью Рида-Соломона позволяет восстановить данные, если число ошибок не превышает порога.

♦ гибкость: возможность выбора уровня избыточности в зависимости от желаемой степени защиты от ошибок.

♦ широкое применение: эти коды используются в различных областях, от хранения данных на оптических носителях до передачи данных по сети.

Генерация признаков заключается в следующем, двоичный вектор b, полученный посредством адаптивной бинаризации и закодированный с помощью RS, подается в нейросетевой блок, который, в свою очередь, генерирует закрытый ключ, что позволяет создавать уникальные приватные ключи для легитимных пользователей в процессе аутентификации без возможности компрометации сжатого устойчивого вектора биометрических признаков.

Генерирование криптографического ключа

В рамках предлагаемого метода криптографический ключ формируется на основе вектора признаков (эмбеддинга), извлечённого из лицевого изображения нейросетевой моделью с применением хеш-функции SHA-256.

Этот хеш представляет собой уникальное значение, которое не может быть преобразовано обратно в исходное изображение. Хеш-функции, как правило, необратимы, и таким образом, извлечение изображения из хеша невозможно.

Хеш-функция H применяется к данным b_{RS}, чтобы получить результат K – 256-битный хеш (криптографический ключ). Это можно записать как:

$$K = H(b_{RS}), \tag{11}$$

где

H – хеш-функция (SHA-256);

b_{RS} – входные данные (кодированный вектор, который необходимо захешировать);

K – итоговый 256-битный хеш, представляющий собой криптографический ключ.

Таким образом осуществляется вычисление криптографического хеша данных b_{RS}, который используется для создания криптографических операций [18].

Распределенное хранение криптографического ключа (схема Шамира)

Чтобы обеспечить высокую устойчивость, безопасность и отказоустойчивость при работе с криптографическими ключами применяется распределенное хранение секрета. Существует несколько решений данного вопроса, каждое из которых имеет свои особенности и области применения (табл. 2).

Таблица 2

Схемы для распределённого хранения криптографического ключа

Название	**Описание**	**Особенности**
Blakley’s Secret Sharing	Геометрическая схема на основе гиперплоскостей	Простая алгебра, менее распространена
Verifiable Secret Sharing (VSS)	Проверка корректности долей при восстановлении	Устойчива к нечестным участникам
Pedersen VSS	Схема с гомоморфными коммитментами	Применяется в протоколах с нулевым разглашением
Asymmetric Secret Sharing (ASS)	Участники имеют разные уровни доступа	Гибкая модель доверия
Proactive Secret Sharing (PSS)	Регулярное обновление долей без изменения секрета	Устойчивость при длительном хранении
Ramp Secret Sharing	Допускает частичную утечку, но снижает размер долей	Экономия объёма хранения
CRT Secret Sharing	Использует китайскую теорему об остатках	Иная математическая база, альтернатива Шамиру
Information Dispersal Algorithms (IDA)	Разделение с избыточностью без криптостойкости	Быстрая реконструкция, не защищает секрет

На практике наиболее широко применяется классическая схема разделения секрета, предложенная А. Шамиром (Shamir's Secret Sharing, SSS). Её популярность обусловлена сочетанием математической строгости, простоты реализации и высокой криптографической стойкости. Алгоритм основывается на интерполяции многочлена над конечным полем, что обеспечивает информационную безопасность: знание менее чем t долей не даёт никакой информации о секрете.

Ключевым преимуществом схемы Шамира является её широкая поддержка в современных криптографических библиотеках, таких как PyCryptodome, Charm или TSS-Lib, а также в программно-аппаратных средствах защиты информации (например, HSM и HashiCorp Vault). Этот метод активно используется в индустрии для управления ключами, реализации распределённых цифровых подписей и защиты криптовалютных кошельков.

Несмотря на существование более сложных модификаций, таких как схемы с верификацией долей (Pedersen VSS) или проактивным обновлением (PSS), именно классическая схема Шамира остаётся стандартом де-факто благодаря своей универсальности, эффективности и минимальным требованиям к вычислительным ресурсам.

Предлагается практическое применение схемы Шамира с порогом восстановления секретов. Существует решение, предложенное в статье Hall J. [19], которое представляет собой современную и безопасную реализацию распределённой генерации ключей на основе эллиптических кривых с вложенной схемой Шамира. Однако, есть направления для улучшения и расширения подхода – как с теоретической, так и с практической стороны:

- оптимизация вычислений с использованием кривых Montgomery/Edwards. Вместо Ed25519 предлагается использовать более производительные модификации Curve25519 в представлении Montgomery, что ускоряет вычисления при меньших затратах на защиту;
- замена вложенной схемы Шамира на более эффективную структуру PVSS, что позволит проверять подлинность каждой доли без полного восстановления секрета;
- использование асинхронного порогового протокола без предварительной координации. В работе предполагается синхронное взаимодействие. Однако предлагается интегрировать асинхронный протокол (FROST), который позволяет сторонам участвовать в распределённой подписи независимо;
- устойчивость к подмене долей. Предлагается внедрить проверку корректности долей через zero-knowledge доказательства, чтобы исключить возможность саботажа со стороны одного из участников схемы.

Перейдем к описанию предлагаемого улучшения схемы Шамира для распределённой генерации приватного ключа EdDSA/Ed25519, включающему несколько математических и криптографических модификаций.

1. Пусть секретный ключ $sk \in F_q$ – элемент конечного поля порядка q. На первом уровне строится многочлен $f(x)$ степени $t-1$:

$$f(x) = sk + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1}, a_i \in F_q, \quad (12)$$

Каждому участнику выдается доля $s_i = f(x_i)$, $x_i \in F_q$.

2. Каждая доля s_i дополнительно разделяется вложенной схемой через многочлен $g_i(x)$ степени (m−1):

$$g_i(x) = s_i + b_1 x + b_2 x^2 + \ldots + b_{m-1} x^{m-1}, b_j \in F_q \quad (13)$$

и создаются вложенные поддоли: $s_{i,j} = g_i(x_j), j = 1, \ldots, m$.

3. Для верифицируемости вводится система обязательных хэш-коммитментов: каждому $f(x)$ и $g_i(x)$ сопоставляется хэш-образ $H(f(x))$ и $H(g_i(x))$, публикуемый публично (например, через Merkle root).

4. Для обеспечения асинхронности протокол адаптируется под схему FROST (Flexible Round-Optimized Schnorr Threshold), где каждая доля используется для локальной генерации частей подписи без раскрытия ключа.

5. Для защиты от компрометации в незащищённой среде каждая поддоля $s_{i,j}$ хранится в средствах HSM. Ключ доступа к доле управляется политиками доступа и мультисигнатурным контролем.

6. Для применения в криптографическом алгоритме, основанном на эллиптических кривых в форме Эдвардса (Ed25519) ключ используется в виде:

$$pk = sk \cdot G, \quad (14)$$

где G – базовая точка эллиптической кривой. Формирование цифровой подписи осуществляется порогово, а проверка подписи возможна централизованно или децентрализованно.

Таким образом, предложенное расширение схемы Шамира сочетает стойкость (разделение ключей), надёжность (вложенность), верифицируемость (хэш-коммитменты), а также защищённое выполнение (TEE/HSM) и поддержку асинхронных вычислений (FROST).

Результаты исследования. В рамках исследования была проведена *программная реализация* предложенного метода формирования криптографических ключей на основе биометрических признаков, включая следующие ключевые этапы:

- детектирование лица на изображении с помощью алгоритма TinyFaceDetector;
- извлечение 68 лицевых ориентиров с использованием модели FaceLandmark68TinyNet;
- преобразование лицевых точек в вектор признаков размерности 128 с помощью сверточной нейросети на архитектуре ResNet;
- бинаризация эмбеддинга и генерация хэша ключа длиной 256 бит с использованием SHA-256;
- применение кодов Рида-Соломона для защиты от ошибок;
- разделение ключа по улучшенной схеме Шамира на несколько долей и передача части данных на удалённый сервер;
- шифрование изображения с использованием алгоритма Кузнечик;
- передача зашифрованного сообщения и получение отклика об успешной идентификации.

Алгоритм реализован на языке Python с использованием библиотек: face-recognition, dlib, numpy, hashlib, PyCryptodome, reedsolo, multiprocessing и других. Результаты тестирования производительности вычислительных этапов отражены в табл. 3 ниже.

Таблица 3

Время выполнения ключевых этапов обработки (средние значения)

Этап	Время (мс)
Обнаружение лица (TinyFaceDetector)	45
Извлечение 68 точек (FaceLandmark68TinyNet)	30
Эмбеддинг (ResNet)	40
Бинаризация и SHA-256	12
Коды Рида-Соломона	18
Секрет Шамира (3 из 5)	25
Шифрование Кузнечиком	17
Суммарное время	187

Время выполнения полной процедуры от захвата лица до получения отклика сервера составляет в среднем около 300–350 миллисекунд на стандартном ПК (без GPU-ускорения). Из них около 105 мс тратится на обнаружение лица и извлечение признаков, остальные – на генерацию ключа, шифрование и сетевое взаимодействие.

Оценка энтропии биометрических ключей

Чтобы обосновать, что криптографические ключи, полученные из биометрических признаков, обладают достаточной энтропией, сравнимой с ключами длиной 256 бит, нужно рассмотреть три ключевых аспекта: источник энтропии, обработку (усиление) и фактическую оценку. Источником случайности является биометрический вектор. Энтропия такого распределения в реальных БС (biometric systems) оценивается в диапазоне 100–140 бит (по данным NIST, IEEE) [22–25]. IEEE P2410 рекомендует использовать хэш-функции для усиления биометрических ключей.

Для обоснования криптографической стойкости ключей, полученных на основе биометрических признаков, была проведена численная симуляция, оценивающая энтропию бинарных эмбеддингов. Методика включает следующие этапы:

1. Генерация 10 000 случайных эмбеддингов размерностью 128, распределённых по нормальному закону.
2. Нормализация каждого эмбеддинга до единичной гиперсферы.
3. Преобразование эмбеддингов в бинарные дескрипторы путём пороговой бинаризации (значения > 0 приравниваются к 1, иначе 0).
4. Вычисление вероятности появления единицы в каждом из 128 битов.
5. Расчёт энтропии каждого бита по формуле:

$$H(p) = -p \cdot log_2(p) - (1-p) \cdot log_2(1-p), \quad (15)$$

где p – вероятность появления единицы в бите.

6. Суммирование энтропии по всем битам. Полученное значение энтропии составило 127.99 бит из 128 возможных, что говорит о высокой степени случайности и достаточной криптографической стойкости получаемых ключей.

Таким образом, бинаризованные эмбеддинги можно использовать в качестве источника при генерации криптографических ключей, например, с помощью SHA-256.

Необратимость биометрических признаков

Использование однонаправленной хэш-функции (SHA-256) поверх бинаризированного эмбеддинга, полученного из глубокого нейросетевого представления изображения, гарантирует криптографическую необратимость ключа. Это означает, что по полученному ключу невозможно восстановить ни биометрический шаблон, ни тем более оригинальное изображение пользователя.

Ключевые положения:

- хэш-функция SHA-256 необратима и обладает аваланш-эффектом;
- эмбеддинг лица, полученный с помощью ResNet, – это нелинейное, сжатое представление, не поддающееся обратному преобразованию;
- дополнительная бинаризация шаблона уничтожает амплитудную информацию;
- даже при наличии вектора признаков невозможно восстановить исходное изображение без генеративной модели, обученной отдельно.

Таким образом, криптографические ключи, полученные на основе биометрии, безопасны с точки зрения утечки приватной информации и соответствуют требованиям стандартов ISO/IEC 24745 и NIST SP 800-63B.

Заключение. Генерация биометрически зависимого ключа дает существенные преимущества в области безопасности, делая криптографические системы более подходящими для приложений с высоким уровнем безопасности. Любой субъект, зарегистрированный в BCS, может сгенерировать криптографические ключи при предъявлении биометрических характеристик. Затем ключи, зависящие от биометрии, передаются применяемому криптографическому алгоритму для шифрования обычных данных. Впоследствии зашифрованные данные передаются по любому ненадежному каналу. Чтобы снова расшифровать зашифрованный текст, предъявляются биометрические данные для получения ключей дешифрования.

Создание ключей шифрования на основе биометрических характеристик лица представляет собой сложную задачу, требующую учета множества факторов, связанных с получением идентификационных признаков, точностью и сложностью реализации.

Практическая ценность работы достигается путем выбора и обоснования из комплекса известных технологий тех решений, которые в своей совокупности и последовательности формируют метод, заявленный в названии статьи.

Криптографическое вычисление ключей из биометрических данных на основе устойчивой к ошибкам трансформации непрерывно значимых собственных проекций лица в строки битов с нулевой ошибкой подходит для криптографической защиты. Результирующая идентификация пользователя в терминах небольшого набора строк битов надежно сводится к одному криптографическому ключу, защищенного с помощью секретного обмена Шамира.

Были решены следующие задачи:

1. Разработан алгоритм SBC-KG, объединяющий идеи Cancelable Biometrics и коррекции ошибок. За счёт использования CNN + RS добились лучшего компромисса между ложными допусками и ложными отказами.

2. Ключи, полученные из биометрии:

♦ обладают достаточной энтропией (случайностью), сравнимой с криптографическими ключами длиной 256 бит;

♦ необратимы, то есть исключают возможность восстановления оригинального изображения из ключа, обладают достаточной энтропией (случайностью), сравнимой с криптографическими ключами длиной 256 бит;

♦ совместимы с криптографическими протоколами, поскольку: имеют корректный формат и длину (через хэш), могут быть встроены в стандартные схемы (AES, GOST, HMAC).

3. Разделение секрета (Шамира) даёт механизм распределённого хранения ключа. При утере или компрометации одного места (например, смарт-карты), злоумышленник не может восстановить ключ без других долей.

Таким образом, предложенный метод устойчив к шумам, позволяет обновлять (revocation) ключи и даёт улучшенные показатели точности, что делает его потенциально интересным для применения в банковских, государственных и корпоративных системах. Предложенный метод генерации 256-битных криптографических ключей, сгенерированных на основе биометрических признаков, позволит повысить надёжность системы идентификации и аутентификации, а пользователей избавит от необходимости носить с собой физические ключи, что сделает процесс аутентификации более удобным и быстрым.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Приказ от 24 октября 2022 г. № 524 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств».
2. *Волхонский В.В.* Системы телевизионного наблюдения: основы проектирования и применения: учеб. пособие. – М.: Горячая линия – Телеком, 2022. – 390 с.
3. ГОСТ Р 34.12-2015. «Информационная технология. Криптографическая защита информации. Блочные шифры».
4. *Soutar C., Roberge D., Stoianov A., Gilroy R., Kumar B. V. K.* Biometric Encryption™.
5. *Brown T. et al.* Large-scale Fingerprint Data Breach: Analysis and Consequences // Proc. Security Conf. – 2019.
6. *Goh A., Ngo D.C.L.* Computation of Cryptographic Keys from Face Biometrics // Proc. CMS 2003. – LNCS 2828.
7. *Ratha S., Connell J., Bolle R.* Enhancing Security and Privacy in Biometrics-Based Authentication Systems // IBM Systems Journal. – 2001.
8. *Yasuda M., Shimoyama T., Abe N., Yamada S., Shinzaki T., Koshiba T.* Privacy-Preserving Fuzzy Commitment for Biometrics via Layered Error-Correcting Codes / Garcia-Alfaro J., Kranakis E., Bonfante G. (ed.). FPS 2015. – LNCS, Vol. 9482. – Springer, Cham, 2016.
9. *Juels A., Sudan M.* A Fuzzy Vault Scheme // Designs, Codes and Cryptography. – 2002. – Vol. 38. – P. 237-257.
10. *Chitaliya N., Trivedi A.I.* Feature Extraction Using Wavelet-PCA and Neural Network for Application of Object Classification & Face Recognition // 2nd Int. Conf. on Computer Engineering and Applications. – 2010. – Vol. 1. – P. 510-514.
11. *King D.E.* Max-Margin Object Detection // ArXiv:1502.00046. – 2015.
12. ГОСТ Р ИСО/МЭК 19794-5-2013 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Ч. 5. Данные изображения лица» (утв. приказом Росстандарта от 6 сентября 2013 г. № 987-ст) (с изм. и доп.).
13. *Кольцов П.П.* Оценка размытия изображения // Компьютерная оптика. – 2011. – № 1.
14. *Лазарев К.В., Калиберда И.В., Костоглотов А.А., Сарыев М.М.* Метод биометрической двухфакторной аутентификации с использованием определения жизнеспособности // AISMA-2024: Конспект лекций. – Т. 863. – Springer, 2024.

15. *Кононыхин И.А., Ежов Ф.В., Мартынюк Р.А. и др.* Реализация системы распознавания и отслеживания лиц // Молодой ученый. – 2020. – № 28 (318). – С. 8-12. – URL: https://moluch.ru/archive/318/72492//.
16. *Schroff, F., Kalenichenko, D., & Philbin, J.* FaceNet: A Unified Embedding for Face Recognition and Clustering // arXiv.org. – 2015. – URL: https://arxiv.org/abs/1503.03832 (дата обращения: 30.06.2025).
17. *Дружинин В.И., Кузьмин О.В.* Коды Рида-Соломона в системах обнаружения и исправления ошибок при передаче данных // Современные технологии. Системный анализ. Моделирование. – 2015. – № 1 (45).
18. *Дремов И.С., Гирина А.Н.* Использование алгоритма SHA-256 для хеширования данных // Тенденции развития науки и образования. – 2022. – № 86-1. – С. 57-61. – DOI 10.18411/trnio-06-2022-19. – EDN ZIKXGD.
19. *Hall J. L., Hertzog Y., Loewy M. et al.* Manifesting Unobtainable Secrets: Threshold Elliptic Curve Key Generation using Nested Shamir Secret Sharing // arXiv preprint. – 2023. – URL: https://arxiv.org/abs/2309.00915 (дата обращения: 20.06.2025).
20. *Spacek L.* Faces94 Database. University of Essex [Электронный ресурс].
21. *Huang G.B., Ramesh M., Berg T., Learned-Miller E.* Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments. – 2007.
22. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. – National Institute of Standards and Technology, Gaithersburg, MD, USA, 2017. – Режим доступа: https://pages.nist.gov/800-63-3/sp800-63b.html.
23. ISO/IEC 19792:2009. Information technology – Security techniques – Security evaluation of biometrics. – International Organization for Standardization, Geneva, 2009. – 37 p. – Режим доступа: https://www.iso.org/standard/42136.html.
24. IEEE P2410. Standard for Biometric Open Protocol Standard (BOPS). – IEEE Standards Association, 2023. – Режим доступа: https://standards.ieee.org/ieee/2410/6314/.
25. *Dodis Y., Ostrovsky R., Reyzin L., Smith A.* Fuzzy extractors: How to generate strong keys from biometrics and other noisy data // SIAM Journal on Computing. – 2008. – Vol. 38, No. 1. – P. 97-139.

REFERENCES

1. Prikaz ot 24 oktyabrya 2022 g. № 524 «Ob utverzhdenii trebovaniy o zashchite informatsii, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh, s ispol'zovaniem shifroval'nykh (kriptograficheskikh) sredstv» [Order No. 524 of October 24, 2022, "On Approval of Requirements for the Protection of Information Contained in State Information Systems Using Encryption (Cryptographic) Means"].
2. *Volkhonskiy V.V.* Sistemy televizionnogo nablyudeniya: osnovy proektirovaniya i primeneniya: ucheb. posobie [Television surveillance systems: design and application fundamentals: a tutorial]. Moscow: Goryachaya liniya – Telekom, 2022, 390 p.
3. GOST R 34.12-2015. «Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnye shifry» [GOST R 34.12-2015 «Information technology. Cryptographic data security. Block ciphers»].
4. *Soutar C., Roberge D., Stoianov A., Gilroy R., Kumar B. V. K.* Biometric Encryption™.
5. *Brown T. et al.* Large-scale Fingerprint Data Breach: Analysis and Consequences, *Proc. Security Conf.*, 2019.
6. *Goh A., Ngo D.C.L.* Computation of Cryptographic Keys from Face Biometrics, *Proc. CMS 2003*, LNCS 2828.
7. *Ratha S., Connell J., Bolle R.* Enhancing Security and Privacy in Biometrics-Based Authentication Systems, *IBM Systems Journal*, 2001.
8. *Yasuda M., Shimoyama T., Abe N., Yamada S., Shinzaki T., Koshiba T.* Privacy-Preserving Fuzzy Commitment for Biometrics via Layered Error-Correcting Codes,Garcia-Alfaro J., Kranakis E., Bonfante G. (ed.). FPS 2015. LNCS, Vol. 9482. Springer, Cham, 2016.
9. *Juels A., Sudan M.* A Fuzzy Vault Scheme, *Designs, Codes and Cryptography*, 2002, Vol. 38, pp. 237-257.
10. *Chitaliya N., Trivedi A.I.* Feature Extraction Using Wavelet-PCA and Neural Network for Application of Object Classification & Face Recognition, *2nd Int. Conf. on Computer Engineering and Applications*, 2010, Vol. 1, pp. 510-514.
11. *King D.E.* Max-Margin Object Detection, *ArXiv:1502.00046*, 2015.
12. GOST R ISO/MEK 19794-5-2013 «Informatsionnye tekhnologii. Biometriya. Formaty obmena biometricheskimi dannymi. Ch. 5. Dannye izobrazheniya litsa» (utv. prikazom Rosstandarta ot 6 sentyabrya 2013 g. № 987-st) (s izm. i dop.) [GOST R ISO/IEC 19794-5-2013 "Information technology. Biometrics. Biometric data exchange formats. Part 5. Facial image data" (approved by order of Rosstandart dated September 6, 2013 No. 987-st) (as amended and supplemented)].

13. *Kol'tsov P.P.* Otsenka razmytiya izobrazheniya [Image blur assessment], *Komp'yuternaya optika* [Computer Optics], 2011, No. 1.
14. *Lazarev K.V., Kaliberda I.V., Kostoglotov A.A., Saryev M.M.* Metod biometricheskoy dvukhfaktornoy autentifikatsii s ispol'zovaniem opredeleniya zhiznesposobnosti [A Method of Biometric Two-Factor Authentication Using Liveness Determination], *AISMA-2024: Konspekt lektsiy* [AISMA-2024: Lecture notes], Vol. 863. Springer, 2024.
15. *Kononykhin I.A., Ezhov F.V., Martynyuk R.A. i dr.* Realizatsiya sistemy raspoznavaniya i otslezhivaniya lits [Implementation of a face recognition and tracking system], *Molodoy uchenyy* [Young Scientist], 2020, No. 28 (318), pp. 8-12. Available at: https://moluch.ru/archive/318/72492//.
16. *Schroff, F., Kalenichenko, D., & Philbin, J.* FaceNet: A Unified Embedding for Face Recognition and Clustering, *arXiv.org*, 2015. Available at: https://arxiv.org/abs/1503.03832 (accessed 30 June 2025).
17. *Druzhinin V.I., Kuz'min O.V.* Kody Rida-Solomona v sistemakh obnaruzheniya i ispravleniya oshibok pri peredache dannykh [Reed-Solomon codes in error detection and correction systems for data transmission], *Sovremennye tekhnologii. Sistemnyy analiz. Modelirovanie* [Modern technologies. Systems analysis. Modeling], 2015, No. 1 (45).
18. *Dremov I.S., Girina A.N.* Ispol'zovanie algoritma SHA-256 dlya kheshirovaniya dannykh [Using the SHA-256 algorithm for data hashing], *Tendentsii razvitiya nauki i obrazovaniya* [Trends in the Development of Science and Education], 2022, No. 86-1, pp. 57-61. DOI 10.18411/trnio-06-2022-19. EDN ZIKXGD.
19. *Hall J. L., Hertzog Y., Loewy M. et al.* Manifesting Unobtainable Secrets: Threshold Elliptic Curve Key Generation using Nested Shamir Secret Sharing, *arXiv preprint*, 2023. Available at: https://arxiv.org/abs/2309.00915 (accessed 20 June 2025).
20. *Spacek L.* Faces94 Database. University of Essex [Electronic resource].
21. *Huang G.B., Ramesh M., Berg T., Learned-Miller E.* Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments, 2007.
22. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. National Institute of Standards and Technology, Gaithersburg, MD, USA, 2017. Available at: https://pages.nist.gov/800-63-3/sp800-63b.html.
23. ISO/IEC 19792:2009. Information technology – Security techniques – Security evaluation of biometrics. International Organization for Standardization, Geneva, 2009, 37 p. Available at: https://www.iso.org/standard/42136.html.
24. IEEE P2410. Standard for Biometric Open Protocol Standard (BOPS). – IEEE Standards Association, 2023. Available at:https://standards.ieee.org/ieee/2410/6314/.
25. *Dodis Y., Ostrovsky R., Reyzin L., Smith A.* Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, *SIAM Journal on Computing*, 2008, Vol. 38, No. 1, pp. 97-139.

Калиберда Игорь Владимирович – Пятигорский институт (филиал) Северо-Кавказскго федерального университета; e-mail: kaliberda-igor@yandex.ru; г. Пятигорск, Россия; тел.: +79283632214; кафедра систем управления и информационных технологий; старший преподаватель.

Kaliberda Igor Vladimirovich – Pyatigorsk Institute (Branch of NCFU); e-mail: kaliberda-igor@yandex.ru; Pyatigorsk, Russia; phone: +79283632214; the Department of Management Systems and Information Technologies; senior lecturer.