УДК 004.056

А.М.ВУЛЬФИН, Р.Р. ЯГАФАРОВ

[*roma.yagafarov@gmail.com*](mailto:roma.yagafarov@gmail.com)

Науч. руковод. - канд. техн. наук, доцент А.М.ВУЛЬФИН

***Уфимский государственный авиационный технический университет***

**АЛГОРИТМЫ НЕЙРОСЕТЕВОЙ КРИПТОГРАФИИ**

*Аннотация***:** Создание ключевых цепочек последовательностей символов (далее – паролей) постепенно теряет актуальность в силу возможности их перехвата, кражи и дальнейшей модификации из-за невысокой сложности или же низкой степени защищенности, что и является проблемой. Актуальность работы состоит в том, что биометрия позволяет забыть о запоминании паролей, и использовать свои черты лица для создания (а в дальнейшем и использования) уникального пароля. Цель работы: рассмотреть применение нейросетевых технологий в криптографических системах, предложить метод по созданию секретной пары ключей (Key, Initialization Vector) для дальнейшего шифрования по алгоритму Advanced Encryption Standard (AES).

*Ключевые слова:*биометрия; нейронные сети; криптография; нейросетевая криптография.

**Введение**

Использование биометрических данных в настоящее время приобрело повсеместное распространение (как пример, использование лица или отпечатка пальца при аутентификации и (или) идентификации от простой разблокировки телефона, до входа в банковское хранилище). Использование биометрии действительно удобное решение, так как пропадает надобность в запоминании паролей, которые могут быть успешно забыты в лучшем случае, в худшем – перехвачены, украдены, а в дальнейшем – изменены. Считается, что использование биометрических данных в качестве ключа/пароля означает, что такие данные подделать невозможно, однако стоит помнить, что в случае кражи таких данных самому пользователю будет труднее отозвать образцы данных, нежели чем простой пароль или аппаратный ключ.

Углубляясь в предмет биометрических данных [1], переходим к тому, что практический аспект распознавания образов на текущий момент чаще всего сводится [2] к использованию искусственных нейронных сетей, а в последнее время в связи с развитием технологий и повышением вычислительных мощностей – с нейронными сетями глубокого обучения.

Т.к. биометрия может использоваться в качестве секретного ключа (пароля) или пары ключей, то это означает, что биометрию можно использовать и в качестве создания шифра (ассиметричного шифра), для обеспечения конфиденциальности, безопасности неких важных данных.

**Применение нейросетевых технологий в криптографических системах**

В основе современных криптографических систем шифрования данных лежат два принципа управления ключами. Первый использует один секретный ключ, который должен быть известен только абонентам, передающим информацию. Второй принцип базируется на двухключевой схеме, в которой один ключ является открытым и используется для шифрования, а второй – секретным и используется для дешифрования. Достоинства симметричных криптосистем заключаются в высокой скорости обработки данных. Их недостатком является низкая эффективность управления ключами, которая требует дополнительных механизмов безопасности. При проектировании систем защиты информации руководствуются высокой однородностью данных систем для обеспечения высокой криптостойкости. Поэтому асимметричное шифрование и системы на их основе более привлекательны для применения в компьютерных сетях. Однако в вычислительном отношении использование несимметричных схем менее эффективно, поскольку одним из криптографических примитивов является возведение в степень по модулю, что приводит к существенным вычислительным затратам и снижению общей производительности.

В развитии криптографических систем с открытым ключом можно выделить [2] несколько направлений. Первое связано с построением и совершенствованием арифметических и функциональных расширителей персональных ЭВМ. Использование китайской теоремы об остатках позволяет на порядок увеличит производительность шифропроцессора RSA. Для второго пути развития характерен поиск более эффективных конечных алгебраических структур. Примером являются криптосистемы на базе эллиптических кривых, использующие ключи разрядности меньше, чем ключи RSA. Третье направление является экстенсивным, поскольку ему свойственен лишь выбор открытых и секретных параметров, удовлетворяющих заданному быстродействию, в рамках одной криптосистемы.

Для решения прикладных задач обеспечения информационной безопасности их переводят в нейросетевой логический базис в случае, когда стоимость вычислительной системы значительно возрастает при достижении необходимого времени решения задачи. Нейрокомпьютеры используются для шифрования и дешифрования, формирования секретного ключа, порогового разделения данных мультимедиа и т. д. За счет массового параллелизма нейронных сетей решение задач большой размерности осуществляется за время, недоступное классическим ЭВМ.

Однако недостаток, заключающийся в отсутствии прозрачности нейронной сети, ограничивает возможности использования нейротехнологий в криптографии. Так, при компрометации ключа или при его пролонгации требуется полное переобучение сети. Поэтому в нейросетевой криптографии нашли применение специфические структуры и режимы работы нейронных сетей: нейронные сети конечного кольца (НСКК), хаотические нейронные сети, нейронные сети с обратными связями и др.

Целью работы является совершенствование систем нейросетевой криптографии при помощи преобразований биометрических признаков в уникальный криптографический ключ (пару ключей) для решения проблемы утеря доступа, перехвата, кражи, внесения модификаций в криптографический ключ.

**Система нейросетевой криптографии на основе биометрических признаков**

В данной работе предлагается метод создания уникальной пары ключей (Key, Initialization Vector) для дальнейшего шифрования по алгоритму Advanced Encryption Standard (AES) на основе возвращаемых данных обученной нейронной сети.

Обученная нейронная сеть возвращает в качестве одного из параметров пары значений – координаты ориентиров (относительно X, Y) лица (пример см. рис. 1) на изображении.

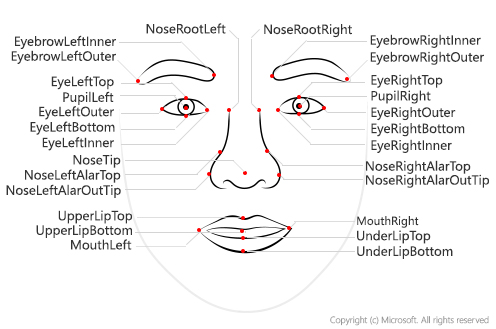


Рисунок 1. Ориентиры лица

Так, при формировании пары ключей, если в базе данных хранится похожее с большой вероятностью лицо, то в наше распоряжение можем получить 2 значения (как пример, подъем правой брови справа по X \* уголок рта слева по Y + местоположение левого зрачка по X и аналогичное второе число). Для полученных двух чисел можно вычислить хэш-функцию для каждого, и использовать полученную пару хэшей для дальнейшего шифрования (см. рис. 2). В работе использовалось вычисление хэш-функции по алгоритму SHA-2 (SHA-512), а в качестве криптографического ключа были отобраны первые 16 байт вычисленной хэш-функции (аналогичный отбор и для Initialzation Vector).

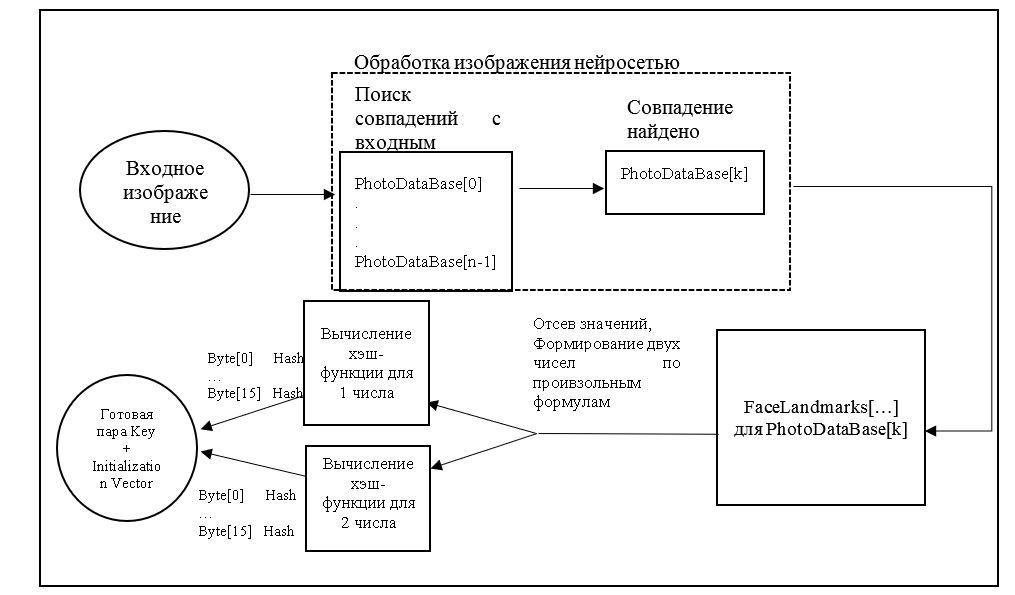


Рисунок 2. Схема формирования пары ключей на основе ориентиров лица

**Эксперимент**

Для проведения эксперимента был использован набор данных (датасет) [3] из 65 изображений с изображениями лиц людей [4]. Формирование пары ключей для соответствующего изображения выполняла программа (см. рис. 3) написанная на языке C# [5] в соответствии со схемой работы программы (см. рис. 2).

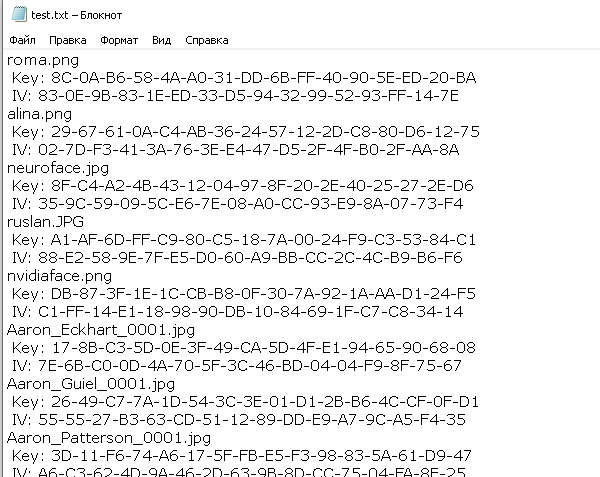


Рисунок 3. Пример создания пары ключей для соответствующих изображений из базы данных

**Анализ результатов**

В ходе анализа результатов был использован сервис по нахождению совпадений в текстовых файлах [6]. Результат показал 1 совпадение на 65 пар ключей (см. рис. 4).

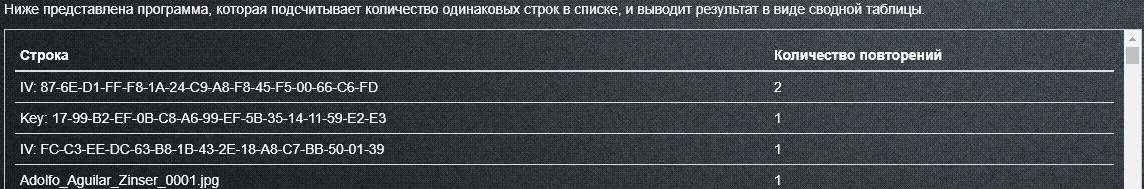


Рисунок 4. Анализ количества повторений ключа

Выводом анализа служит утверждение о том, в 1/130 случаев может произойти ошибка второго рода, когда нарушитель быть классифицирован как авторизованный пользователь (может произойти промах).

**Выводы**

В работе предложен метод по созданию секретных криптографических пар ключей на основе биометрии лица.

Анализ результатов приводит к выводу о присутствии несущественной ошибке промаха, т.к. при шифровании файлов по алгоритму AES необходима пара из 2 ключей.

# **Список использованной литературы**

|  |
| --- |
| 1. Гультяева Т.А., Основы информационной безопасности, Новосибирск: НГТУ, 2018. |
| 1. Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н., Применение искусственных нейронных сетей и системы остаточных классов в криптографии, М.: Физматлит, 2012. |
| 1. Вичугова А., «Отберем то, что нужно Data Mining: как сформировать датасет для машинного обучения» 05 Май 2019. [В Интернете]. Available: https://www.bigdataschool.ru/blog/dataset-data-preparation.html. [Дата обращения: 20 Август 2020]. |
| 1. Huang G., «Labeled Faces in the Wild» Gary Huang, 09 Январь 2018. [В Интернете]. Available: http://vis-www.cs.umass.edu/lfw/#download. [Дата обращения: 20 Август 2020]. |
| 1. Р. Ягафаров, «GitHub: страница проекта» [В Интернете]. Available: https://github.com/romaib116/NIR2020. |
| 1. А.Дорохов, «Подсчёт количества одинаковых строк в списке» Андрей Дорохов, [В Интернете]. Available: https://dorohoff.net/tools/repeats-calculator. |