УДК 004.056.52 **DOI: 10.18413/2518-1092-2019-4-2-0-8**

Гончаренко Ю.Ю.
Нестеренко В.Р.

ИСПОЛЬЗОВАНИЕ СЛУЧАЙНЫХ БИОМЕТРИЧЕСКИХ ОБРАЗОВ ДЛЯ ГЕНЕРАЦИИ КРИПТОСТОЙКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПРИМЕНЕНИЕМ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ НЕЙРОННЫХ СЕТЕЙ

ФГАОУ ВО «Севастопольский государственный университет»,
ул. Университетская 33, г. Севастополь, 299053, Россия

e-mail: iuliay1985@mail.ru, closetonowhere@protonmail.com

Аннотация
В данной статье рассмотрены перспективы, технологии и способы использования биометрических данных в криптосистемах. А также предложен способ использования случайных биометрических данных для генерации 256-битных последовательностей.
Ключевые слова: биометрический образ; генеративно-состязательные нейронные сети; искусственные нейронные сети; криптография.

UDC 004.056.52

Goncharenko J.J.
Nesterenko V.R.

USE OF RANDOM BIOMETRIC IMAGES FOR GENERATING CRYPTO-RESISTANT SEQUENCES USING GENERATIVE-COMPETITIVE NEURAL NETWORKS

FSAEI HE "Sevastopol state University", University street 7, Sevastopol, 299053, Russian

e-mail: iuliay1985@mail.ru, closetonowhere@protonmail.com

Abstract
This article discusses the prospects, technologies and methods of using biometric data in cryptosystems. A method of using random biometric data for generating 256-bit sequences is also proposed.
Keywords: biometric image; generative-competitive neural networks; artificial neural networks; cryptography.

ВВЕДЕНИЕ

Криптографические системы с использованием биометрических данных открывают новые перспективы в обеспечении информационной безопасности. Совокупность таких технологий, как преобразование нечетких биометрических параметров в ключевые последовательности, распознавание биометрических образов и криптография, образуют новый вид криптографии – биометрическую криптографию. В криптосистемах такого вида ключи зависят от биометрических данных абонентов.

Со стремительным развитием алгоритмов машинного обучения и алгоритмов распознавания образов, качество биометрических криптосистем многократно возросло, что проявляется в снижении ошибок первого и второго рода и в повышении надежности.

Выделяют три вида биометрических криптосистем в зависимости от цели: биометрические криптографические системы с освобождением ключа, биометрические криптографические системы со связыванием ключа и биометрические криптографические системы с генерацией ключа.

В криптосистемах с освобождением ключа биометрический эталон и ключ хранятся отдельно друг от друга и процесс аутентификации осуществляется независимо от операции

освобождения ключа. Ключ освобождается после аутентификации пользователя. В криптосистемах со связыванием ключа биометрический эталон и ключ связаны криптографическим преобразованием. Ключ закрывается биометрическими данными и может быть раскрыт только обладателем соответствующих биометрических параметров. Криптосистемы с генерацией ключа обладают отличительной особенностью: ключ генерируется из биометрических данных пользователя [1]. Подобный подход позволяет не передавать ключ, а передавать только биометрические данные. Генерация ключа происходит с использованием преобразования «биометрический образ – код». Используя данные преобразование, становится возможным выделять из вектора биометрических данных двоичный код размером 256 бит.

Последние достижения в машинном обучении, а именно создание генеративно-состязательной нейронной сети, и преобразование «биометрический образ-код» предоставляют альтернативный способ использовать биометрические данные в криптосистемах: теоретически использовать псевдослучайные биометрические данные для генерации ключей и псевдослучайных последовательностей размером 256 бит.

ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫЕ НЕЙРОСЕТИ

Генеративно-состязательная сеть (GAN) – алгоритм машинного обучения без учителя, состоящий из двух нейронных сетей: генератора и дискриминатора. Одна из основных целей такой нейронной сети – генерация искусственно-созданных изображений определенных объектов, которые будут максимально неотличимы от изображений реально существующих объектов. На вход генератора подается случайный вектор, который будет преобразован в изображение и отправлен в дискриминатор. Дискриминатор производит сравнения сгенерированного изображения с реальными примерами и поддерживает обратную связь с генератором. Со временем генератор начнет производить более реалистичные изображения, а дискриминатор будет все сложнее и сложнее обойти. Таким образом, в процессе обучения изображения будут генерироваться с каждым разом все более приближенно к реальным объектам. Изображение создается следующим образом: начинается создание основание изображения с малого разрешения, постепенно повышая разрешение и добавляя новые детали на изображение. Подобный подход был предложен в 2018 разработчиками из NVidia и назван ProGAN.

StyleGAN – нейронная сеть, основанная на ProGAN, но с некоторыми нововведениями, качественно меняющими принцип работы Генератора с входными данными. В ProGAN генерация изображения полностью зависела от входного случайного вектора значений и данных, которые были до этого использованы для обучения. Например, если изображения с людьми с черными волосами повторяются слишком часто в наборе данных, то большая часть входных значений случайного вектора будет «привязана» к этой особенности.

Однако в StyleGAN реализована еще одна нейронная сеть, которая обрабатывает поток входных случайных данных генератора таким образом, чтобы создать новый вектор $\overline{W}$, который не должен зависеть от распределения особенностей при тренировке и должен понизить корреляцию между биометрическими особенностями [2].

$$AdaIN\left(x_i, y\right) = y_{s,i}\frac{x_i - \mu\left(x_i\right)}{\sigma\left(x_i\right)} + y_{b,i}, \quad (1)$$

где $y_{s,i}$ – вектор масштаба;

$y_{b,i}$ – вектор смешения;

x_i – результат операции свертки.

Адаптивная нормализация образца (AdaIN) – модуль, который переводит данные вектора W в сгенерированное изображение. Модуль добавляется на каждый уровень разрешения

нейронной сети и определяет визуальное отображение особенностей лица на данном уровне разрешения (рис. 1)

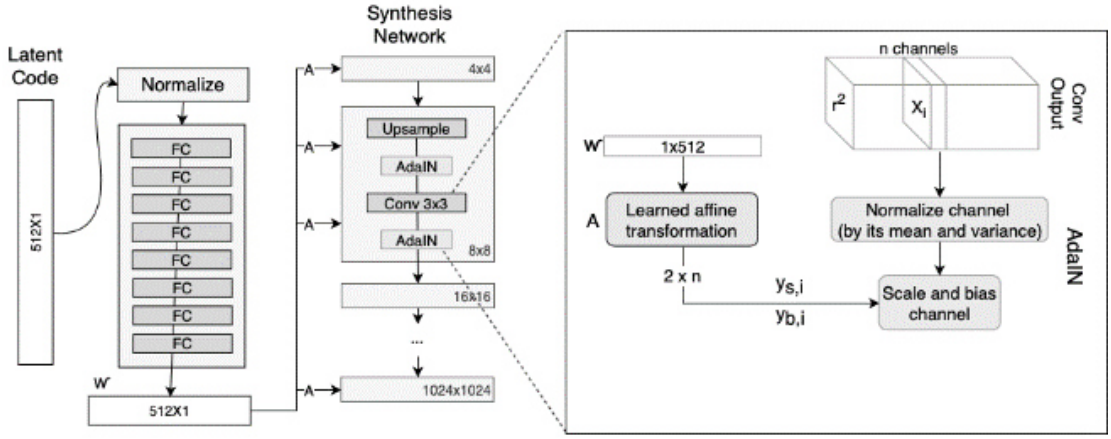

Рис. 1. Генеративно-состязательная нейронная сеть AdaIN
Fig. 1. Generative-adversarial neural network AdaIN

Визуальное отображение определяется в 3 этапа:

1) каждый канал выхода сверточного слоя нормализуется, чтобы убедиться в том, что этап 3 имеет ожидаемый эффект;

2) слой A преобразовывает вектор $\overline{W}$ в векторы масштаба и смещения для каждого канала;

3) векторы масштаба и смещения сдвигают каждый канал выхода операции свертки.

Эта настройка переводит информацию из вектора $\overline{W}$ в ее визуальное отображение [2].

Множество аспектов человеческого лица достаточно малы и могут рассматриваться, как случайные. Например, морщины, веснушки, пятна, точное положение волос. Для повышения реалистичности изображения данные виды особенностей должны размещаться максимально случайно. Для этого используется шум, который вводится в каждый канал нейронной сети, перед операцией AdaIN и изменяет немного отображение особенностей лица, которые вводятся в соответствующих слоях (рис. 2) [2].

Генерация каждого лица в данной системе организована таким образом, что множество биометрических особенностей приближено к случайному. Учитывая введение шума в каждом слое нейронной сети, который отвечает за добавление определенных особенностей на генерируемое изображение, можно сделать вывод, что каждый биометрический эталон, включая мельчайшие особенности лица, будет приближен к оригинальному. Вероятность повторения такого эталона крайне мала, учитывая архитектуру нейронной сети и природу шума, вводимого после каждой операции AdaIN.

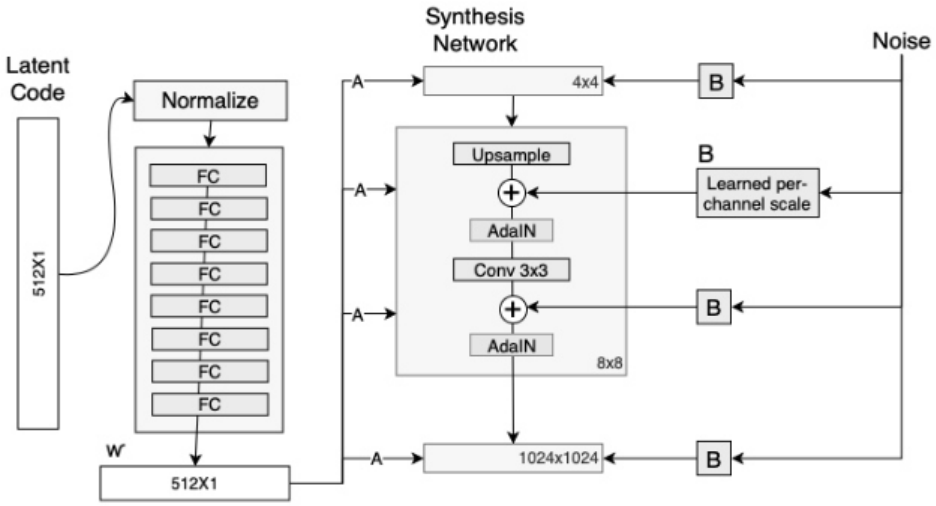

Рис. 2. Генеративно-состязательная нейронная сеть с добавлением шума
Fig. 2. Generative-adversarial neural network with the addition of noise

Для выделения биометрических эталонов с изображения лица целесообразно будет использовать один из алгоритмов распознавания лиц. Для решения задачи распознавания образов оптимальны сверточные нейронные сети [3].

ПРЕОБРАЗОВАНИЕ «БИОМЕТРИЯ-КОД»

Когда набор биометрических данных для случайно сгенерированного лица будет выделен и сформирован, необходимо переводить данную совокупность биометрических характеристик в 256-битный код. Существует два приемлемых способа преобразования «биометрия – код»: нечеткие экстракторы и нейросетевые преобразователи.

Нечеткие экстракторы позволяют восстанавливать секретный ключ из неточно воспроизводимых биометрических данных [4]. Метод извлекает случайную последовательность из изначальных биометрических данных, а затем восстанавливает ее из любых данных, имеющих минимальные отличия с изначальными.

Нейросетевой преобразователь «биометрия – код» – заранее обученная искусственная нейронная сеть с большим числом входов и выходов, преобразующая частично случайный вектор входных биометрических параметров «СВОЙ» в однозначный код криптографического ключа и преобразующая любой иной случайный вектор входных данных в случайный выходной код [5]. Результатом такого преобразования будет 256-битный криптостойкий код, полученный преобразованием биометрического образа человека. Данный преобразователь наиболее оптимально использовать для получения последовательностей и ключей длиной 256 бит.

Нейросетевой преобразователь «Биометрия – код доступа» на уровне работы нейрона первого слоя (320 нейронов) может быть описан формулами

$$x_1 = \overline{M} \cdot \bar{a} \cdot \Delta = \Delta \cdot \sum_{j}^{n} M_j \cdot a_j , \tag{2}$$

$$y_1(x_1) = \frac{2}{1+e^{x_1}} - 1 , \tag{3}$$

$$f_1(y_1) = \begin{cases} 1, y_1 \geq 0 \\ -1, y_1 < 0 \end{cases}, \tag{4}$$

где $\bar{a}$ – вектор биометрических данных;

n –количество биометрических данных в векторе $\bar{a}$;

$\overline{M}$ – вектор весовых коэффициентов, первого слоя нейронной сети, соответствующий вектору $\bar{a}$;

x_1 – результат работы сумматора нейрона первого слоя;

Δ –коэффициент использования вектора в нейроне ($\Delta = 1$, если используется в данном нейроне, в ином случае 0);

y_1 – передаточная функция первого слоя нейронной сети;

f_1 –решающее правило для нейрона первого слоя.

Второй слой данной нейронной сети состоит из 256 нейронов и принимает на вход вектор $\bar{t}$ – результирующий вектор первого слоя, состоящий из 320 элементов. Каждый нейрон второго слоя можно описать следующим образом

$$x_2 = \sum \overline{M} \cdot \bar{t} \cdot \Delta = \Delta \cdot \sum_{k}^{320} M_k \cdot t_k , \quad (5)$$

$$y_2(x_2) = \frac{2}{1+e^{x_2}} - 1, \quad (6)$$

$$f_2(y_2) = \begin{cases} 1, y_2 \geq 0 \\ -1, y_2 < 0 \end{cases}, \quad (7)$$

где $\overline{M}$ – вектор весовых коэффициентов, второго слоя нейронной сети, соответствующий вектору $\bar{t}$;

x_2 – результат работы сумматора нейрона второго слоя;

Δ – коэффициент использования вектора в нейроне. ($\Delta = 1$, если используется в данном нейроне, в ином случае 0);

y_2 – передаточная функция второго слоя нейронной сети;

f_2 –решающее правило для нейрона второго слоя.

Результат работы каждого нейрона второго слоя является битом секретного криптографического ключа длиной 256 бит, генерируемого из вектора биометрических данных [6].

ВЫВОДЫ

Совокупность приведенных в данной статье технологий и решений позволяет генерировать криптостойкие ключи и псевдослучайные последовательности длиной 256 бит. Способ генерации ключевой последовательности в таком случае сводится к простому алгоритму:

1) генерируется случайное изображение человеческого лица нейросетью StyleGAN;
2) с помощью алгоритмов распознавания создается биометрический образ (вектор биометрических характеристик);
3) вектор биометрических характеристик подается на преобразователь «биометрия-код»;
4) полученный на выходе код является ключевой псевдослучайной последовательностью.

Учитывая, что таких комбинаций 2^{256}, можно сделать вывод о низкой вероятности коллизий при генерации для двух случайных лиц.

Сгенерированный таким образом ключ можно использовать в алгоритме шифрования «Кузнечик», чтобы обеспечить дополнительную криптографическую стойкость при шифровании.

Данный способ позволяет обеспечить необходимую криптостойкость псевдослучайной ключевой последовательности за счет сложной структуры нейронной сети StyleGAN и введения шумов во все каналы перед операцией AdaIN. Совокупность этих особенностей в теории также открывает дополнительные перспективы для дальнейшего улучшения данного метода путем манипуляций с видами шума и его возможной аппаратной реализацией, а также путем возможных улучшений взаимодействия компонентов системы.

Список литературы

1. Uludag U., Pankanti S., Prabhakar S. and Jain A.K. Biometric cryptosystems: issues and challenges. Proceedings of the IEEE, 2004. – Vol. 92, № 6. – P. 948–960.
2. Style-based GANs – Generating and Tuning Realistic Artificial Faces, 2018, URL: https://www.lyrn.ai/2018/12/26/a-style-based-generator-architecture-for-generative-adversarial-networks/ (дата обращения: 13.02.2019).
3. Друки А. А. Система поиска, выделения и распознавания лиц на изображениях // Известия ТПУ. 2011. №5.
4. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data // April 13, 2004.
5. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации». URL: http://docs.cntd.ru/document/1200048922 (дата обращения: 21.02.2019).
6. Гончаров С. М., Боршевников А. Е. Построение нейросетевого преобразователя «Биометрия код доступа» на основе параметров визуального вызванного потенциала электроэнцефалограммы // Доклады ТУСУР. 2014. №2 (32).

References

1. Uludag U., Pankanti S., Prabhakar S. and Jain A.K. Biometric cryptosystems: issues and challenges. Proceedings of the IEEE, 2004. – Vol. 92, № 6. – P. 948–960.
2. Style-based GANs – Generating and Tuning Realistic Artificial Faces, 2018, URL: https://www.lyrn.ai/2018/12/26/a-style-based-generator-architecture-for-generative-adversarial-networks/ (handling date: 13.02.2019).
3. Druki A. Search, selection and face recognition system for images. Izvestiya TPU. №5, 2011.
4. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. April 13, 2004.
5. GOST R 52633-2006 "Information protection. Information security technology. Requirements for highly reliable biometric authentication" URL: http://docs.cntd.ru/document/1200048922 (handling date: 21.02.2019).
6. Goncharov S. M., Borshevnikov A. E. Construction of a neural network Converter "Biometrics access code" based on the parameters of the visual evoked potential of the electroencephalogram. Doklady TUSUR. №2 (32), 2014.

Гончаренко Юлия Юрьевна, доктор технических наук, доцент, профессор кафедры «Информационная безопасность» ФГАОУ ВО «Севастопольский государственный университет»
Нестеренко Владимир Романович, студент четвертого курса кафедры «Информационная безопасность» ФГАОУ ВО «Севастопольский государственный университет»

Goncharenko Julia Jurievna, doctor of technical Sciences, associate Professor, Professor of "Information security" FSAEI HE "Sevastopol state University", "Sevastopol state University", "Sevastopol state University", University street 7, Sevastopol, 299053, Russian.
"Sevastopol state University"
Nesterenko Vladimir Romanovich, fourth-year student of the Department "Information security" FSAEI HE "Sevastopol state University"