

ТЕХНОЛОГИЧЕСКИЕ ОСНОВЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ И КАЧЕСТВА ИЗДЕЛИЙ

УДК 004.056; 51-76

DOI 10.21685/2307-4205-2017-2-5

СИНТЕЗ ТЕСТОВЫХ ОБРАЗОВ ДЛЯ ОЦЕНКИ СТОЙКОСТИ НЕЙРОСЕТЕВЫХ ПРЕОБРАЗОВАТЕЛЕЙ В СИСТЕМАХ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

А. К. Гришко, В. С. Лукин, Н. К. Юрков

Введение

Благодаря высоким оперативно-техническим характеристикам биометрические средства защиты информации уже более 20 лет пользуются заслуженным вниманием специалистов.

Развитие современных нейросетевых преобразователей биометрия-код характеризуется значительным увеличением их сложности [1–4]. Оценка их стойкости является одной из важнейших задач, стоящих перед разработчиками данного вида аппаратуры. Оценка производится тестированием с помощью биометрических образов [5–7]. Так как для тестирования требуется большое количество образов, их нецелесообразно вводить вручную, потому что данный метод создания образов занимает слишком много времени и является малоэффективным. Чтобы процесс создания тестовых образов был автоматизирован, необходимо разработать модель, которая бы по заданным параметрам и требованиям выполняла эти действия в автоматическом режиме.

Определение и анализ статистических параметров образов

Генерация случайных векторов не может быть применена в решении задачи построения баз образов, так как для создания нужно повторять статистические характеристики рукописных образов для более точной оценки работы биометрических программ. Если использовать стандартные функции генерации случайных чисел, можно получить вектора, чьи параметры заведомо будут выходить из области определения образов «все чужие», что в свою очередь на этапе тестирования будут давать ложную информацию и занижать ошибку второго рода [7–10].

На начальном этапе уточняется количество желаемых векторов, которые будут получены на выходе программы. Производится анализ статистических данных образов «СВОЙ». Подсчет математического ожидания и дисперсии осуществляется по каждому параметрам векторов «СВОЙ». Реализован алгоритм создания корреляционной матрицы по всем параметрам размерностью 480 на 480. Далее вычисляется средний коэффициент корреляции по модулю для дальнейшего его применения в алгоритме генерации тестовых биометрических рукописных образов «Чужие».

Одна из наиболее распространенных задач статистического исследования состоит в изучении связи между выборками. Обычно связь между выборками носит не функциональный, а вероятностный (или стохастический) характер. В этом случае нет строгой, однозначной зависимости между величинами [11–13]. При изучении стохастических зависимостей различают корреляцию и регрессию.

Корреляционный анализ состоит в определении степени связи между двумя случайными величинами X и Y . В качестве меры такой связи используется коэффициент корреляции [14–17].

Коэффициент корреляции оценивается по выборке объема n связанных пар наблюдений (x_i, y_i) из совместной генеральной совокупности X и Y . Существует несколько типов коэффициентов корреляции, применение которых зависит от измерения (способа шкалирования) величин X и Y .

Для оценки степени взаимосвязи величин X и Y , измеренных в количественных шкалах, используется коэффициент линейной корреляции (коэффициент Пирсона), предполагающий, что выборки X и Y распределены по нормальному закону. На рис. 1 представлен пример двух образов «СВОЙ».

Коэффициент корреляции – параметр, который характеризует степень линейной взаимосвязи между двумя выборками, рассчитывается по формуле

$$r_{xy} = \frac{\sum(x_i - \bar{x}) * (y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 * \sum(y_i - \bar{y})^2}}$$

Коэффициент корреляции изменяется от -1 (строгая обратная линейная зависимость) до 1 (строгая прямая пропорциональная зависимость). При значении 0 линейной зависимости между двумя выборками нет.

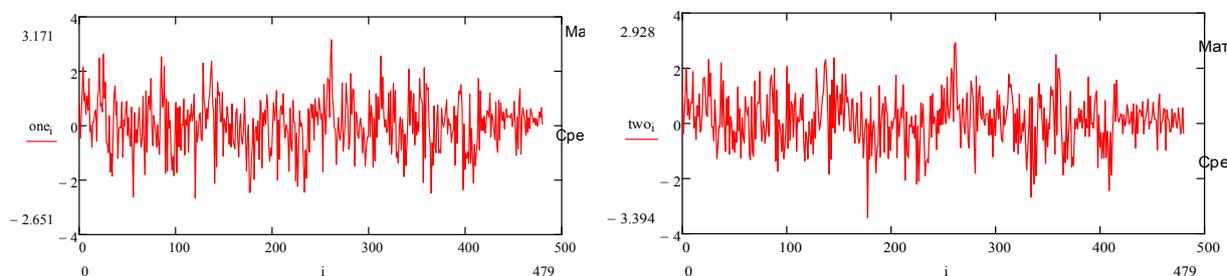


Рис. 1. Пример двух образов «СВОЙ»

На рис. 2 изображен пример распределения двух образов «СВОЙ».

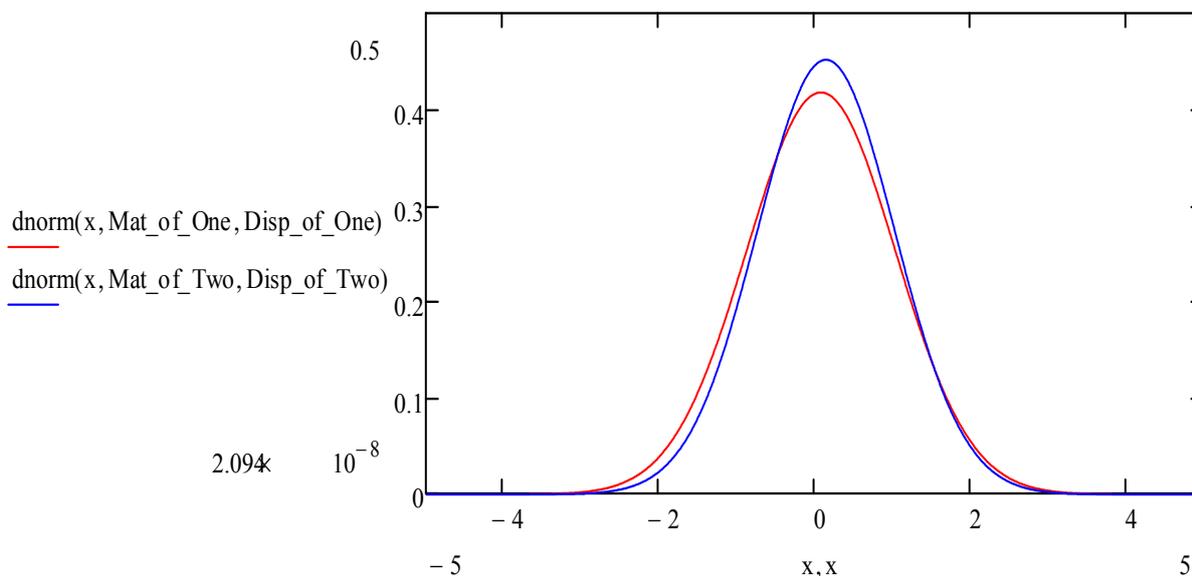


Рис. 2. Пример распределения двух образов «СВОЙ»

На вход подается таблица параметров образов «СВОЙ» размерностью k на 480 , где k – количество своих образов. На выходе получается матрица размерностью 480 на 480 . На рис. 3 представлена блок-схема получения статистических параметров.



Рис. 3. Вычисление статистических параметров

После первого этапа получения статистических параметров были построены и проанализированы графики, изображенные на рис. 4 и 5.

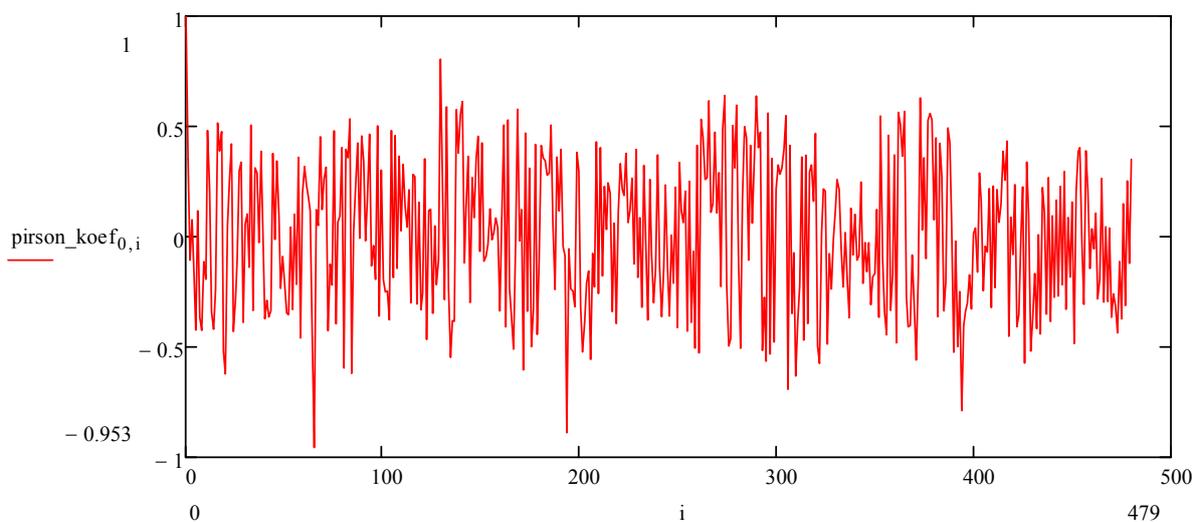


Рис. 4. График корреляционных связей первого параметра

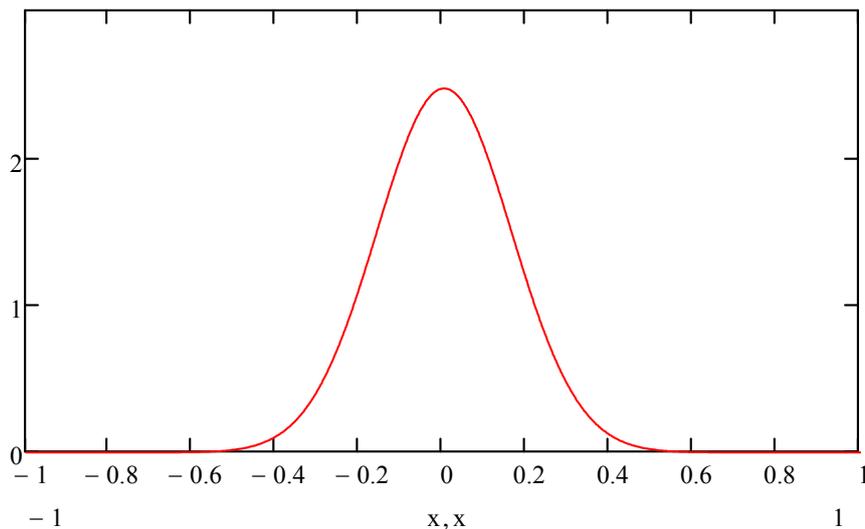


Рис. 5. Распределение корреляционных связей первого параметра

Как видно из рис. 5, вектор имеет нормальное распределение.

Алгоритм синтеза модели тестовых биометрических рукописных образов «Чужие»

После определения вышеописанных параметров совершается реализация самого генератора тестовых биометрических рукописных образов «Чужие».

На рис. 6 изображена блок-схема алгоритма синтеза моделей тестовых образов. Для первоначальной генерации использована стандартная функция системы Mathcad – «gnorm». «gnorm(M, μ, σ)» – вектор M независимых случайных чисел, каждое из которых имеет нормальное распределение:

- μ – математическое ожидание;
- σ – среднеквадратичное отклонение.

Генерация применяется для двух векторов x_0 и z из формулы

$$xx_0^i = \frac{(a * x_0^i + z^i)}{\sqrt{1 + a^2}}.$$

Данная формула в свою очередь служит функцией для подбора коэффициента a . Подбор коэффициента осуществляется итерационно, на каждом шаге вычисляется средний коэффициент корреляции и сравнивается с исходным. При достижении максимально похожего коэффициента корреляции цикл прекращается, вектор xx_0 фиксируется при данном значении коэффициента a .

Нормируются выходные данные (xx_0) относительно дисперсии и математического ожидания образов «СВОЙ». Для нормировки генерируется вектор дисперсий функцией «rchisq» – возвращает вектор случайных чисел, имеющих хи-квадрат распределение. Каждый элемент выборки умножается на соответствующее значение дисперсии и к этому же значению прибавляется математическое ожидание образов «СВОЙ». Нормированные векторы отправляются в файл с расширением «txt».

На каждом этапе реализации алгоритма в системе Mathcad встроены графики, выведенные на экран для зрительного восприятия поведения функций.

При построении модели тестовых образов необходима проверка распределения и гистограмм функций.

Использованы основные функции Mathcad для вывода результатов на экран: «dnorm(x, m, s)» – возвращает плотность вероятности нормального распределения, в котором m и s есть среднее значение и среднеквадратичное отклонение, а s больше 0:

$$\frac{1}{\sqrt{2\pi\sigma}} \exp\left[-\frac{1}{2\sigma^2}(x - \mu)^2\right].$$

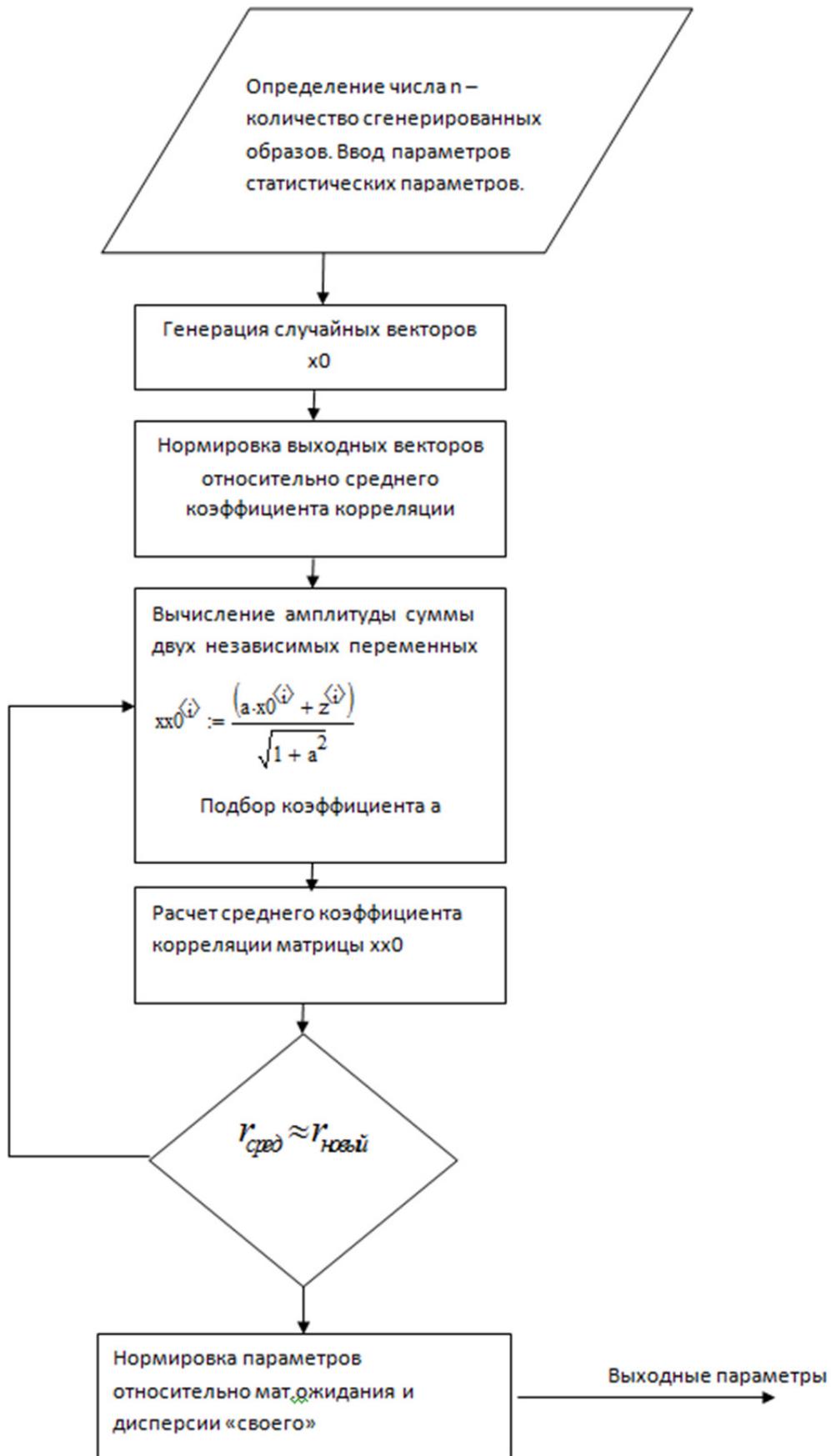


Рис. 6. Синтез модели тестовых рукописных биометрических образов «Чужие»

Сравнение полученных образов «Чужие» с образами «Свои»

В качестве оценки результата работы программы полученные вектора можно посмотреть на графике, оценить их распределение. Так, на рис. 7 представлены два выходных вектора, имеющие амплитудное различие между собой.

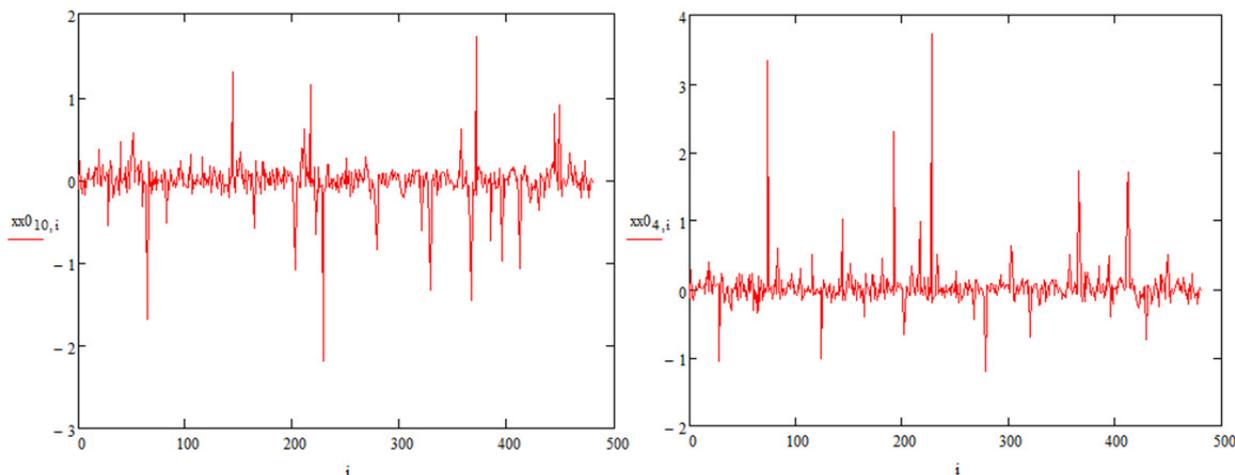


Рис. 7. Вариация из двух выходных векторов

На рис. 8 представлено распределение пяти образов. Из распределения видно, что параметры у векторов имеют существенное различие, тем не менее сохранены статистические параметры образов «СВОЙ». Из этого можно сделать вывод, что получившиеся образы в результате синтеза по своим статистическим свойствам похожи на входные образы «СВОЙ».

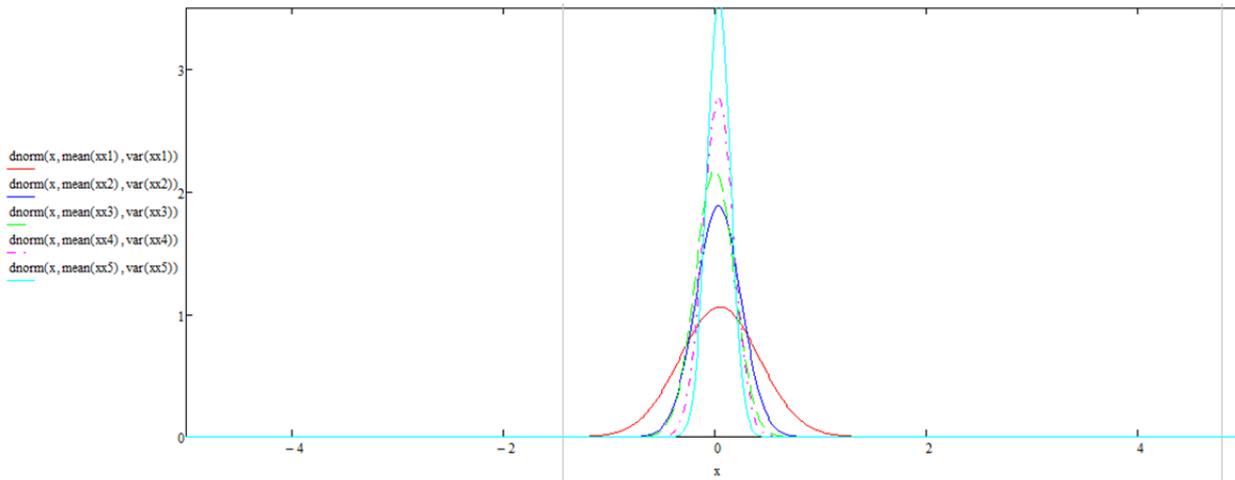


Рис. 8. Распределение пяти входных образов

Анализ и обобщение результатов применения полученных образов при оценке стойкости нейросетевых преобразователей биометрия-код

Полученные образы интегрируются в «.txt» файл, который в дальнейшем может быть использован сотрудниками лаборатории для проведения тестовых испытаний оценки стойкости нейросетевых преобразователей.

Полученный образ интегрируется в систему «БиоНейроАвтограф» для прохода на проверку результата тестирования и подсчета меры Хемминга. Пример тестового испытания представлен на рис. 9.

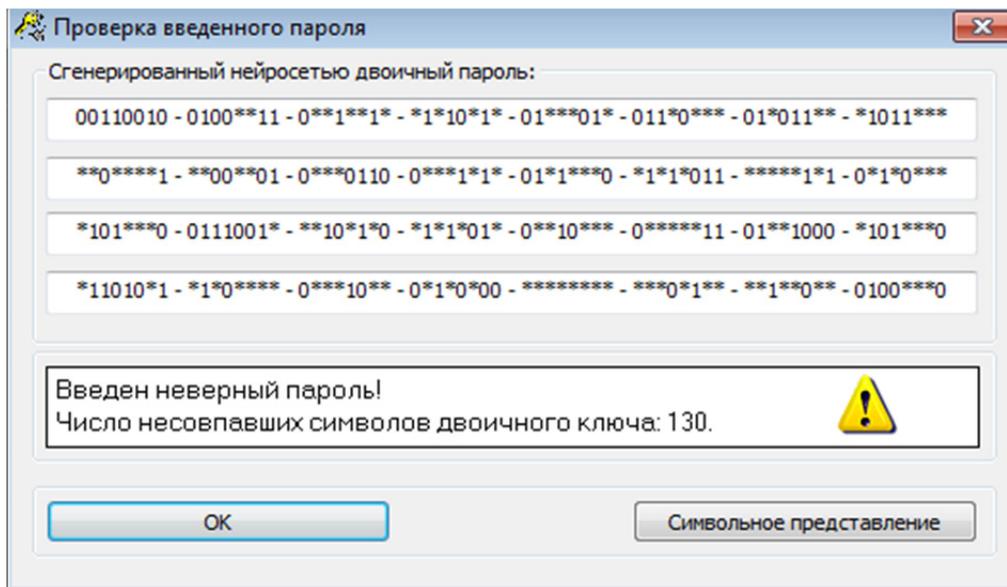


Рис. 9. Пример тестового испытания

Для получения образов в системе Mathcad пользователю достаточно ввести число выходных образов n .

После ввода количества образов необходимо нажать клавиши «ctrl + F9». Спустя определенное количество времени произойдет вывод тестовых образов в файл «Выходные_образы.dat», находящийся в той же папке, где находится сам файл программы. Также в конце файла можно посмотреть распределение получившихся образов.

Заключение

Разработанная модель на основе входных образов синтезирует случайные рукописные биометрические образы, статистические характеристики которых повторяют статистические характеристики входных образов. Синтезируется любое количество образов в зависимости от запроса пользователя.

Произведена проверка получившихся образов, сравнение их с исходными образами. Тестовые биометрические образы в дальнейшем могут быть использованы для оценки стойкости нейросетевых преобразователей биометрия-код.

Библиографический список

1. Руководство по биометрии / Р. М. Болл, Дж. Х. Коннен, Ш. Панканти, Н. К. Ратха, Э. У. Сеньор. – М. : Техносфера, 2007. – 368 с.
2. Глотов, Н. В. Биометрия / Н. В. Глотов, Л. А. Животовский, Н. В. Хованов, Н. Н. Хромов-Борисов. – Л. : ЛГУ, 1982. – 236 с.
3. Лукин, В. С. Обзор основных параметров и методов оценки стойкости нейросетевых биометрических преобразователей / В. С. Лукин, А. К. Гришко, Н. В. Горячев // Современные информационные технологии. – 2015. – Вып. 22. – С. 33–37.
4. Иванов, А. И. Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции : моногр. / А. И. Иванов. – Пенза : Изд-во АО «ПНИЭИ», 2016. – 133 с.
5. Малыгин, А. Ю. Быстрые алгоритмы тестирования нейросетевых механизмов биометрико-криптографической защиты информации / А. Ю. Малыгин, В. И. Волчихин, А. И. Иванов, В. А. Фунтиков. – Пенза : Изд-во ПГУ, 2006. – 161 с.
6. Гришко, А. К. Анализ применения методов и положений теории статистических решений и теории векторного синтеза для задач структурно-параметрической оптимизации / А. К. Гришко // Надежность и качество сложных систем. – 2016. – № 4 (16). – С. 26–34. DOI: 10.21685/2307-4205-2016-4-4.
7. ГОСТ Р 52633.0–2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. – М. : Стандартинформ, 2007. – 19 с.

8. Гришко, А. К. Алгоритм поддержки принятия решений в многокритериальных задачах оптимального выбора / А. К. Гришко // Модели, системы, сети в экономике, технике, природе и обществе. – 2016. – № 1 (17). – С. 242–248.
9. Зудов, А. Б. Интерфейсы на естественном языке как связь нейронных сетей с экспертными системами / А. Б. Зудов, А. К. Гришко // В мире научных открытий. – 2010. – № 5-1. – С. 119–122.
10. Гришко, А. К. Определение показателей надежности структурных элементов сложной системы с учетом отказов и изменения параметров / А. К. Гришко // Измерение. Мониторинг. Управление. Контроль. – 2016. – № 2 (16). – С. 51–57.
11. Гришко, А. К. Оптимальное управление параметрами системы радиоэлектронных средств на основе анализа динамики состояний в условиях конфликта / А. К. Гришко // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2016. – № 2 (38). – С. 102–111. DOI: 10.21685/2072-3059-2016-2-9.
12. Гришко, А. К. Анализ надежности сложной системы на основе динамики вероятности отказов подсистем и девиации параметров / А. К. Гришко // XXI век: итоги прошлого и проблемы настоящего плюс. – 2016. – № 6 (34). – С. 116–121.
13. Лукин, В. С. Помехоустойчивое кодирование информации в системах хранения и восстановления данных / В. С. Лукин, А. П. Иванов, М. В. Бойцова // МАТЕРИАЛЫ И ТЕХНОЛОГИИ 21 ВЕКА : сб. ст. XIII Междунар. науч.-техн. конф. – Пенза : Приволжский дом знаний, 2015. – С. 38–44.
14. Гришко, А. К. Алгоритм оптимального управления в сложных технических системах с учетом ограничений / А. К. Гришко // Модели, системы, сети в экономике, технике, природе и обществе. – 2017. – № 1 (21). – С. 117–123.
15. Grishko, A. Adaptive Control of Functional Elements of Complex Radio Electronic Systems / A. Grishko, N. Goryachev, N. Yurkov // International Journal of Applied Engineering Research. – 2015. – Vol. 10, № 23. – P. 43842–43845.
16. Management of Structural Components Complex Electronic Systems on the Basis of Adaptive Model / A. Grishko, N. Goryachev, I. Kochegarov, S. Brostilov, N. Yurkov // 13th International Conference on Modern Problems of Radio Engineering, Telecommunications, and Computer Science (TCSET). – Lviv-Slavsko, Ukraine. – 2016. – P. 214–218. DOI: 10.1109/TCSET.2016.7452017.
17. Grishko, A. Parameter control of radio-electronic systems based of analysis of information conflict / A. Grishko // 13th International Scientific-Technical Conference on Actual Problems of Electronics Instrument Engineering (APEIE). – Novosibirsk, Russia, 2016. – Vol. 2. – P. 107–111. DOI: 10.1109/APEIE.2016.7806423.

Гришко Алексей Константинович

кандидат технических наук, доцент,
кафедра конструирования
и производства радиоаппаратуры,
Пензенский государственный университет
(440026, Россия, г. Пенза, ул. Красная, 40)
E-mail: alexey-grishko@rambler.ru

Лукин Виталий Сергеевич

аспирант,
Пензенский государственный университет
(440026, Россия, г. Пенза, ул. Красная, 40)
E-mail: Kipra@pnzgu.ru

Юрков Николай Кондратьевич

доктор технических наук, профессор,
заведующий кафедрой конструирования
и производства радиоаппаратуры,
Пензенский государственный университет
(440026, Россия, г. Пенза, ул. Красная, 40)
E-mail: yurkov_NK@mail.ru

Аннотация. Актуальность и цели. Современное общество предполагает активное использование интернет-ресурсов. Существующая практика парольной защиты доступа к личным кабинетам обладает

Grishko Aleksey Konstantinovich

candidate of technical sciences, associate professor,
sub-department of radio equipment design
and production,
Penza State University
(440026, 40 Krasnaya street, Penza, Russia)

Lukin Vitaliy Sergeevich

postgraduate student,
Penza State University
(440026, 40 Krasnaya street, Penza, Russia)

Yurkov Nikolay Kondrat'evich

doctor of technical sciences, professor,
head of sub-department of radio equipment
design and production,
Penza State University
(440026, 40 Krasnaya street, Penza, Russia)

Abstract. Background. Modern society assumes active use of Internet resources. The current practice of password protecting access to personal offices has a significant vulnerability. To strengthen the protection of ac-

существенной уязвимостью. Для усиления защиты доступа к электронным ресурсам госструктур и личным кабинетам пользователей необходимы технологии биометрической аутентификации личности путем преобразования личных биометрических данных человека в его криптографический ключ или длинный пароль доступа. Для реализации поставленной цели используются специальные преобразователи на основе нейронных сетей. В этом случае информационная безопасность напрямую зависит от стойкости нейросетевых преобразователей и генерации для процедуры ее оценки тестовых биометрических образов. Целью является разработка тестовых биометрических рукописных образов для оценки стойкости нейросетевых преобразователей биометрия-код с помощью программы. *Материалы и методы.* В статье использованы методы имитационного моделирования и теория нейронных сетей. Используются среда моделирования Mathcad и среда БиоНейроАвтограф. *Результаты.* Синтезирована модель тестовых биометрических рукописных образов. Произведено сравнение статистических данных полученных образов с исходными. Модель протестирована в среде БиоНейроАвтограф. *Выводы.* С помощью данной модели можно производить оценку стойкости нейросетевых преобразователей биометрия-код. Модель позволяет пользоваться ограниченной исходной информацией и существенно сократить время на создание образов. Это приведет к уменьшению временных, физических и экономических затрат на оценку стойкости нейросетевых преобразователей.

Ключевые слова: нейронная сеть, биометрия, биометрический образ, стойкость, модель.

УДК 004.056; 51-76

Гришко, А. К.

Синтез тестовых образов для оценки стойкости нейросетевых преобразователей в системах биометрической идентификации / А. К. Гришко, В. С. Лукин, Н. К. Юрков // Надежность и качество сложных систем. – 2017. – № 2 (18). – С. 32–40. DOI 10.21685/2307-4205-2017-2-5.

cess to electronic resources of state agencies and offices to personal users the necessary technology for biometric authentication of the individual by the transformation of personal biometric data of a person in his cryptographic key or a long password. To achieve this goal using special converters based on neural networks. In this case, information security depends on the strength of the neural network converters and generating the procedure of its evaluation test of biometric images. The purpose is to develop biometric handwritten test images for evaluating the resistance of neural network converters biometrics code when using the program. *Materials and methods.* The article uses methods of simulation and theory of neural networks. Used simulation environment and the Mathcad environment Bioneurological. *Results.* The synthesized model test biometric handwritten images. A comparison of statistics obtained from the source images. The model is tested in the environment of Bioneurological. *Conclusions.* Using this model it is possible to assess the resistance of neural network converters biometrics code. The model allows to use a limited source of information and significantly reduce the time to create images. This will lead to amnesia temporary, physical and economic costs of the assessment of persistence of neural network converters.

Key words: neural network, biometrics, biometric image, durability, model.