ДИАГНОСТИЧЕСКИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ И КАЧЕСТВА СЛОЖНЫХ СИСТЕМ

DIAGNOSTIC METHODS FOR ENSURING RELIABILITY AND QUALITY OF COMPLEX SYSTEMS

УДК 519.24; 53; 57.017
doi:10.21685/2307-4205-2023-1-11

НЕЙРОСЕТЕВОЕ ПРЕОБРАЗОВАНИЕ БИОМЕТРИИ В КОД АУТЕНТИФИКАЦИИ: ДОПОЛНЕНИЕ ЭНТРОПИИ ХЭММИНГА ЭНТРОПИЕЙ КОРРЕЛЯЦИОННЫХ СВЯЗЕЙ МЕЖДУ РАЗРЯДАМИ

А. И. Иванов[1], А. П. Иванов[2], К. А. Горбунов[3]

[1] Пензенский научно-исследовательский электротехнический институт, Пенза, Россия
[2, 3] Пензенский государственный университет, Пенза, Россия
[1] ivan@pniei.penza.ru, [2] ap_ivanov@pnzgu.ru, [3] kirill.gobunov@mail.ru

Аннотация. *Актуальность и цели.* Рассматривается проблема вычисления энтропии кодов длиной в 256 бит с зависимыми разрядами на малых тестовых выборках, состоящих из 20 примеров. *Материалы и методы.* Предложено оценивать энтропию выходных кодов нейросетевого преобразователя через вычисление взаимных коэффициентов корреляции кодовых последовательностей длиной в 256 бит, полученных для примеров одного образа «Чужой». *Результаты.* Показано, что предложенный метод существенно точнее использовавшегося ранее метода оценки через вычисление математического ожидания и стандартного отклонения расстояний Хэмминга для одного и того же образа «Чужой». *Выводы.* Полученные результаты позволяют ставить вопрос о корректировке в ближайшем будущем национального стандарта ГОСТ Р 52633.3 через введение в него дополнительного раздела, касающегося вычисления корреляционной энтропии.

Ключевые слова: тестирование на малых выборках, искусственные нейроны, преобразование биометрии в код

Для цитирования: Иванов А. И., Иванов А. П., Горбунов К. А. Нейросетевое преобразование биометрии в код аутентификации: дополнение энтропии хэмминга энтропией корреляционных связей между разрядами // Надежность и качество сложных систем. 2023. № 1. С. 91–98. doi:10.21685/2307-4205-2023-1-11

NEURAL NETWORK CONVERSION OF BIOMETRY INTO AUTHENTICATION CODE: ADDITION OF HAMMING ENTROPY WITH ENTROPY OF CORRELATION RELATIONS BETWEEN DISCHARGES

A.I. Ivanov[1], A.P. Ivanov[2], K.A. Gorbunov[3]

[1] Penza Research Institute of Electrical Engineering, Penza, Russia
[2, 3] Penza State University, Penza, Russia
[1] ivan@pniei.penza.ru, [2] ap_ivanov@pnzgu.ru, [3] kirill.gobunov@mail.ru

Abstract. *Background.* The problem of calculating the entropy of 256-bit codes with dependent bits on small test samples consisting of 20 examples is considered. *Materials and methods.* It is proposed to estimate the entropy of the output codes of the neural network transformer by calculating the mutual correlation coefficients of the code se-

quences 256 bits long, obtained for examples of one “Alien” image. *Results.* It is shown that the proposed method is much more accurate than the previously used estimation method by calculating the mathematical expectation and standard deviation of Hamming distances for the same “Alien” image. *Conclusions.* The results obtained make it possible to raise the question of adjusting the national standard GOST R 52633.3 in the near future through the introduction of an additional section into it concerning the calculation of the correlation entropy.

Keywords: small sample testing, artificial neurons, biometrics-to-code conversion

For citation: Ivanov A.I., Ivanov A.P., Gorbunov K.A. Neural network conversion of biometry into authentication code: addition of hamming entropy with entropy of correlation relations between discharges. *Nadezhnost' i kachestvo slozhnykh sistem = Reliability and quality of complex systems.* 2023;(1):91–98. (In Russ.). doi:10.21685/2307-4205-2023-1-11

Введение

При классическом тестировании стойкости биометрической защиты к атакам подбора международный стандарт [1] рекомендует использовать правило 30-кратной избыточности тестовой базы[1]. Наиболее стойким к атакам подбора сегодня считается рисунок радужной оболочки глаза [1, 2]. Будем исходить из того, что тестируемый рисунок радужной оболочки глаза дает вероятность ошибок второго рода $P_2 \approx 10^{-14}$. Тогда 30-кратное увеличение приводит к необходимости использовать тестовую базу размерами $10^{15.5}$ биометрических образов. Создать такую тестовую базу технически невозможно, так как все население Земли составляет не более 8 миллиардов, т.е. сбор радужных оболочек всех людей даст базу в 16 миллиардов, тогда как необходима тестовая база примерно в миллион раз больше.

Выход из создавшегося положения только один, необходимо скрещивать между собой реальные биометрические образы и получать от них синтетические образы-потомки[2]. В этом случае мы можем получить реальный объем в $10^{15.5}$ тестовых образов «Чужой».

Наряду с проблемами синтезирования дополнительных биометрических образов возникает еще одна проблема их последующего хранения. Если предположить, что на хранение одного биометрического шаблона рисунка радужной оболочки глаза требуется 32 Кбайт, то общий объем долговременной памяти может составить 10^{17} Кбайт или 10^{11} Гбайт. Хранение тестовой информации столь значительного объема само по себе является сложной технической задачей.

Еще одной дополнительной проблемой являются законодательные ограничения, введенные большинством стран. Так, в России для сбора и хранения персональных биометрических данных требуется письменное согласие их владельцев, что делает юридически ущербным даже выполнение лабораторных работ по биометрии.

Обойти эту юридическую проблему можно воспользовавшись средой моделирования «БиоНейроАвтограф» [3, 4]. Эта среда моделирования позволяет преобразовывать динамику рукописных образов человека в 416 биометрических параметров. Далее эти данные используются для обучения нейросети алгоритмом ГОСТ Р 52633.5 в код ключа аутентификации длиной 256 бит[3]. Примеры экранных форм среды моделирования приведены на рис. 1.

Законодательные ограничения снимаются тем, что студент работает только со своими биометрическими данными. После выполнения лабораторных работ он может удалить свои персональные биометрические параметры. Нет необходимости при тестировании формировать и хранить большие тестовые базы биометрических образов «Чужой».

Заметим также, что алгоритм обучения ГОСТ Р 52633.5 обеспечивает равновероятные значения состояний «0» и состояний «1» в каждом из 256 разрядов выходного кода, если на входы, обученной нейросети подавать примеры случайных образов «Чужой»[3]. Если мы попытаемся оценить полную энтропию кодов в первом приближении, вычислив энтропию каждого разряда и сложив частные энтропии разрядов, то получим предельное значение оценки энтропии в 256 бит. Такая предельная энтропия соответствует вероятности угадывания ключа с первой попытки на уровне

[1] ГОСТ Р ИСО/МЭК 19795-1–2007. Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура.

[2] ГОСТ Р 52633.2–2010. Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации.

[3] ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа.

$P_2 \approx 10^{-85.3} \approx 2^{-256}$. Столь малые величины не сопоставимо меньше реальных оценок и являются следствием пренебрежения значительными корреляционными связями между разрядами исследуемых кодов.

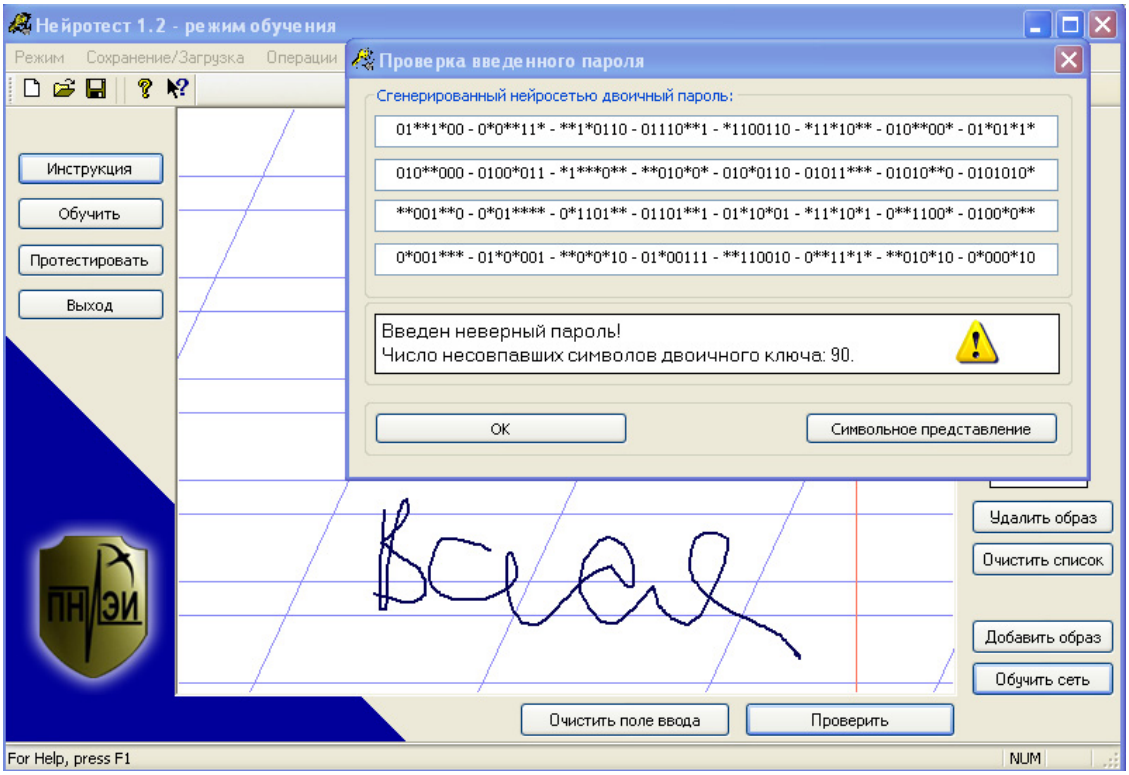

Рис. 1. Режим «Проверить» рукописное слово «*Вася*» нейросетью, обученной распознавать слово «*Пенза*» (неправильные биты ключа помечены звездочками)

Экономия памяти и сокращение времени при тестировании обученной нейросети на малых выборках в пространстве расстояний Хэмминга

Для того, чтобы оценить реальное число выходных классов нашей нейросетевой конструкции, следует воспользоваться рекомендациями ГОСТ Р 52633.3 и перейти от анализа статистик появления обычных кодов к анализу статистик расстояний Хэмминга между кодами[1]:

$$"h" = \sum_{i=1}^{256} ("c_i") \oplus ("x_i"), \qquad (1)$$

где $"c_i"$ – состояние i-го разряда кода «Свой»; $"x_i"$ – состояние i-го разряда кода «Чужой»; $\oplus$ – операция сложения по модулю два.

В случае, если мы используем достаточно большое число случайных рукописных образов «Чужой», то мы получим дискретное распределение расстояний Хэмминга с практически нормальным распределением. Распределение расстояний Хэмминга стремится к нормальному из-за того, что 256-кратное суммирование случайных состояний (1) является хорошим нормализатором по «*центральной предельной теореме статистики*».

Пользуясь гипотезой нормальности, мы можем по математическому ожиданию и стандартному отклонению оценить вероятность, когда код «Чужой» даст полное совпадение с кодом «Свой». В рассматриваемом приложении есть специальный режим «Операции» → «Тестирование на тестовых образах» → «Открыть». В этом случае появляется форма отчета о вычислениях, приведенная на рис. 2.

[1] ГОСТ Р 52633.3–2011. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора.

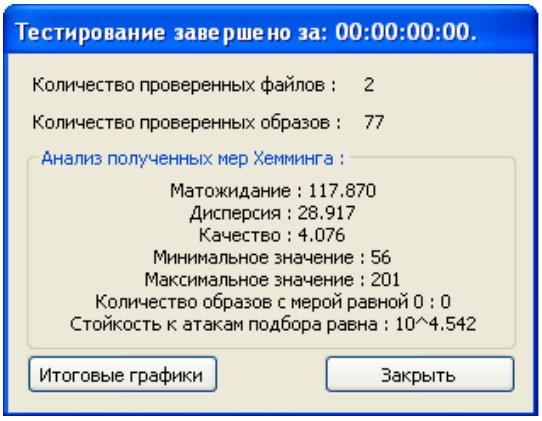

Рис. 2. Экранная форма статистик нейросетевого классификатора, отображающая результат вычислений по 77 тестовым образам «Чужой», $10^{4.542}$ – попытка атаки случайной подстановки может привести к удаче

Последнее означает, что исследуемая нейросеть «*Пенза*» способна различать между собой примерно $10^{4.54} \approx 2^{15}$ классов рукописных образов. Для этого числа классов достаточно коротких кодов длиной в 15 бит. Реально наблюдаемый 256-битный выходной код нейросети избыточен. Его 17-кратная избыточность может быть использована для корректировки случайно возникающих редких ошибок в коде в «Свой» [5].

В первом приближении можно считать, что энтропия выходных кодов нейросети должна составлять примерно 15 бит вместо 256 «видимых» бит. Еще одним важным моментом является то, что энтропия каждого образа «Чужой» будет разной. Эта ситуация отображена на рис. 3.

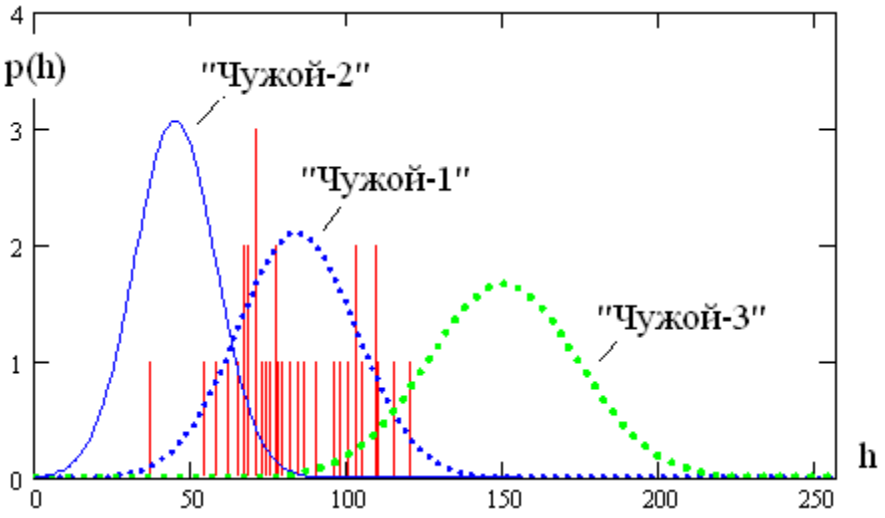

Рис. 3. Эффект взаимной сортировки биометрических образов в пространстве расстояний Хэмминга

Чем дальше математическое ожидание расстояний Хэмминга от точки $h = 0.0$ и чем меньше стандартное отклонение $\sigma(h)$, тем выше энтропия кодов исследуемого биометрического образа «Чужой». В связи с этим, рассчитав энтропию для группы образов «Чужой», мы легко можем их взаимно упорядочить.

В рамках гипотезы нормального распределения расстояний Хэмминга энтропия образов «Чужой» вычисляется по следующей формуле:

$$\begin{cases} P_2(h) = \dfrac{1}{\sigma(h)\sqrt{2\pi}} \int\limits_{-\infty}^{1} \exp\left\{ \dfrac{-\left(u - E(h)\right)^2}{2\left(\sigma(h)\right)^2} \right\} du; \\ H(\text{"}x_1, x_2, ..., x_{256}\text{"}) \approx -\log_2\left(P_2(h)\right). \end{cases} \quad (2)$$

Для нас принципиально важным является то, что вычисление энтропии длинных кодов по Шеннону является задачей экспоненциальной вычислительной сложности [6]. Энтропия, оцениваe-

мая в пространстве расстояний Хэмминга (2) является задачей с линейной вычислительной сложностью. При переходе от обычного наблюдения длинных кодов в пространство расстояний Хэмминга наблюдается гигантское ускорение вычислений энтропии.

Если бы мы решили оставаться в рамках классической статистики, то для корректного вычисления вероятности ошибок второго рода P_2 (ошибочного признания образа «Чужой» как образ «Свой») нам пришлось бы использовать примерно 100 000 примеров образов «Чужой». Если же мы перейдем в пространство расстояний Хэмминга (1), то для вычисления математического ожидания $E(h)$ и стандартного отклонения $\sigma(h)$ достаточно 20 случайно выбранных примеров образов «Чужой». Мы наблюдаем эффект сокращения требуемого объема памяти примерно в 5000 раз и во столько же раз ускорение вычислений.

Экономия памяти и сокращение времени при тестировании обученной нейросети на малых выборках в пространстве корреляционной сцепленности разрядов длинных кодов

В среде моделирования «БиоНейроАвтограф» предусмотрен файл «testKeys.txt», где записываются двоичные ключи, полученные на 256 выходах нейросети при ее тестировании. На рис. 4 приведены два ключа-отклика нейросети «*Пенза*», полученные при предъявлении двух примеров одного образа «*Хопер*».

```
Двоичный ключ:
0101100001111010011001111101001101011010011010110010001001011100011101111010111001
1110010000101001111010011100001001010011010001101011001011001001111111000000011001
0100100101011001001010011100100101100101010011001100100000110111010010100011101 0
0110101001010

Двоичный ключ:
1001100011111011001000101110101011101001011110100100101000110011110101011110011111110
0101111000100111100100011010010111111111011000101011001011010111101110000011001
0000100010011010001011011111010010110000111111110100010001000011110110110100011001
1110111000101
```

Рис. 4. Два ключа длинной 256 бит, полученные как отклики нейросети на два примера одного образа «*Хопер*»

Из рис. 4 видно, что первая и вторая битовые последовательности содержат много общего, но они же имеют и существенные расхождения [7, 8]. Это означает, что корреляционная сцепленность этих выходных последовательностей может быть оценена прямым вычислением коэффициентов корреляции между ними, т.е. если обозначить бинарные последовательности файла «testKeys.txt» как $\{x1, x2, \ldots, x21\}$, то мы можем вычислить нужные нам коэффициенты корреляции и корреляционную матрицу в целом:

$$\begin{bmatrix} 1 & r(x1,x2) & :::::::::: & r(x1,x21) \\ r(x1,x2) & 1 & r(x2,x3) & :::::::::::::: \\ :::::::::::::: & :::::::::::::: & :::::::::: & :::::::::::::: \\ r(x1,x21) & r(x2,x21) & :::::::::: & 1 \end{bmatrix}, \tag{3}$$

где

$$r("xk","xj") = \frac{1}{256}\sum_{i=1}^{256}\frac{(E("xk_i")-"xk_i")(E("xj_i")-"xj_i")}{\sigma("xk_i")\cdot\sigma("xj_i")}. \tag{4}$$

Для того, чтобы далее вычислить коэффициент эквивалентной симметричной матрицы $\tilde{r}$, следует усреднить модули всех коэффициентов корреляции матрицы (3), находящихся вне ее диагонали, и оценить их стандартное отклонение [9].

Если мы имеем дело с 20 примерами образа «*Хопер*» и образа «*Сура*», то сможем получить матрицы коэффициентов корреляции 20×20, которые будут иметь 180 разных коэффициентов корреляции. На рис. 5 даны распределения значений коэффициентов корреляции, рассматриваемых образов, построенные в рамках гипотезы нормальности их распределений.

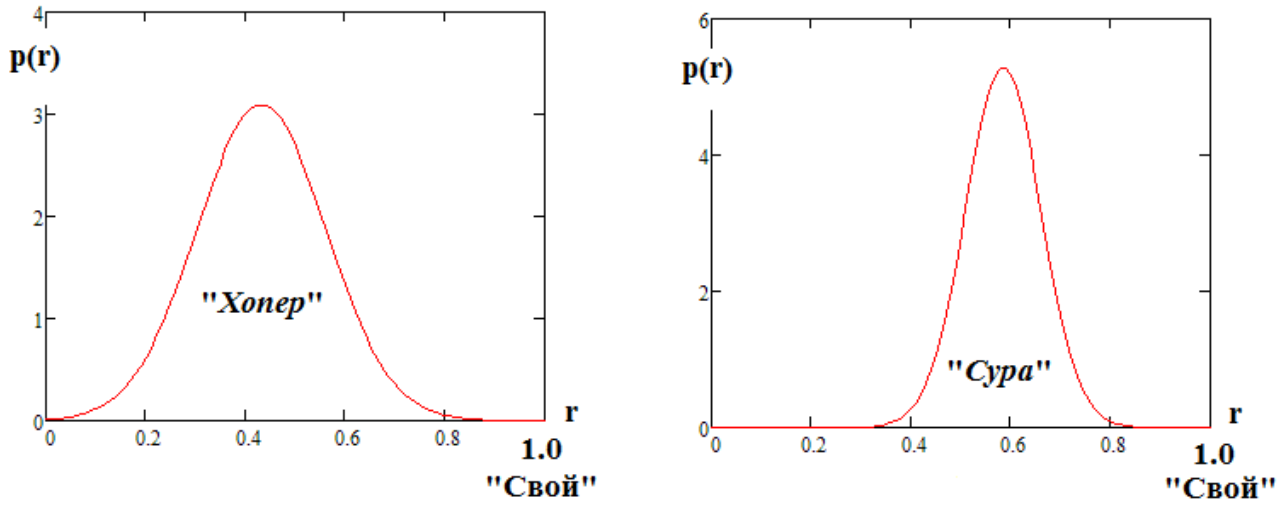

Рис. 5. Распределение расстояний корреляционной сцепленности между ключами от примеров образа Хопер и ключами от образа Сура (предельное значение корреляции «Свой» в правой части рисунка r = 1,0)

Как итог, мы можем в дополнение к энтропии Хэмминга (2) построить аналогичную по содержанию энтропию корреляционной сцепленности разрядов длинного кода:

$$\begin{cases} P_2(r) = \dfrac{1}{\sigma(r)\sqrt{2\pi}} \int\limits_{0.99}^{\infty} \exp\left\{ \dfrac{-\left(u - E(r)\right)^2}{2\left(\sigma(r)\right)^2} \right\} du; \\ H("x_1, x_2, ..., x_{256}") \approx -\log_2\left(P_2(r)\right). \end{cases} \tag{5}$$

Отметим, что и в случае вычисления энтропии корреляционной сцепленности по сравнению с вычислением энтропии Шеннона мы получаем выигрыш по экономии памяти, что составляет примерно 5000 раз, а выигрыш по ускорению вычисления оказывается примерно 300 раз. Это примерно такой же показатель, что и для вычислений энтропии в пространстве расстояний Хэмминга, однако выражения (1) и (2) существенно отличаются от выражения (5) по вычислительным затратам. Главное же состоит в том, что для вычисления энтропии корреляционной сцепленности (5) не нужна информация о значении разрядов кода «Свой», как этого требует ГОСТ Р 52633.3[1]. Это открывает возможность вычисления энтропии любой, неизвестно чему обученной нейросети.

Повышение точности вычислений энтропии за счет учета большего числа моментов на малых выборках

Еще одной важной особенностью нового алгоритма вычисления энтропии (5) является снижение ошибок оценки энтропии, обусловленных малым объемом тестовых выборок. В частности, при вычислении математического ожидания и стандартного отклонения для энтропии Хэмминга должны использоваться следующие выражения:

$$\begin{cases} E(h) \approx \sum\limits_{i=1}^{20} \dfrac{h_i}{20}; \\ \sigma(h) \approx \sqrt{\sum\limits_{i=1}^{20} \dfrac{\left(E(h) - h_i\right)^2}{20}}. \end{cases} \tag{6}$$

Очевидно, что усреднение по 20 примерам будет давать значительные ошибки ΔE и $\Delta\sigma$. Ситуация меняется, когда мы переходим к реализации второго вычислительного алгоритма. В этом случае мы должны вычислять среднее и стандартное отклонение по значительно большему числу примеров коэффициентов корреляции:

[1] ГОСТ Р 52633.3–2011. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора.

$$\begin{cases} E(|r|) \approx \sum_{i=1}^{180} \frac{|r_i|}{180}; \\ \sigma(r) \approx \sqrt{\sum_{i=1}^{180} \frac{(E(|r|) - |r_i|)^2}{180}}. \end{cases} \quad (7)$$

При прочих равных условиях ошибка вычисления математического ожидания в выражении (6) должна быть выше, чем в выражении (7). То же самое относится и к стандартным отклонениям. Все это является прямым следствием роста выборки с 20 до 180 примеров.

Даже в том случае, если ошибки вычисления оказываются сопоставимыми $\Delta E(h) \approx \Delta E(r)$ и $\Delta\sigma(h) \approx \Delta\sigma(r)$, итоговый результат вычислений по формулам (2) и (5) оказывается слабо коррелированным. Это означает, что их усреднение должно приводить к снижению итоговой ошибки оценки энтропии в корень из двух раз (примерно на 41,4 %).

Заключение

Передовой национальный стандарт по тестированию ГОСТ Р 52633.3-2011 нейросетевых преобразователей биометрия-код на малых выборках коренным образом изменил ситуацию по росту доверия к процедурам биометрико-криптографической аутентификации. Появилась возможность быстро тестировать нейросетевой преобразователь после каждого его обучения. При этом тестирование оказывается технически реализуемо, даже при использовании в качестве доверенной вычислительной среды мало потребляющих процессоров SIM-карт и микро-SD-карт [14, 15].

Приведенные в данной статье данные позволяют утверждать, что точность оценок энтропии выходных кодов нейросетей может быть существенно увеличена, если вычисление энтропии Хэмминга дополнить вычислением еще и корреляционной энтропии. Это ставит в повестку дня вопрос о разработке новой версии национального стандарта ГОСТ Р 52633.3 взамен действующей. В новую версию наряду с вычислением энтропии Хэмминга должен войти раздел, касающийся вычисления корреляционной энтропии.

Список литературы

1. Болл Р. М., Коннел Дж. Х., Панканти Ш. [и др.]. Руководство по биометрии. М. : Техносфера, 2007. 367 с.
2. Hao F., Anderson R., Daugman J. Crypto with Biometrics Effectively // IEEE Transactions on Computers. 2006. Vol. 55, № 9.
3. Иванов А. И., Захаров О. С. Среда моделирования «БиоНейроАвтограф». 2009. URL: http://пниэи.рф/activity/science/noc/bioneuroautograph.zip (дата обращения: 10.12.2022).
4. Иванов А. И. Автоматическое обучение больших искусственных нейронных сетей в биометрических приложениях : учеб. пособие. Пенза, 2013. 30 с. URL: http://пниэи.рф/activity/science/noc/tm_IvanovAI.pdf (дата обращения: 10.12.2022).
5. Безяев А. В. Биометрико-нейросетевая аутентификация: обнаружение и исправление ошибок в длинных кодах без накладных расходов на избыточность : препринт. Пенза : Изд-во ПГУ, 2020. 40 с.
6. Иванов А. И. Искусственный интеллект высокого доверия. Ускорение вычислений и экономия памяти при тестировании больших сетей искусственных нейронов на малых выборках // Системы безопасности. 2020. № 5. С. 60–62.
7. Иванов А. И., Иванов А. П., Ратников К. А. Статистико-нейросетевой анализ биометрических образов в пространствах спектров кроссверток и автосверток Хэмминга : препринт. Пенза : Изд-во ПГУ, 2021. 56 с.
8. Горбунов К. А., Никитин В. В. Нейросетевая биометрия: подтверждение гипотезы обратных шкал для метрики корреляционной сцепленности и метрики расстояний Хэмминга при их применении к ключам-откликам на примеры одного образа «Чужой» // Безопасность информационных технологий : сб. науч. ст. по материалам III Всерос. науч.-техн. конф. : в 2 т. Пенза : Изд-во ПГУ, 2021. Т. 1. С. 83–85.
9. Иванов А. И., Банных А. Г., Серикова Ю. И. Учет влияния корреляционных связей через их усреднение по модулю при нейросетевом обобщении статистических критериев для малых выборок // Надежность. 2020. № 20. С. 28–34. doi:10.21683/1729-2646-2020-20-2-28-34

References

1. Boll R.M., Konnel Dzh.Kh., Pankanti Sh. et al. *Rukovodstvo po biometrii = Guide to biometrics*. Moscow: Tekhnosfera, 2007:367. (In Russ.)
2. Hao F., Anderson R., Daugman J. Crypto with Biometrics Effectively. *IEEE Transactions on Computers*. 2006;55(9).

3. Ivanov A.I., Zakharov O.S. *Sreda modelirovaniya «BioNeyroAvtograf» = Modeling environment "Bioneiroautograph"*. 2009. (In Russ.). Available at: http://pniei.rf/activity/science/noc/bioneuroautograph.zip (accessed 10.12.2022).
4. Ivanov A.I. *Avtomaticheskoe obuchenie bol'shikh iskusstvennykh neyronnykh setey v biometricheskikh prilozheniyakh: ucheb. posobie = Automatic training of large artificial neural networks in biometric applications : textbook*. Penza, 2013:30. (In Russ.). Available at: http://pniei.rf/activity/science/noc/tm_IvanovAI.pdf (accessed 10.12.2022).
5. Bezyaev A.V. *Biometriko-neyrosetevaya autentifikatsiya: obnaruzhenie i ispravlenie oshibok v dlinnykh kodakh bez nakladnykh raskhodov na izbytochnost': preprint = Biometric-neural network authentication: detection and correction of errors in long codes without redundancy overhead : preprint*. Penza: Izd-vo PGU, 2020:40. (In Russ.)
6. Ivanov A.I. Artificial intelligence of high trust. Acceleration of calculations and memory savings when testing large networks of artificial neurons on small samples. *Sistemy bezopasnosti = Security systems*. 2020;(5):60–62. (In Russ.)
7. Ivanov A.I., Ivanov A.P., Ratnikov K.A. *Statistiko-neyrosetevoy analiz biometricheskikh obrazov v prostranstvakh spektrov krossvertok i avtosvertok Khemminga: preprint = Statistical and neural network analysis of biometric images in the spaces of the spectra of Hamming cross-convolutions and auto-convolutions : preprint*. Penza: Izd-vo PGU, 2021:56. (In Russ.)
8. Gorbunov K.A., Nikitin V.V. Neural network biometrics: confirmation of the hypothesis of inverse scales for the metric of correlation coupling and the metric of Hamming distances when they are applied to key responses to examples of one image of a "Stranger". *Bezopasnost' informatsionnykh tekhnologiy: sb. nauch. st. po materialam III Vseros. nauch.-tekhn. konf.: v 2 t. = Information technology security: collection of scientific articles based on the materials of the III All-Russian scientific-technical. conf.: in 2 vol*. Penza: Izd-vo PGU, 2021;1:83–85. (In Russ.)
9. Ivanov A.I., Bannykh A.G., Serikova Yu.I. Accounting for the influence of correlations through their modulus averaging in neural network generalization of statistical criteria for small samples. *Nadezhnost' = Reliability*. 2020;(20):28–34. (In Russ.). doi:10.21683/1729-2646-2020-20-2-28-34

Информация об авторах / Information about the authors

Александр Иванович Иванов
доктор технических наук, доцент,
ведущий научный сотрудник,
Пензенский научно-исследовательский
электротехнический институт
(Россия, г. Пенза, ул. Советская, 9)
E-mail: ivan@pniei.penza.ru

Aleksandr I. Ivanov
Doctor of technical sciences, associate professor,
leading researcher,
Penza Research Electrotechnical Institute
(9 Sovetskaya street, Penza, Russia)

Алексей Петрович Иванов
кандидат технических наук, доцент,
заведующий кафедрой технических средств
информационной безопасности,
Пензенский государственный университет
(Россия, г. Пенза, ул. Красная, 40)
E-mail: ap_ivanov@pnzgu.ru

Aleksey P. Ivanov
Candidate of technical sciences, associate professor,
head of the sub-department of technical means
of information security,
Penza State University
(40 Krasnaya street, Penza, Russia)

Кирилл Александрович Горбунов
аспирант,
Пензенский государственный университет
(Россия, г. Пенза, ул. Красная, 40)
E-mail: kirill.gobunov@gmail.com

Kirill A. Gorbunov
Postgraduate student,
Penza State University
(40 Krasnaya street, Penza, Russia)

Авторы заявляют об отсутствии конфликта интересов /
The authors declare no conflicts of interests.

Поступила в редакцию/Received 15.12.2022
Поступила после рецензирования/Revised 15.01.2023
Принята к публикации/Accepted 10.13.2023