УДК: 612.087.1+004.032.26+347.2:004.056.5:612.087.1

Безяев А. В., Иванов А. И., Фунтикова Ю. В.

ОПТИМИЗАЦИЯ СТРУКТУРЫ САМОКОРРЕКТИРУЮЩЕГОСЯ БИО-КОДА, ХРАНЯЩЕГО СИНДРОМЫ ОШИБОК В ВИДЕ ФРАГМЕНТОВ ХЕШ-ФУНКЦИЙ

Анализируются «нечеткие экстракторы» и нейросетевые преобразователи биометрия-код. Показано, что применение в них классических избыточных кодов с обнаружением и исправлением ошибок нерационально. Предложено использовать коды, хранящие синдромы ошибок в виде фрагментов хеш-функций. Это позволяет исключить нерациональное расходование бит био-кода на заполнение избыточных фрагментов классических самокорректирующихся кодов. Даны процедуры выравнивания распределения ошибок между блоками био-кода. Показано, что распределение расстояний Хемминга между кодами «Свой» хорошо описывается распределением Пирсона, адаптированным под сильно коррелированные биометрические данные.

Ключевые слова: *коды с обнаружением и исправлением ошибок, устранение избыточности, «нечеткие экстракторы», нейросетевые преобразователи биометрия-код, распределение Пирсона для зависимых данных.*

Bezev A. V., Ivanov A. I., Funtikova U. V.

OPTIMIZATION OF THE STRUCTURE SELF-CORRECTING BIO-CODE, STORING SYNDROMES ERROR AS FRAGMENTS HASH-FUNCTIONS

Analyzed «fuzzy extractors» and neural network converters biometrics code. It is shown that the use of them in classical redundant codes with error detection and correction irrationally.

Proposed to use a code storing error syndromes as fragments of hash functions. This eliminates waste of bio-bit code to fill excess fragments of classical self-correcting codes. Given alignment procedure error distribution between the blocks bio-code. It is shown that the distribution of the Hamming distance between the codes «their» well describes the distribution of Pearson, adapt strongly correlated biometric data.

Keywords: *codes with error detection and correction, eliminating redundancy, «fuzzy extractors» neural network converters biometrics code Pearson distribution for dependent data.*

1. Введение

В настоящее время во всем мире идут процессы создания средств биометрической защиты прав личности. Россия и Казахстан идут по пути использования больших искусственных нейронных сетей [1, 2, 3] и создания под эту технологию пакета стандартов серии ГОСТ Р 52633.xx-20xx. Англоязычные исследователи [4, 5, 6, 7] идут по пути применения так называемых «нечетких экстракторов», являющихся частным случаем нейросетевых преобразователей. Различие между «нечеткими экстракторами» и нейросетевыми преобразователями обусловлено их структурами, приведенными на рис. 1. Квантователь «нечеткого экстрактора» имеет вырожденный входной сумматор с одним входом, полноценные нейросетевые преобразователи оказываются намного сложнее «нечетких экстракторов», так как каждый искусственный нейрон имеет полноценный входной сумматор, осуществляющий обогащение континуальных входных данных.

Из рис. 1 видно, что «нечеткие экстракторы» квантуют «сырые» биометрические данные, получают длинный био-код, содержащий от 30% до 50% ошибок, далее преобразуют этот нестабильный код каким-либо клас-

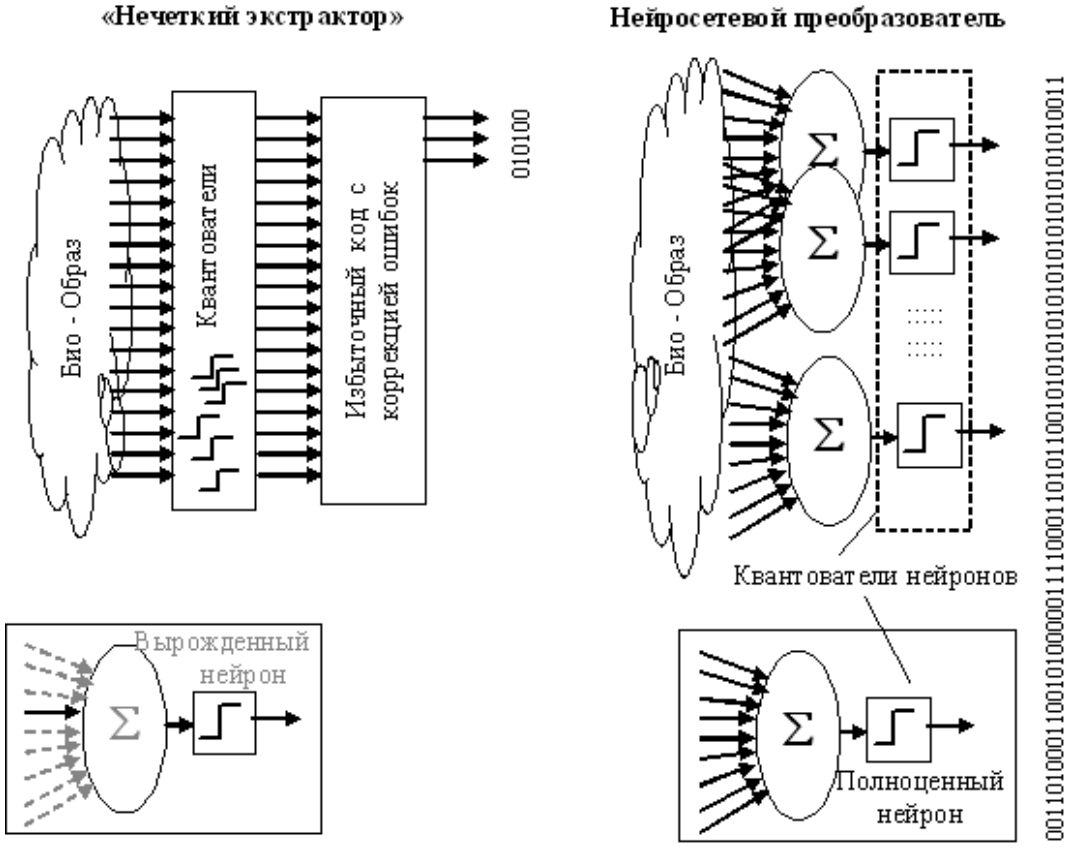

Рис. 1. Структурные схемы нечетких экстракторов и нейросетевых преобразователей

сическим самокорректирующимся кодом с избыточностью. Самокорректирующийся классический код пытается исправлять возникающие в био-коде ошибки.

Иную структуру имеют нейросетевые преобразователи биометрия-код. Этот тип преобразователей перед квантованием данных осуществляет их обогащение. Каждый нейрон преобразователя заранее обучается обогащать «сырые» биометрические данные путем подбора весовых коэффициентов сумматоров. А уже обогащенные биометрические данные на выходах сумматоров квантуются, преобразуясь в выходной био-код искусственной нейронной сети. Фактически во время обучения нейросетевой преобразователь биометрия-код учитывает реальную неравномерность расположения слабых и сильных бит био-кода.

Практика показывает, что «нечеткие экстракторы» всегда работают хуже, чем нейросетевые преобразователи биометрия-код. Подтверждением этого служит ситуация, когда квантование «сырых» био-данных дает код с 30% ошибок. Ни один из классических самокорректирующихся кодов не способен править столь значительное число ошибок. Для того чтобы самокорректирующиеся коды заработали, приходится маскировать (выбрасывать) порядка 30% наиболее нестабильных разрядов био-кода. При этом оставшиеся 70% наиболее стабильных разрядов будут иметь примерно 10% ошибок, что уже можно поправить самокорректирующимся кодом с избыточностью порядка 800%. Если био-код длинный (например, Даугман [7] преобразует радужную оболочку глаза в 2048-битный код), то «нечеткие экстракторы» работают. В этом случае даже после маскирования нестабильных разрядов и изъятия «сырых» разрядов био-кода на заполнение многократно избыточной части кода остается достаточно длинный фрагмент полезной информативной части био-кода. У Даугмана [7] полезный остаток био-кода составляет 128 бит, что эквивалентно применению им самокорректирующегося кода с избыточностью в 1500% (15-кратная избыточность).

Если био-код изначально короткий (технология дает мало контролируемых биометрических параметров), то применять «нечеткие экстракторы» нет смысла. В частности, при преобразовании рисунков отпечатка пальца [6], имеющих от 20 до 40 особых точек, положение которых описывается двумя координатами, длина био-кода составляет от 40 до 80 бит. При 15-кратной избыточности кода (как у Даугмана [7]) его полезная (информативная часть) составит от 2 до 4 бит. При столь коротком коде говорить о сколько-нибудь серьезной криптографической защите биометрических данных не приходится. Подбор био-кода Даугмана [7], состоящего из 128 бит при правильной схеме выполненных защищающих преобразований, можно рассматривать как некоторый барьер, так как перебрать столь значительное число состояний разрядов био-кода трудно. Корректировка коротких био-кодов классическими кодами с обнаружением и исправлением ошибок не может рассматриваться как способ защиты их из-за крайне малых затрат вычислительных ресурсов на перебор.

Заметим, что причина плохой работы классических кодов с обнаружением и исправлением ошибок состоит в том, что они обладают крайне высокой избыточностью. Для коротких кодов практически вся биометрическая информация уходит на заполнение избыточной части кода. Этот коренной недостаток может быть устранен, если отказаться от классических самокорректирующихся кодов и перейти к использованию кодов с нулевой избыточностью [8].

2. Самокорректирующиеся био-коды, не обладающие избыточностью

Идея создания таких кодов состоит в отказе от траты части разрядов био-кода на заполнение избыточной части. В качестве информации эквивалентной избыточности используются три последних разряда хеш-функции био-кода $(\mathrm{hash}(\text{“}\bar{c}_{[1...512]}\text{”})_{[126,127,128]})$. Например, если мы используем стандартную хеш-функцию MD5, которая дает случайное число длиной 128 бит, то три ее последних разряда могут использоваться для корректировки от одной до четырех ошибок био-кода $\bar{c}$. Попытки корректировать большее число разрядов кода возможны, но связаны с ростом затрат времени на перебор.

Стандартные хэш-функции оптимизированы по времени вычисления, и современные вычислительные машины для био-кода длиной в 512 бит перебирают возможные положения до 4 ошибок за приемлемое время от 0,01 до 0,8 секунды без применения аппаратных ускорителей.

Если требуется корректировать до 8 ошибок, то нужно разбить био-код на 2 фрагмента

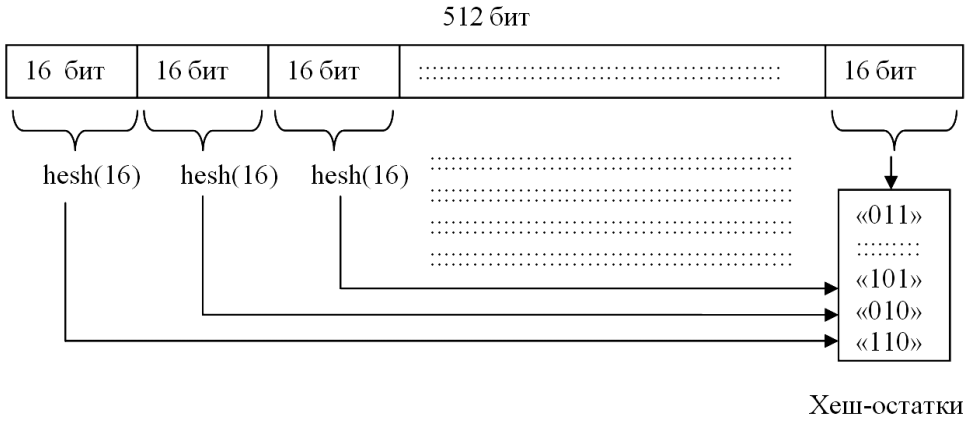

Рис. 2. Опасная схема структурной организации самокорректирующихся хеш-кодов

по 128 бит, вычислить от них хэш-функцию MD5 и хранить два трехбитных хеш-остатка. Среднее время корректировки данных таким кодом удваивается. Если дробить био-код на большее число фрагментов (4, 8, 16, 32), то такой код будет способен корректировать до 16, 32, 64, 128 ошибочных разрядов 512-битного био-кода без катастрофически больших затрат на формирование избыточности. То есть, мы оказываемся способны корректировать до 25% ошибок в био-коде, компрометируя не более 12, 24, 48, 96 его разрядов в виде хранящихся открыто хеш-остатков. Получается, что мы можем относительно безопасно корректировать рекордно большое число в 50% ошибок био-кода, сохраняя его первоначальную длину в 512 бит.

Как показали предварительные оценки, защитные свойства хеш-кодов зависят от схемы организации сбора хеш-остатков. Попытки увеличения исправляющей способности хеш-кода приводят к росту числа фрагментов, на которые разбивается код, и к уменьшению их длины. Чем больше коротких фрагментов хешитуется, тем серьезнее необходимо подходить к выбору схемы формирования хеш-остатков. Простейшая схема дробления кода на фрагменты по 16 бит с независимым хешированием каждого из этих фрагментов (схема преобразований приведена на рис. 2) является самой опасной.

Высокий уровень опасности схемы формирования хеш-остатков (рис. 2) обусловлен тем, что число неопределенных состояний линейно связано с числом 16-битных фрагментов:

$$N \approx k \cdot 2^{(16-3)}. \qquad (1).$$

Злоумышленник, пытающийся воспользоваться k трехразрядными остатками, при извлечении знаний о био-коде сталкивается с инженерной задачей полиномиальной вычислительной сложности. Для того чтобы положение изменилось и защита данных усилилась, необходимо использовать схему формирования хеш-остатков, приведенную на рис. 3.

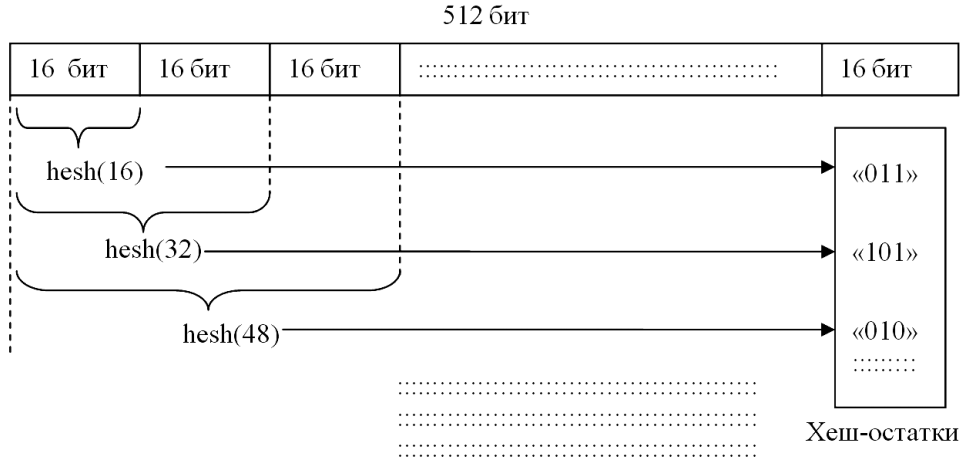

Рис. 3. Безопасная схема рекурсивного формирования эталонных хеш-остатков

На первом шаге обработки данных вычисляется хеш-функция от первых 16 разрядов био-кода. На втором шаге вычисляется хеш-функция от первых 32 разрядов биокода. На каждом следующем шаге длина хешируемого фрагмента био-кода увеличивается на 16 бит. На последнем k-том шаге хешируется весь био-код. При такой схеме формирования хеш-остатков исправляющая способность хеш-кода остается прежней, а число перебираемых злоумышленником состояний оказывается экспоненциально связано с числом фрагментов – k:

$$N \approx 2^{k\cdot(16-3)}. \qquad (2).$$

Независимо от числа фрагментов, на которые разбивается корректируемый био-код, вторая схема формирования хеш-остатков (рис. 3) являет предпочтительнее. При практической реализации ее желательно дополнительно усилить, добавив открыто хранящейся «соли» при хешировании первых 16 разрядов. Если «соль» для каждого преобразователя биометрия-код будет своя, то атакующие лишаются возможности ускорения вычисления обратных хеш-преобразований относительно коротких кодов за счет их предварительного табулирования.

3. Усиление корректирующей способности хеш-кода за счет выравнивания распределения «слабых» разрядов био-кода

Следует отметить, что рассматриваемый класс самокорректирующихся хеш-кодов может быть применен как к «нечетким экстракторам» [4 -:- 7], так и к нейросетевым преобразователям биометрия-код [2, 3, 8]. Естественно, что хеш-коды намного выгоднее применять для нейросетевых преобразователей, так как их био-коды содержат в десятки раз меньше ошибок в сравнении с биокодами «нечетких экстракторов».

Рассмотрим случай, когда био-код нейросетевого преобразователя имеет длину 256 бит, бьется на 4 фрагмента длиной 64 бита и способен исправлять 8 ошибок (осуществляется перебор возможного положения пары ошибок в каждом из 4 фрагментов). Очевидно, что такая схема организации самокорректирующегося хеш-кода не сработает, если все 8 ошибок попадут в один из 4 фрагментов биокода. В связи с этим возникает задача выявления наиболее «слабых» разрядов био-кода и их перегруппировки. Перегруппировка должна обеспечить равномерность распределения слабых разрядов.

Выявить слабые разряды био-кода проще всего через тестирование нейросетевого преобразователя [9]. Нейросетевой преобразователь обычно хорошо обучается на 20 примерах биометрического образа «Свой». В этом можно убедиться, например, воспользовавшись средой моделирования «БиоНейроАвтограф» [10]. При обучении на 20 примерах вероятность ошибок первого рода (отказ в доступе) будет составлять 0,1. То есть, для надежного выявления 8 наиболее слабых разрядов био-кодов пользователю необходимо предъявить дополнительно от 40 до 80 примеров биометрического образа «Свой». При использовании среды моделирования «БиоНейроАвтограф» [10] придется от 40 до 80 раз воспроизводить рукописное парольное слово на графическом планшете или воспроизводить своею рукою буквы (цифры) на экране компьютера манипулятором «мышь». На воспроизведение десятков тестовых примеров образа «Свой» уходит больше времени, чем на обучение нейросетевого преобразователя биометрия-код.

Положение еще больше ухудшается, если техническое задание потребует обеспечить вероятность ошибок первого рода в 10 раз меньше. В этом случае потребуется использовать от 400 до 800 тестовых проверок, выявляющих слабые разряды био-кода с целью их последующего равномерного распределения по всей длине био-кода. Пользователи средств биометрической аутентификации негативно относятся к необходимости сотни раз предъявлять свои рукописные образы для того, чтобы корректно настроить хеш-корректировщик био-кода «Свой».

4. Сокращение затрат на тестирование путем искусственного ухудшения качества обучения нейросетевого преобразователя

Одним из технических приемов, позволяющих сократить затраты на тестирование, является искусственное ослабление нейросетевого преобразователя [10-1] за счет снижения числа примеров в обучающей выборке образа «Свой». В этом можно убедиться, проведя соответствующий численный эксперимент в среде моделирования «БиоНейроАвтограф». Результаты численного эксперимента сведены в табл. 1. Тестирование преобра-

Таблица № 1. Вероятность появления ошибок первого рода (отказ в доступе) и суммарного расстояния Хэмминга всех ошибок в зависимости от числа примеров, использованных при обучении нейронной сети

Рукописный образ	Число примеров в обучающей выборке									
	10	**12**	**14**	**16**	**18**	**20**	**22**	**24**	**26**	**28**
Пенза	0.67 94	0.34 48	0.21 31	0.13 18	0.12 15	0.05 6	0.05 5	0.04 4	0.03 3	0.04 4
сорока	0.81 104	0.41 63	0.24 39	0.16 22	0.14 19	0.08 11	0.06 6	0.06 7	0.04 4	0.05 5
добро	0.5384	0.31 41	0.27 39	0.12 15	0.12 12	0.09 13	0.07 9	0.07 7	0.07 8	0.07 7

зователя велось на базе из 100 примеров образа «Свой», не использованных ранее при обучении. Ввод биометрических данных осуществлялся графическим планшетом фирмы Genius: модель EasyPen.

Из табл. № 1 видно, что при уменьшении числа примеров в обучающий выборке нейросетевой преобразователь биометрия-код допускает все больше и больше ошибок. Ошибки бывают одиночные (в одном бите кода – это правая часть таблицы) и кратные (в нескольких битах био-кода – это левая часть таблицы). То есть, теоретически вполне возможно использовать данные, полученные на ослабленном преобразователе, и пытаться предсказывать вероятность правильной работы каждого из разрядов био-кода в полноценно обученном нейросетевом преобразователе. Мы имеем дело с обычной задачей почти линейного прогнозирования, предполагающей, что «слабые» разряды био-кода становятся еще «слабее» при снижении числа примеров в обучающей выборке. Стабильные разряды био-кода становятся еще стабильнее при увеличении числа примеров в обучающей выборке.

Это предположение верно далеко не для всех алгоритмов обучения искусственных нейронных сетей. Большинство известных алгоритмов обучения искусственных нейронных сетей неустойчивы. При их применении необходимо проверять гипотезу монотонности показателей стабильности разрядов биокода как функции числа примеров в обучающей выборке. О монотонности можно судить по соотношению вероятности появления ошибок, которая должна быть близка к отношению суммарного расстояния Хэмминга к числу проведенных опытов (правая часть таблицы).

Самым устойчивым на сегодняшний день является алгоритм автоматического обучения нейросети по ГОСТ Р 52633.5-2011 [11]. Именно этот алгоритм использован при реализации среды моделирования «БиоНейроАвтограф» и получения данных табл. № 1.

5. Оценка показателя стабильности каждого из разрядов био-кода случайным размыванием тестовых био-данных «Свой»

Чем больше мы будем иметь информации о поведении каждого из разрядов био-кода, тем надежнее будет прогноз его поведения. Получить дополнительную информацию о стабильности каждого из разрядов био-кода удается, если к тестовым примерам «Свой» добавить случайный шум - γ. Добавление к данным случайного шума эквивалентно введению мутации при размножении примеров биометрических данных в терминологии ГОСТ Р 52633.2-2010 [13-1].

При обучении нейросетевого преобразователя биометрия-код стандартным алгоритмом [12-1] вычисляют математическое ожидание $E(v_i)$ и стандартное отклонение $\sigma(v_i)$ по каждому из i-тых биометрических параметров (в среде моделирования «БиоНейроАвтограф» учитываются 416 биометрических параметров). Очевидно, что тестовый пример «Свой» может быть преобразован в сотню тестовых примеров (j = 1,2,…,100) путем добавления к его биометрическим параметром нормального случайного шума с нулевым математическим ожиданием $E(\xi)=0$:

$$\tilde{v}_{i,j} = v_i + \xi_{i,j}, \qquad (3)$$

Если дисперсия добавляемого шума мала $\sigma(\xi_i) << \sigma(v_i)$, то все разряды выходного биокода будут стабильны. Однако по мере увеличения стандартного отклонения добавляемого шума до величины, сопоставимой с $\sigma(v_i)$, положение меняется, наиболее нестабиль-

ные разряды био-кода проявляются. В них начинается изменение состояний. Чем чаще меняется состояние в разряде био-кода, тем разряд менее стабилен. Показатель стабильности определяется по формуле стандарта [11]

$$\omega_i = 2 \cdot \left| 0.5 - P_{"0",i} \right| = 2 \cdot \left| 0.5 - P_{"1",i} \right|, \qquad (4)$$

где: $P_{"0",i}$ – вероятность появления состояния «0» в контролируемом i-том разряде; $P_{"0",i}$ – вероятность появления состояния «1» в контролируемом разряде. При $\omega_i = 1$ контролируемый разряд полностью стабилен, при $\omega_i = 0$ контролируемый разряд предельно нестабилен.

Получается, что добавляя внешний шум, мы можем добиться появления 10% наиболее нестабильных разрядов. Более того, пользуясь показателем (4), нам удается упорядочить разряды био-кода по показателю их стабильности. После подобного упорядочивания нестабильных разрядов легко осуществить перекомпоновку разрядов био-кода с тем, чтобы выровнять частоту появления ошибок в каждом из фрагментов самокорректирующегося хеш-кода. При перекомпоновке слабых разрядов био-кода следует добиться совпадения суммы показателей стабильности (4) «слабых» разрядов в каждом из k-фрагментов.

6. Интегральная оценка вероятности появления ошибок первого рода в пространстве расстояний Хэмминга

Выше были описаны процедуры структурирования хеш-кодов, построенные на вычислении показателей стабильности разрядов био-кода. Практика синтеза хеш-кодов показала, что этого недостаточно. Необходимо иметь интегральное статистическое описание вероятностей появления ошибок первого рода для «нечетких экстракторов», нейросетевых преобразователей как с самокорректирующимися хеш-кодами, так и без них. Оказалось, что проще всего удается получить такое описание в пространстве расстояний Хэмминга между верным био-кодом "$\bar{c}$"и его ошибочными вариантами "$\bar{c}_j$":

$$h_j = \sum_{i=1}^{n} \left("c_i"\right) \oplus \left("c_{i,j}"\right), \qquad (5)$$

где: n – длина био-кода, $\oplus$ – операция сложения по модулю два состояний i-тых разрядов био-кодов.

Проведенные исследования показали [9], что плотность распределения расстояний Хэмминга – $p(h_j)$ хорошо описывается χ^2 распределением Пирсона, если его модифицировать под зависимые данные. Для осуществления такой модификации необходимо вектор случайных нормальных данных $\bar{\xi}$ с нулевыми математическими ожиданиями $E(\xi_i)=0$ и единичными стандартными отклонениями $\sigma(\xi_i)=1$ умножить на связывающую матрицу:

$$\begin{bmatrix} 1 & a & \cdots & a \\ a & 1 & \cdots & a \\ \cdots & \cdots & \cdots & \cdots \\ a & a & \cdots & 1 \end{bmatrix} \times \begin{bmatrix} \xi_{1,i} \\ \xi_{2,i} \\ \cdots \\ \xi_{n,i} \end{bmatrix} = \begin{bmatrix} y_{1,i} \\ y_{2,i} \\ \cdots \\ y_{n,i} \end{bmatrix}, \qquad (6)$$

$$R = \begin{bmatrix} 1 & r & \cdots & r \\ r & 1 & \cdots & r \\ \cdots & \cdots & \cdots & \cdots \\ r & r & \cdots & 1 \end{bmatrix}, \qquad (7)$$

Связывающая матрица имеет единичные элементы на диагонали и одинаковые элементы вне диагонали [2, 3]. В результате преобразования (6) корреляционная матрица (7) данных будет иметь одинаковые значения парных коэффициентов корреляции. Мы получаем так называемые «равнокоррелированные» данные. Далее, точно повторяя путь Пирсона, мы получаем зависимые χ^2 распределения с дискретными показателями числа степеней свободы - m. На рис. 4 даны примеры χ^2 распределений зависимых данных для $m = 3$ и $m = 4$.

Как для зависимых, так и для независимых данных математическое ожидание χ^2 распределения точно совпадает с числом степеней свободы. Для биометрических данных математическое ожидание расстояний Хэмминга $E(h)$ всегда является дробной (фрактальной) величиной. Нет никаких серьезных причин ожидать точного совпадения математического ожидания распределения расстояний Хэмминга с целыми величинами. Эта величина оказывается близка к целой, только если строго придерживаться пути Пирсона при численном моделировании χ^2 распределения.

Для перехода к дробным (фрактальным) показателям необходимо учитывать расстояния до ближайших целых чисел степеней свободы:

$$\begin{aligned} p_{\chi^2}\left(E(h), h, r\right) = (E(h) - a_0) \cdot p_{\chi^2}\left(a_0, h, r\right) + \\ + (a_0 + 1 - Eh(h)) \cdot p_{\chi^2}\left((a_0 + 1), h, r\right) \end{aligned}, \qquad (8)$$

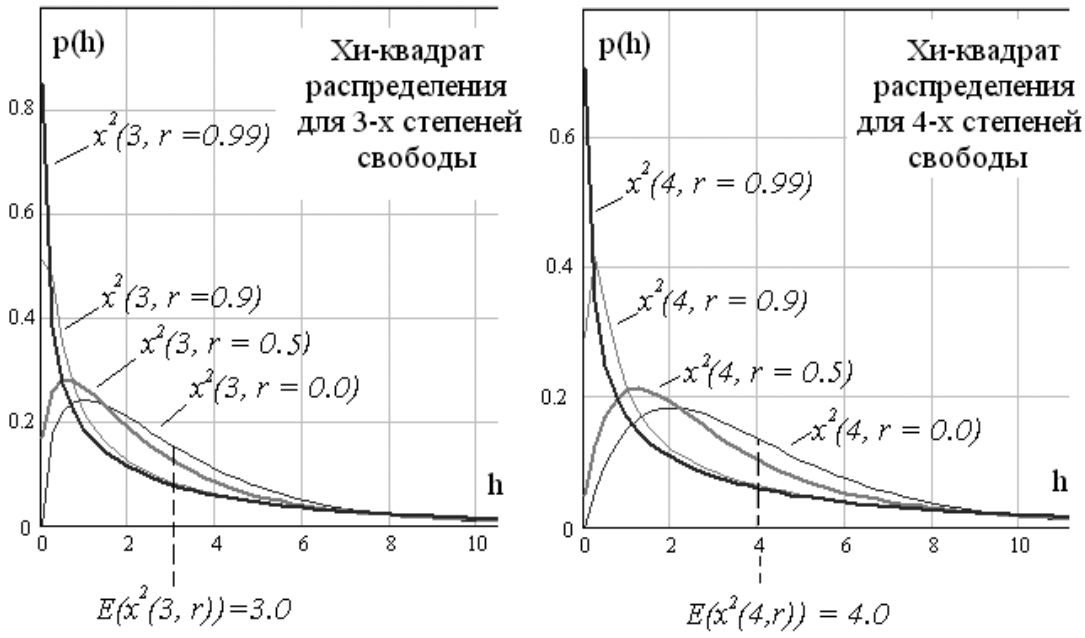

Рис. 4. Кривые плотности χ^2 распределения для трех и четырех степеней свободы, полученные для разных значений коррелированности данных

где параметр a_0 – это ближайшее целое число меньшее или равное вычисленному – $E(h)$;

$$a_0 = \text{floor}(E(h)), \qquad (9)$$

где операция $\text{floor}(.)$ отбрасывает дробную часть числа $E(h)$.

Следует отметить, что использование равнокоррелированных данных (6) для моделирования зависимых распределений Пирсона – это не что иное, как один из приемов симметризации ядер многомерной статистической обработки (многомерных вложенных в друг друга интегралов вычисления вероятности). Этот прием получен копированием идеи симметризации ядер Вольтерра, активно используемой при идентификации нелинейных динамических объектов [13, 14, 15, 16].

7. Заключение

«Нечеткие экстракторы» оказываются много слабее нейросетевых преобразователей биометрия-код из-за применения в них классических самокорректирующихся кодов с 15-кратной избыточностью. Применение рассматриваемых в данной статье кодов безопасно, так как в качестве синдромов ошибок в них используются фрагменты необратимых криптографических хеш-функций. При этом отпадает необходимость в искусственном сокращении био-кода путем изъятия части его разрядов на покрытия избыточности самокорректирующегося кода. Хеш-коды не имеют избыточности в обычном понимании этого слова. Их применение для защиты биометрических данных радужной оболочки глаза позволит поднять длину био-кода с 128 бит до 2048 бит (в 15 раз). Однако полноценный расчет оптимального соотношения параметров хеш-кодов требует перейти от использования классического распределения Пирсона к его модификации, построенной для дробных (фрактальных) показателей числа степеней свободы и учета сильной коррелированности состояний разрядов био-кода «Свой».

В целом открывается перспектива создания так называемых «высокодоступных» преобразователей биометрия-код, которые будут способны обеспечивать любую заданную вероятность ошибок первого рода при сохранении высокого значения вероятности ошибок второго рода. Предположительно, эта новая ветвь преобразователей будет строиться путем усиления нейросетевых преобразователей, выполненных по требованиям отечественных стандартов серии ГОСТ Р 52633.xx-20xx с дополнительным применением рассматриваемых в данной статье самокорректирующихся хеш-кодов.

ЛИТЕРАТУРА:

1. Иванов А. И., Сомкин С. А., Андреев Д. Ю., Малыгина Е. А. О многообразии метрик, позволяющих наблюдать реальные статистики распределения биометрических данных «нечетких экстракторов» при их защите наложением гаммы // «Вестник Уральского федерального округа. Безопасность в информационной сфере». 2014. № 2(12). С. 16–23.

2. Язов Ю. К. и др. Нейросетевая защита персональных биометрических данных // Ю. К. Язов (редактор и автор), соавторы В. И. Волчихин, А. И. Иванов, В. А. Фунтиков, И. Г. Назаров // М. : Радиотехника, 2012. 157 с.

3. Ахметов Б. С., Иванов А. И., Фунтиков В. А., Безяев А. В., Малыгина Е. А. Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа: // Монография. Казахстан, г. Алматы, ТОО «Издательство LEM», 2014. 144 с.- свободный доступ http://portal.kazntu.kz/files/publicate/2014-06-27-11940.pdf

4. Y. Dodis, L. Reyzin, A. Smith Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy, Data April 13, In EUROCRYPT, pages 523–540, 2004.

5. F. Monrose, M. Reiter, Q. Li, S. Wetzel. Cryptographic key generation from voice. In Proc. IEEE Symp. on Security and Privacy, 2001.

6. Ramírez-Ruiz J., Pfeiffer C., Nolazco-Flores J. Cryptographic Keys Generation Using FingerCodes // Advances in Artificial Intelligence – IBERAMIA-SBIA 2006 (LNCS 4140), p. 178–187, 2006.

7. Feng Hao, Ross Anderson, and John Daugman. Crypto with Biometrics Effectively, IEEE TRANSACTIONS ON COMPUTERS, VOL. 55, NO. 9, SEPTEMBER 2006.

8. Безяев А. В. Нейросетевой преобразователь в самокорректирующийся код, совершенно не обладающий избыточностью // «Нейрокомпьютеры: разработка, применение» № 3, 2012, С. 52–55

9. Фунтикова Ю. В., Иванов А. И., Захаров О. С. Гипотеза № 2 распределения расстояний Хэмминга для кодов биометрической аутентификации примеров образа «Свой». Труды научно-технической конференции кластера пензенских предприятий, обеспечивающих безопасность информационных технологий. Том 9. Пенза, 2014, с. 7–8. Свободный доступ http://www.pniei.penza.ru/RV-conf/T9/C7.

10. Среда моделирования «БиоНейроАвтограф» размещена на сайте ОАО «Пензенский научно-исследовательский электротехнический институт»: http://пниэи.рф/activity/science/noc.htm. Продукт создан лабораторией биометрических и нейросетевых технологий ОАО «ПНИЭИ» для свободного распространения среди университетов России, Белоруссии, Казахстана.

11. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».

12. ГОСТ Р 52633.2-2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации».

13. Мармарелис П., Мармарелис В. Анализ физиологических систем (метод белого шума) М.: Мир. 1981, 480 с.

14. Billings S. A. Identification of nonlinear system (A survey)// Proc. IEEE, part D, 1980, V 127, N 6, p.p. 272–285.

15. Пупков К. А., Капалин В. И., Ющенко А. С.. Функциональные ряды в теории нелинейных систем. - М.: Наука, 1976, 448 с.

16. Иванов А. И. Нейросетевые технологии биометрической аутентификации пользователей открытых систем. Автореферат на соискание ученой степени доктора технических наук по специальности 05.13.01. Пенза, 2002. 34 с. Пензенский государственный университет.

Безяев Александр Викторович, к. т. н., ведущий специалист Пензенского филиала ФГУП НТЦ «Атлас». E-mail: ivan@pniei.penza.ru

Иванов Александр Иванович, д. т. н., доцент, начальник лаборатории биометрических и нейросетевых технологий «ОАО Пензенский научно-исследовательский электротехнический институт». E-mail: ivan@pniei.penza.ru

Фунтикова Юлия Вячеславовна, инженер ОАО «Пензенский научно-исследовательский электротехнический институт». E-mail: ivan@pniei.penza.ru

Bezyaev Alexander, PhD, a leading specialist Penza branch of FGUP NTC «Atlas». E-mail: ivan@pniei.penza.ru

Ivanov Alexander, doctor of technical sciences, Associate Professor, head of the laboratory of biometric and neural network technology «Penza research Electrotechnical Institute». E-mail: ivan@pniei.penza.ru

Funtikova Yulia, engineer «Penza research Electrotechnical Institute». E-mail: ivan@pniei.penza.ru