Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 10, Пенза-2016, с. 43-46 (http://пниэи.рф/activity/science/BIT/T10-p43.pdf)

УДК: 519.2, 612.087, 621.319.7

Безяев А.В.

Оценка выигрыша от использования фрагментов квантовой суперпозиции при корректировке ошибочных состояний нейросетевого преобразователя биометрия-код

В настоящее время активно идут процессы информатизации современного общества, как итог, наша персональная информация постепенно перемещается в Интернет облака. Примером тому могут являться электронные медицинские документы, хранящиеся на облачном сервере [1, 2, 3]. Примерно такая же ситуация возникает при использовании «облачного» кассового аппарата. В этом случае владелец «облачного» кассового аппарата может получить информацию о кассовых операциях только в своем электронном кабинете. И в том, и в другом случае чувствительная для нас информация оказывается в облачном хранилище и необходимо предпринимать специальные действия по ее дополнительной защите.

Биометрия рукописного почерка, голоса, лица, рисунка отпечатка пальца, рисунка подкожных кровеносных сосудов позволяет решить задачу ограничения доступа при ее хранении на облачных серверах.

За рубежом идут работы по защите биометрических данных через использование, так называемых, «нечетких экстракторов» [4, 5, 6, 7]. Однако, это техническое решение не является стойким по отношению к атакам, построенным на применении высокоразмерных наблюдателей [8, 9].

Задача данной работы показать, что нейросетевые преобразователи биометрия-код [10], автоматически обученные по ГОСТ Р 52633.5 [11], имеют значительные дополнительные резервы по повышению их корректирующей способности за счет введения обратной связи, работающей в режиме поддержки квантовой суперпозиции нестабильных разрядов [12].

На рисунке 1 дано двухмерное отображение работы обученной нейронной сети преобразователя биометрия-код. Каждый нейрон делит пространство все «Чужие» пополам. Двухмерное сечение дает множество линий деления пространства «Чужие», пересекающихся в центре.

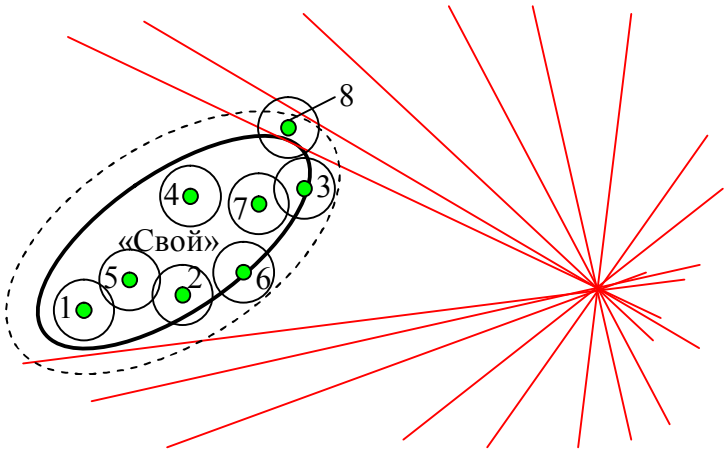

Рис. 1. Двухмерное представление нейронной сети, обученной алгоритмом ГОСТ Р 52633.5

Алгоритм обучения по ГОСТ Р 52633.5 [11] обеспечивает условие по которому линии, разделяющие пространство, не пересекают область распределения данных «Свой». Однако, эта область не может быть точно описана при использовании малой обучающей выборки. Из рисунка 1 видно, что примеры образа «Свой» с номерами 1, 2, 3, 4, 5, 6, 7 дают верный выходной код нейронной сети. Восьмой пример образа «Свой» дает ошибочное состояние одного нейрона на фоне 10 верных состояний (на рисунке 1 отображены 11 проекций разделяющих гиперплоскостей).

Для того, что бы определить слабый (неустойчивый) разряд выходного кода нейронной сети, необходимо к входным биометрическим данным подмешать тестовый шум, как это показано на рисунке 2.

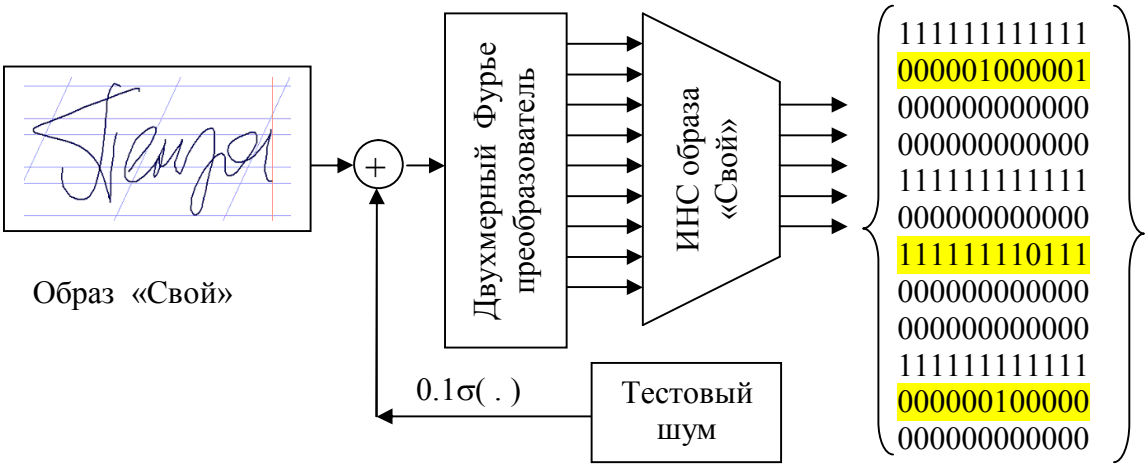

Рис. 2. Организация сканирования окрестностей примера образа «Свой» через добавление шума к биометрическим данным

Как видно из рисунка 2, большинство выходных разрядов кода нейронной сети при тестовом шуме в 0.1 от естественного стандартного отклонения биометрических данных, оказываются стабильными. Однако, часть разрядов, порождаемых зашумленными биометрическим данными, имеют некоторую нестабильность. На рисунке 2 нестабильные разряды помечены заливкой. Из 12 отображенных разряда 2 разряда имеют по одному отклонению на 12 верных состояний, а один разряд имеет 2 ошибочных состояния (верхняя залитая строка) на 11 верных состояний.

Получается, что, пользуясь очень простым решающим правилом, мы можем отделить стабильные разряды от нестабильных. У девяти разрядов рисунка 2 показатель стабильности оказывается единичным:

$$w_1 = w_3 = w_4 = w_5 = w_6 = w_8 = w_9 = w_{10} = w_{12} = 1 .$$

У двух разрядов он будет составлять:

$$w_7 = w_{11} = 2\left|\frac{1}{2} - \frac{1}{12}\right| = 0.833 .$$

Для самого нестабильного разряда показатель примет значение:

$$w_2 = 2\left|\frac{1}{2} - \frac{2}{12}\right| = 0.667 .$$

Эта информация может быть использована для ускорения вычислений корректора ошибок, безопасно хранящего сведения о синдромах ошибок в виде фрагментов хэш-функций [13, 14, 15]. Структурная схема такого корректора приведена на рисунке 3.

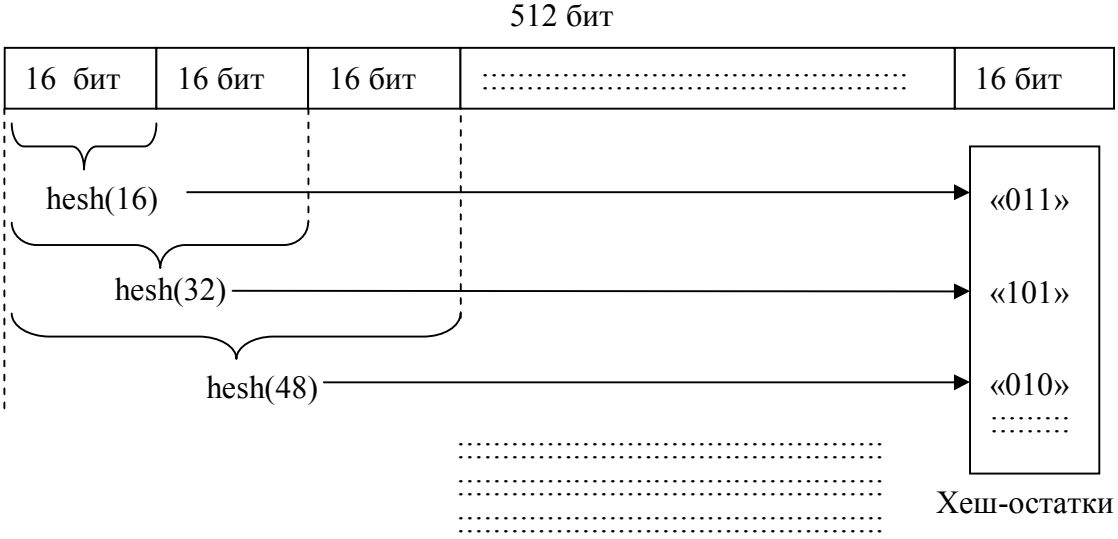

Рис. 3. Безопасная схема рекурсивного формирования эталонных хеш-остатков

Корректирующий код построен на том, что защищаемая последовательность в 512 бит делится на 32 фрагмента по 16 бит. Для верного состояния защищаемого кода вычисляются хеш-функции от 16, 32, 48,…., 512 бит. Три бита каждой хеш-функции запоминают в таблицу хеш-остатков, например, это могут быть последние 3 бита каждой из хеш-функций.

Такой код способен корректировать по три ошибки в каждом из выделенных 32 фрагментах. Корректировка выполняется путем перебора состояний всех возможных положений трех ошибок. Всего приходится проверять: $C_{16}^{3} = \frac{16!}{3!(16-3)!} = 560$ состояний для каждого из 16-битных фрагментов кода.

Если же мы будем сканировать показатель стабильности состояний разрядов кода в соответствии с блок-схемой рисунка 2, то появляется возможность выявить три самых нестабильных разряда. Нет смысла проверять данные, изменяя состояния стабильных разрядов. Получается, что вместо 560 проверяемых положений возможных ошибок мы будем анализировать только одно состояние, если обнаружен один нестабильный бит. Если обнаружены два нестабильных бита, то потребуется проверять 2 возможных состояния положения двух ошибок. При обнаружении трех нестабильных разрядов придется проверять 3!=6 состояний. Мы наблюдаем многократное снижение проверяемых состояний возможного положения ошибок.

Очевидно, что столь значительные возможности повышения корректирующей способности кодов будут реализованы наиболее эффективно после 2018 года, когда «Фонд перспективных исследований» выполнит ОКР по разработке отечественной мало потребляющей микросхемы, ориентированной на аппаратно-программное воспроизведение больших искусственных нейронных сетей. Использование новых кодов с высоким уровнем исправляемых ошибок даст возможность работы в реальном масштабе времени при мобильном (мало потребляющем) варианте исполнения изделий биометрического контроля.

ЛИТЕРАТУРА:

1. Федеральная типовая медицинская информационная система (ФТМИС). Разработчик «Крокус Консалдинг» 2008 г., государственный контракт по ФЦП «Электронная Россия (2002-2010 годы).

2. Электронное рабочее место врача. Руководство пользователя. Москва-2014 г., 23 с.
3. Зингерман Б.В., Шкловский-Корди Н.Е., Карп В.П., Воробъев А.И. Интегрированная электронная медицинская карта: задачи и проблемы. //Врач и информационные технологии. №1, 2015 г., с. 24-27.
4. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy // Proc. EUROCRYPT, April 13, pages 523-540, 2004.
5. Monrose F., Reiter M., Li Q., Wetzel S. Cryptographic key generation from voice. //Proc. IEEE Symp. on Security and Privacy, pp. 202-213, 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. Hao F., Anderson R., Daugman J. Crypto with Biometrics Effectively //IEEE TRANSACTIONS ON COMPUTERS, VOL. 55, NO. 9, SEPTEMBER, Page(s):1073 – 1074, 2006.
8. Иванов А.И. Нечеткие экстракторы: проблема использования в биометрии и криптографии. // Первая миля. № 1, 2015 г. с. 40-47.
9. 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 г. № *2(12)* с. 16-23.
10. 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 г. 157 с. IBSN 978-5-88070-044-8.
11. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».
12. Иванов А.И. Многомерная нейросетевая обработка биометрических данных с программным воспроизведением эффектов квантовой суперпозиции. Издательство АО «ПНИЭИ», Пенза-2016 г., 133 с. Свободный доступ http://пниэи.рф/activity/science/BOOK16.pdf
13. Безяев А.В. Безкомпроматная индикация качества ввода фрагментов тайного составного биометрического образа «Нейрокомпьютеры: разработка, применение» №6, 2009 с. 59- 62
14. 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 г. -144 с., находится в открытом доступе (http://portal.kazntu.kz/files/publicate/2014-06-27-11940.pdf).
15. Безяев А.В., Иванов А.И., Фунтикова Ю.В. Оптимизация структуры самокорректирующегося био-кода, хранящего синдромы ошибок в виде фрагментов хеш-функций. «Вестник Уральского федерального округа. Безопасность в информационной сфере» 2014 г. № 3*(13)* с. 4-14.

Статья поступила 02.10.2016, опубликована 23.11.2016 по положительной рецензии к.т.н. Зефирова С.Л.