Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 8, Пенза-2012, с. 76-80 (http://пниэи.рф/activity/science/BIT/T8-p76.pdf)

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ ХЭШ-КОДОВ, ОСУЩЕСТВЛЯЮЩИХ ОБНАРУЖЕНИЕ И КОРРЕКТИРОВАНИЕ ОШИБОК В БИОМЕТРИЧЕСКИХ ПРЕОБРАЗОВАТЕЛЯХ

Безяев А.В., Фунтикова Ю.В. (Пенза)

Использование классических кодов, обнаруживающих и исправляющих ошибки в «нечетких» преобразователях биометрия-код [1, 2, 3, 4], обусловлено тем, эти коды хорошо изучены, и для них имеются проверенные технические решения. Основной недостаток всех подобных технических решений состоит во введении значительной избыточной части кода до 300% как это показано на рис. 1.

В биометрических приложениях требуется правильно восстанавливать только эталонный ключ пользователя "Свой". В связи с этим, нет необходимости использовать избыточные разряды био-кода биометрического преобразователя для перекодировки в самокорректирующийся код. Можно безопасно записать избыточную часть кода (контрольные разряды) в память биометрического приложения, если осуществить их предварительное хеширование [5, 6]. Этот технический прием позволяет уйти от «накладных» расходов на избыточность и тем самым более рационально расходовать кодовое пространство.

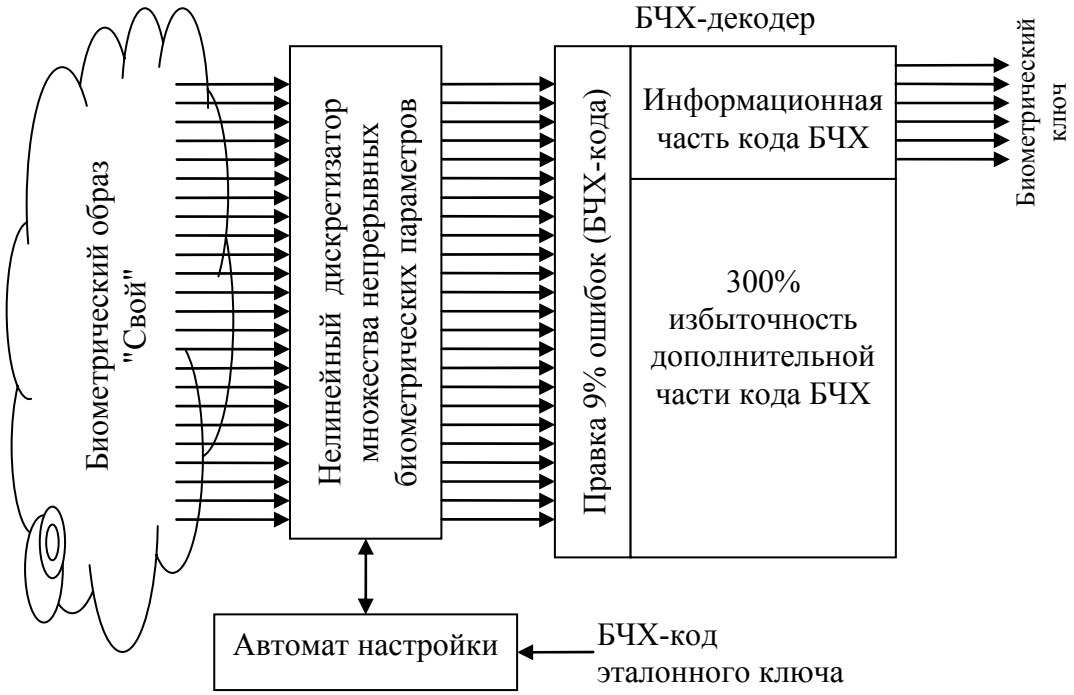

Рис. 1. Простейший нечеткий экстрактор с классическим кодом обнаружения и исправления ошибок

Еще одним отрицательным моментом хранения избыточной части кода, обнаруживающего и исправляющего ошибки, в биометрическом приложении является угроза компрометации биометрического ключа. Зная значение избыточной части кода, удается частично скомпрометировать сам ключ. Как следствие, избыточная часть кода может храниться совместно с биометрическим

преобразователем только при обеспечении безопасности хранения в доверенной вычислительной среде.

Отказаться от необходимости применения доверенной вычислительной среды возможно в том случае, если синдромы ошибок хранятся в безопасной форме. Например, в качестве синдромов ошибок могут быть использованы усеченные хэш-функции биометрического ключа или его фрагментов [5, 6]. На рисунке 2 приведена блок-схема организации вычислений для корректировки кода с синдромами ошибок в виде трех разрядов хэш-функции. Производится усечение хэш-функции до трех разрядов для того, чтобы дополнительно усложнить возможность обратного преобразования.

При работе таких кодов производится хэширование биометрического кода с ошибками, полученная хэш-функция сравнивается с ее эталоном. Если хэш-функция не совпадает, то запускается автомат последовательного перебора состояний разрядов биометрического кода. Программный автомат перебора способен очень быстро проверить возможность наличия одиночной ошибки. Если цикл проверки всех состояний одиночной ошибки не дал совпадения хэш-функций и эталона, то производится проверка всех возможных положений двух ошибок в биометрическом коде. Процесс идет постепенным наращиванием числа возможных ошибок в коде до момента совпадения очередной хэш-функции с эталоном. Очевидно, что большое число ошибок в подобных кодах скорректировать нельзя из-за экспоненциального роста сложности решаемой задачи направленного перебора. Тем не менее, удается за приемлемое время скорректировать до 4-5 ошибок биометрического кода длиной 256 бит, что составляет примерно 0.6% ошибок.

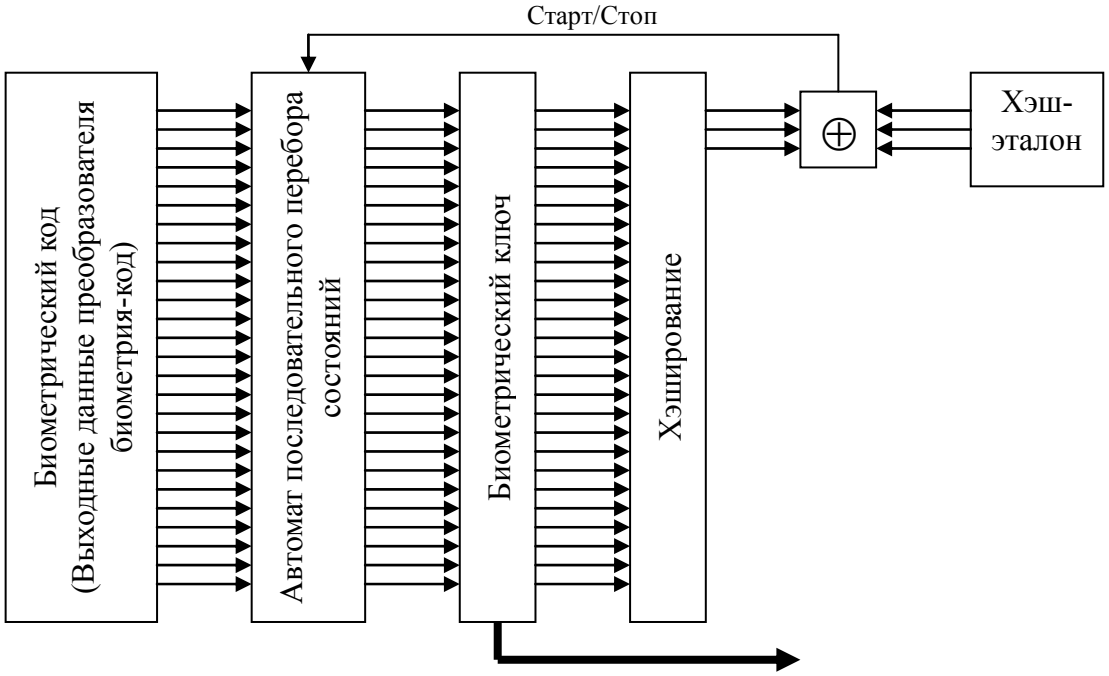

Рис. 2. Самокорректирующийся код, не обладающий избыточность из-за возможности безопасного хранения усеченных хэш-эталонов

Практика применения нейросетевых преобразователей биометрия-код показывает, что ошибок в биометрическом коде может быть больше, чем 1%, кроме того длина самого кода может составлять 512, 1024, 2048 бит. Увеличение длины биометрического кода и числа возможных ошибок в нем требуют модернизации схемы рисунка 2.

Для более длинных кодов и кодов с большим числом ошибок следует уменьшить длину кода, перебираемого автоматом, и увеличить число вычисляемых хэш-функций.

Еще одним техническим приемом является объединение хэшируемых данных в матрицу (см. рис. 3) по аналогии с простейшими блочными кодами проверки на четность. Подобное объединение позволяет сравнивать синдромы ошибок строк и столбцов информационной части матрицы без перебора состояний хэшируемых данных. Сокращается время обнаружения и исправления ошибок, без «накладных» расходов на избыточность.

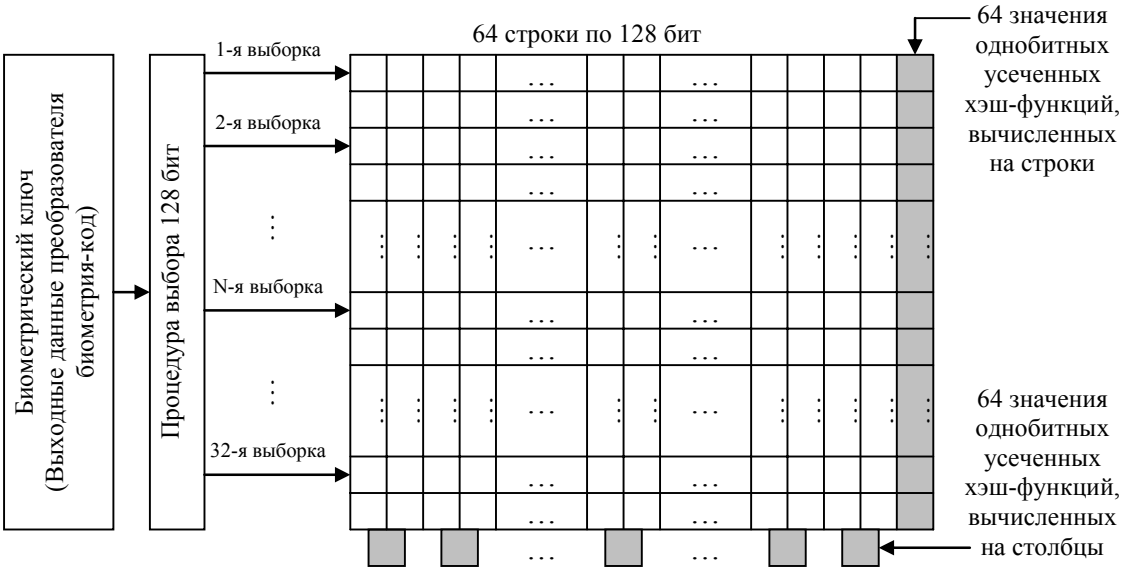

Рис. 3. Блок-схема хэш-кода способного обнаруживать и исправлять ошибки

По предложенному техническому решению на этапе обучения преобразователя биометрия-код для эталонного биометрического ключа, кроме вычисления хэш-эталона всего ключа, выполняется вычисление набора усеченных хэш-функций следующим образом.

Из эталонного биометрического ключа производят псевдо случайную выборку 128 бит (рис. 3). Выбранные 128 бит записываются в первую строку матрицы, оставшиеся 128 бит записываются во вторую строку. В результате 32 выборок получаем матрицу 128*64 бита.

Для каждой 128-битной строки и для каждых двух 64-битных столбцов производится вычисление 1 бита усеченной хэш-функции.

Вычисленные эталонные значения усеченных хэш-функций и правило выборки 128 бит хранятся вместе с преобразователем биометрия-код.

При вводе пользователем своего биометрического образа полученный биометрический ключ по тому же правилу выборки 128 бит преобразуется в матрицу 128*64 бита и производится проверка совпадения усеченных хэш-эталонов.

При отклонении введенного биометрического образа полученный биометрический ключ будет отличаться от эталонного. Если отклонения при вводе были незначительные (количество не совпавших разрядов ключа порядка 10%), то выбирая пересечения строк и столбцов матрицы с не совпавшими усеченными хэш-эталонами, достаточно просто определяются возможные положения искаженных разрядов биометрического ключа. Далее производится перебор выявленных возможных положений искаженных разрядов и исправление ошибок до достижения совпадения хэш-эталона всего ключа.

При переборе всех разрядов ключа современные вычислительные средства позволяют исправлять до 5 ошибок, так как перебор всех состояний ключа и

вычисление хэш-функций для них требует значительных вычислительных ресурсов и занимает значительное время.

Путем сокращения количества подбираемых разрядов возможно исправление до 7% ошибок биометрического ключа за тоже самое время.

При значительном количестве отклонений введенного биометрического образа из-за большого количества ошибок в полученном биометрического ключе возникает большое количество коллизий при проверке усеченных хэш-эталонов. Так как хэш-эталон содержит всего один бит, то при наличии ошибок в биометрическом ключе с вероятностью 1/2 хэш-эталон на выбранные 128 бит совпадает. Ошибки выявляются в случайных разрядах ключа и перебор выявленных ошибок не приводит к положительному результату проверки хэш-эталона всего биометрического ключа, что не позволяет злоумышленнику произвести подбор биометрического образа пользователя "Свой".

Таким образом, благодаря использованию массива усеченных хэш-эталонов и разбиению биометрического ключа на несколько фрагментов, при вводе пользователем биометрического образа с отклонениями от эталона появляется возможность достаточно точно оценить количество ошибок в полученном биометрическом ключе и исправить обнаруженные ошибки перебором. При этом за счет сокращения количества перебираемых разрядов, время восстановления биометрического ключа значительно сокращается. Технически выгодно осуществлять матричное структурирование корректируемых данных и осуществлять хэширование по строкам и столбцам псевдо-случайной матрицы. При этом алгоритм ее формирования и синдромы ошибок в виде усеченных хэш-функций хранятся открыто.

При вводе биометрического образа со значительными отклонениями большое количество ошибок полученного биометрического ключа не позволит выделить "правильные" разряды ключа и, соответственно, не дает злоумышленнику возможности подобрать биометрический образ, ориентируясь на количество ошибок.

Так же массив из однобитных усеченных хэш-эталонов не дает информации об эталонном ключе, что не позволяет злоумышленнику восстановить эталонный ключ или биометрический образ при получении доступа к исполняемому коду биометрического преобразователя. Поле перебираемых вариантов био-кода остается таким же как и у классических кодов с обнаружением и исправлением ошибок, однако хранение синдромов в виде хэш-функций превращает полиномиальную задачу перебора в задачу экспоненциальной вычислительной сложности.

Таким образом, пользователю "Свой" предоставляется возможность аутентификации при вводе биометрического образа с небольшим количеством отклонений от эталона без компрометации биометрического образа или ключа, получаемого из этого образа.

Предложенный вариант исправления ошибок в биометрическом ключе может быть модернизирован:

1) возможно уменьшение или увеличение количества 128-битных выборок. Например, использование матрицы 128*32 бита значительно сокращает количество вычислений хэш-функций, но уменьшает точность определения искаженных разрядов. Использование матрицы 128*128 бит, наоборот, увеличивает возможности исправления, но также значительно увеличивает количество вычислений.

2) возможно увеличение разрядности усеченных хэш-эталонов. При использовании усеченных хэш-эталонов, содержащих 2 или 3 разряда, значительно увеличивается вероятность определения искаженных разрядов, но

при этом значительное увеличение разрядности хэш-эталонов может привести к возможности компрометации биометрического ключа.

Количество усеченных хэш-эталонов биометрического ключа и их разрядность должны выбираться при разработке и обучении преобразователя биометрия-код исходя из конкретных условий использования разрабатываемого биометрического приложения. Предположительно должны использоваться методы численной оптимизации.

Список использованной литературы:

1. 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.

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

3. Arakala A., Jeffers J., Horadam K.J. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication. //Advances in Biometrics (LNCS 4642), Springer, pp. 760-769, 2007

4. Чморра А.Л. Маскировка ключа с помощью биометрии «Проблемы передачи информации» 2011 № 2(47) с. 128-143.

5. Безяев А. В. Нейросетевой преобразователь биометрии в самокорректирующийся код, совершенно не обладающий избыточностью. Нейрокомпьютеры: разработка и применение, №3 2012, с. 52 – 55.

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

Статья поступила 21.12.2012, опубликовано в Интернет 15.01.2013 по положительной рецензии д.т.н., доцента Иванова А.И.