УДК 004.056.5, 004.522, 004.93’1, 519.2, 57.087, 612.087

ОТМЕНЯЕМАЯ БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ С ИСПОЛЬЗОВАНИЕМ НЕЧЕТКОГО ХРАНИЛИЩА

Н. А. РАЩЕНЯ, Г. Ф. АСТАПЕНКО, М. И. НОВИК
(Научно-исследовательское учреждение «Институт прикладных физических проблем им. А. Н. Севченко» Белорусского государственного университета, Минск)

Аннотация. *Предложена схема биометрической аутентификации на основе отпечатка пальцев и парольной фразы, при этом используются механизмы нечеткого хранилища и возобновляемых биометрических шаблонов. Приведены достоинства предложенной схемы.*

Ключевые слова: *отпечаток пальца, парольная фраза, отменяемый биометрический шаблон, нечеткое хранилище, безопасность критических данных, регистрация пользователя, аутентификация.*

1. Методы отменяемой биометрии. Отменяемая биометрия направлена на усиление защиты конфиденциальности и безопасности шаблонов в существующих биометрических системах [1]. При этом биометрический шаблон искажается таким образом, что исходные данные недоступны злоумышленнику, но все же может быть выполнено распознавание личности. Отменяемая биометрия должна обладать тремя важными характеристиками, а именно:

– разнообразие: один и тот же отменяемый биометрический шаблон нельзя использовать для разных приложений;

– возможность повторного использования/отзыва: шаблон повторно выпускается в случае компрометации;

– необратимость: оригинальные биометрические данные невозможно восстановить, если сгенерированный шаблон был скомпрометирован.

Наиболее популярными в настоящий момент являются методы преобразования, а также методы, основанные на криптографии [1]. Одними из основных методов на основе преобразования являются следующие:

– необратимое преобразование (декартовых, полярных координат);

– преобразование Адамара (на основе функций Уолша);

– проективные преобразования;

– фильтрующие преобразования.

Методы криптографии, в зависимости от типа используемого алгоритма, делятся на различные типы: визуальная криптография, хеширование изображений,

подпись знаний, криптография на основе эллиптических кривых (ECC), хаос, стеганография, нечеткое обязательство и шифр Хилла.

2. Принцип нечеткого хранилища секретных данных (ключей). Безопасность системы аутентификации можно усилить, используя биометрическую систему, вместо традиционного метода аутентификации, такого как удостоверение личности (ID) и пароль, которые можно легко украсть. Среди всех модулей биометрической системы, которым необходимо обеспечить безопасность, защита биометрических шаблонов нуждается в наибольшем внимании из-за чувствительности биометрических данных, хранящихся в форме шаблона. Для обеспечения защиты шаблонов был разработан ряд методов.

Нечеткое хранилище (fuzzy vault) [2] – это один из методов защиты шаблонов, основанный на криптосистеме. Целью метода нечеткого хранилища является защита ненадежных данных с помощью биометрического шаблона таким образом, чтобы только сертифицированный пользователь мог получить доступ к секрету, предоставив действительные биометрические данные.

Нечеткое хранилище может быть процедурой по обеспечению безопасности криптографических ключей для симметричных криптосистем. Нечеткое хранилище защищает шаблон, а также ключ k, блокируя шаблон с помощью ключа, и законный пользователь может получить доступ к ключу только в том случае, если его шаблон пересекается с заблокированным. Нечеткое хранилище состоит из двух этапов: кодирования и декодирования. Секретный ключ кодируется (шифруется) в виде полинома p, коэффициенты которого представляют собой ключ. Вектор биометрических признаков V проецируется на полином, чтобы сформировать набор подлинных точек. Некоторые точки, для повышения безопасности, называемые точками чафф (chaff), генерируются случайным образом и не должны совпадать с подлинными. Коллекция подлинных точек и точек chaff образует хранилище. На этапе декодирования производится разблокирование секретного ключа k'. Пользователь представляет свой собственный набор признаков V' и может разблокировать секрет k, если набор признаков V' в значительной степени совпадает с набором признаков V [3]. Безопасность этого метода зависит от сложности полиномиальной регенерации (например, на основе аппроксимации Лагранжа).

3. Предлагаемая схема аутентификации пользователя. На рисунке 1 приведена обобщенная схема регистрации и аутентификации пользователя на основе хранилища секретных данных.

Функционирование предлагаемой схемы выполняется посредством следующих фаз и шагов.

Фаза регистрации в центре выпуска серии персональных устройств

1. Секретный ключ k (например, мастер-ключ) первоначально записывается в секретную память устройства.

2. В секретную память записывается дополнительная информация [4] (например, идентификационный номер владельца персонального устройства, параметры широковещательного обмена в виртуальной частной сети (ВЧС) и др.).

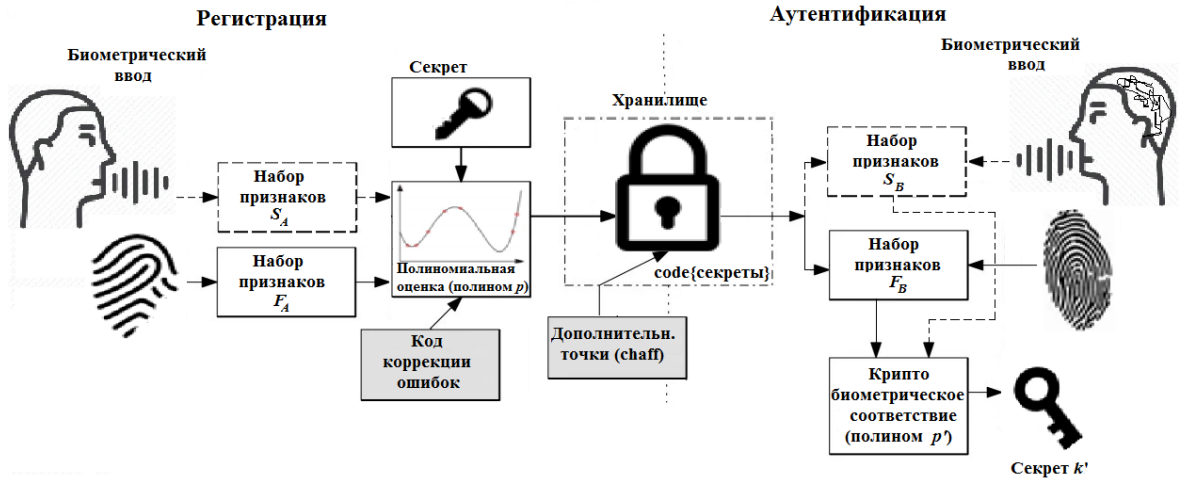

Рисунок 1 – Нечеткая схема хранилища секретных данных

Фаза инициализации

1. Вычисляется хэш-образ секретного ключа h(k).

2. Вводятся не менее трех раз изображения отпечатка пальца для формирования шаблона TF (Template Finger) (посредством преобразования набора признаков F_A).

3. Формируется нечеткий кодировщик GenF с помощью биометрического шаблона TF для скрытия k, при этом используется полиномиальное преобразование (p_1) и один из кодов исправления ошибок Cod_1 (БЧХ, Рида-Соломона или LDPC (Low Density Parity Check)). Следует отметить, что длина двоичной последовательности кодирования должна быть больше L бит, где L – приемлемый уровень безопасности).

4. Кодируется секретный ключ k с помощью GenF: k_{SF} = GenF(k, Cod_1, C_1), где C_1 – вспомогательная случайная последовательность дополнительных точек.

5. Произносятся парольная фраза (при трехкратном повторении) для формирования шаблона TS (Template Speaker) (посредством преобразования набора признаков S_A, сформированном на основе конкатенации вектора признаков при верификации спикера по голосу, а также вектора признаков при распознавании слов фиксированной парольной фразы [4]).

6. Формируется нечеткий кодировщик GenS с помощью биометрического шаблона TS для скрытия k, при этом используется полиномиальное преобразование (p_2) и один из кодов исправления ошибок Cod_2.

7. Кодируется секретный ключ k с помощью GenS: k_{SS} = GenS(k, Cod_2, C_2), где C_2 – вспомогательная случайная последовательность.

Фаза проверки (верификации) инициализации

1. Вводится изображение отпечатка пальца TF′.

2. Формируется нечеткий экстрактор ExtF с помощью биометрического шаблона TF′ (посредством преобразования набора признаков F_B) для восстановления k, при этом используется полином p_1 и один из кодов исправления ошибок Cod_1.

3. Декодируется k' с помощью нечеткого экстрактора ExtF: k' = ExtF(k_{SF}, p_1, Cod_1).

4. Формируется хэш-образ извлеченного k': h(k').

5. Выполняется проверка равенства: h(k') == h(k)?.

6. Если равенство удовлетворяется, продолжение фазы проверки инициализации, иначе – выход по ошибке.

7. Произносится парольная фраза для формирования шаблона TS′ (посредством преобразования набора признаков S_B).

8. Формируется нечеткий экстрактор ExtS с помощью биометрического шаблона TS′ для восстановления k, при этом используется полиномиальное преобразование (p_2) и один из кодов исправления ошибок Cod_2.

9. Декодируется МК′′ с помощью нечеткого экстрактора ExtS: k'' = ExtS(k_{SS}, p_2, Cod_2).

10. Формируется хэш-образ извлеченного k'': h(k'').

11. Выполняется проверка равенства: h(k'') == h(k)? Если равенство удовлетворяется, продолжение фазы проверки инициализации, иначе – выход по ошибке.

12. Зашифрование на мастер-ключе k критических параметров и данных, находящихся в секретной памяти (за исключением h(k)).

13. Удаление из секретной памяти k, а также из оперативной памяти: k', k'' и других оперативных критических данных.

Выводы. Достоинствами предложенной схемы аутентификации являются следующие:

1. После фазы проверки инициализации в памяти устройства не сохраняется мастер-ключ и другие критические данные в открытом виде.

2. Фаза аутентификации пользователя на персональном устройстве преимущественно производится с помощью ввода изображения отпечатка пальца (шаги 1–5 фазы верификации, с возможным повтором не более трех раз).

3. В случае сбоя аутентификации на основе отпечатка пальца реализуется запасной вариант – аутентификация на основе парольной фразы. При успешном восстановлении мастер-ключа k, выполняется повторно этап инициализации (шаги 2–4) для восстановления работоспособности аутентификации на основе отпечатка пальца (возможно другого).

4. Для надежности функционирования системы восстановления (так называемой отменяемой биометрии), может быть задействован механизм периодической проверки работоспособности аутентификации на основе парольной фразы.

Если данная верификация дает сбой, выполняется восстановление данного типа аутентификации посредством повторного прохождения этапа инициализации (шаги 5–7) (возможно с другой парольной фразой).

5. Для приложений с повышенными требованиями безопасности может быть реализован режим двухфакторной аутентификации (на основе отпечатка пальца и парольной фразы).

6. Удовлетворяются условия повышенной защищенности от таких атак злоумышленников, как: а) украденное устройство; б) спуффинг атаки; в) атаки грубой силы и пр.

ЛИТЕРАТУРА

1. Kumar N. Cancelable Biometrics: a comprehensive survey / Manisha and Nitin Kumar // Artificial Intelligence Review – 2020. – V. 53. – P. 3403–3446.
2. Mehmood R. Polynomial Based Fuzzy Vault Technique for Template Security in Fingerprint Biometrics / Reza Mehmood, Arvind Selwal //The International Arab Journal of Information Technology. – 2020. – Vol. 17, No. 6. – P. 926–934.
3. Brindha V. Finger Knuckle Print as Unimodal Fuzzy Vault Implementation / V Brindha // Procedia Computer Science. – 2015. – Vol. 47. – P. 205–213.
4. Астапенко, Г. Ф. Использование голоса (речи) для начальной и периодической верификации / Г. Ф. Астапенко, Н. А. Ращеня // Прикладные проблемы оптики, информатики, радиофизики и физики конденсированного состояния: материалы шестой Междунар. науч.-практ. конф. 20–21 мая 2021 г., Минск, М-во образования Респ. Беларусь, НИУ «Ин-т приклад. физ. проблем им. А. Н. Севченко Беларус. гос. ун-та. – 2021. – С. 110–112.