АНАЛИЗ БИОМЕТРИЧЕСКИХ ПОДХОДОВ К УПРАВЛЕНИЮ КЛЮЧЕВОЙ ИНФОРМАЦИЕЙ

Тигран Андреасян
Государственный инженерный университет Армении (Политехник)
Терян 105, Ереван, Армения
e-mail: tandreasyan@gmail.com

АННОТАЦИЯ

Эта статья посвящена биометрическому подходу к управлению ключевой информацией. Рассмотрены методы биометрической аутентификации и выбран наилучший для управления ключевой информацией метод. Проанализированы методы распознавания отпечатков пальцев и предложен новый метод позволяющий улучшить управление ключевой информацией. Предложенный метод не предполагает хранение эталонного отпечатка или ее фрагмента.

Ключевые слова. Ключ, криптография, биометрия, отпечаток пальца, управление ключами.

1. ВВЕДЕНИЕ

Биометрические технологии – основа безопасности там, где точная аутентификация и защищенность от несанкционированного доступа к объектам или данным имеют исключительную важность[1]. В настоящее время биометрические технологии обеспечивают наибольшую гарантию аутентификации личности. Обусловлено это тем, что в отличие от таких методов аутентификации, как пароли, пропуска, всевозможные электронные ключи – человек не может подделать биометрические признаки, потерять, украсть и передать в пользование другому лицу[1]. Есть много биометрических методов для аутентификации, их также можно использовать для управления ключами.

2. ВЫБОР МЕТОДА БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Биометрия – это множество методов и средств идентификации человека, основанных на физиологической или поведенческой его характеристике. Работа всех без исключения систем биометрической идентификации разделяется на две части. Первая – регистрация объекта – с помощью нескольких измерений со считывающего устройства формируется цифровая модель биометрической характеристики (в зависимости от метода: отпечаток пальца, рисунок радужной оболочки глаза и т.д.). Вторая – распознавание объекта – измерения, считанные при попытке идентификации, преобразуются в цифровую форму, которая затем сравнивается с формой, полученной при регистрации[1].

В настоящий момент все существующие методы биометрической идентификации и верификации делятся на две группы: динамические и статические[2]. Статические методы используют физиологические характеристики, а динамические используют поведенческие характеристики личности. Перечислим наиболее распространенные методы.

Статические методы включают:

1. идентификация по отпечатку пальца,
2. идентификация по расположению вен на ладони,
3. идентификация по сетчатке глаза,
4. идентификация по радужной оболочке глаза,
5. идентификация по форме кисти руки,
6. идентификация по форме лица,
7. идентификация по термограмме лица и т.д.

Динамические методы включают:

1. идентификация по голосу,
2. идентификация по почерку,
3. идентификация по клавиатурному почерку.

Все эти методы можно использовать для аутентификации человека, но не все для генерации ключа. Рассмотрим методы, которые можно легко использовать для ключевой информации: отпечаток пальца, лицо, радужная оболочка глаза, голос[3].

Из показателей таблицы 1 видно, что из этих методов наилучшие - отпечатки пальцев и радужная оболочка глаза. А если сравнить аппаратное обеспечение, то аппарат для метода распознавания радужной оболочки глаза дороже и больше по размеру, чем аппарат для метода распознавания отпечатка пальца. И поэтому мы выбрали отпечатки пальца, и в дальнейшем будем работать на ее основе.

3. АНАЛИЗ ТЕХНОЛОГИИ РАСПОЗНАВАНИЯ ОТПЕЧАТКОВ ПАЛЬЦЕВ

Каждый отпечаток обладает определенными признаками, по которым идентифицируют личность. Эти признаки можно разделить на две группы: глобальные и локальные[1]. К глобальным признакам относят те признаки, которые может увидеть глаз (рис.1):

- *Папиллярный узор*.
- *Область образа* - выделенный фрагмент отпечатка, в котором локализованы все признаки.
- *Ядро* - пункт, локализованный в середине отпечатка или некоторой выделенной области.
- *Пункт "дельта"* - начальная точка. Место, в котором происходит разделение или соединение бороздок папиллярных линий, либо очень короткая бороздка (может доходить до точки).
- *Тип линии* - две наибольшие линии, которые начинаются как параллельные, а затем расходятся и огибают всю область образа.
- *Счётчик линий* - число линий на области образа, либо между ядром и пунктом "дельта".

	Отпечатки пальцев	Лицо	Радужная оболочка глаза	Голос
Различающая способность	Высокая	Низкая	Высокая	Низкая
Долговечность	Высокая	Средняя	Высокая	Низкая
Качество сканирования	Среднее	Высокое	Среднее	Среднее
Скорость, эффективность и стоимость соответствующей аппаратуры	Высокая	Низкая	Высокая	Низкая
Готовность человека пройти идентификацию	Средняя	Высокая	Средняя	Высокая
Сложность соответствующей аппаратуры	Высокая	Низкая	Высокая	Низкая
Процент ошибок при положительном результате идентификации	0,4	1,0-2,5	1,1-1,4	5-10
Процент ошибок при отрицательном результате идентификации	0,1	0,1	0,1	2-5

Таблица 1 - эффективность опознания биометрических методов[3]

Локальные признаки, или минуции – признаки, уникальные для каждого отпечатка. Эти признаки определяют пункты изменения паппилярных линий, таких как раздвоение или разрыв, ориентацию паппилярных линий и координаты в этих пунктах[4].

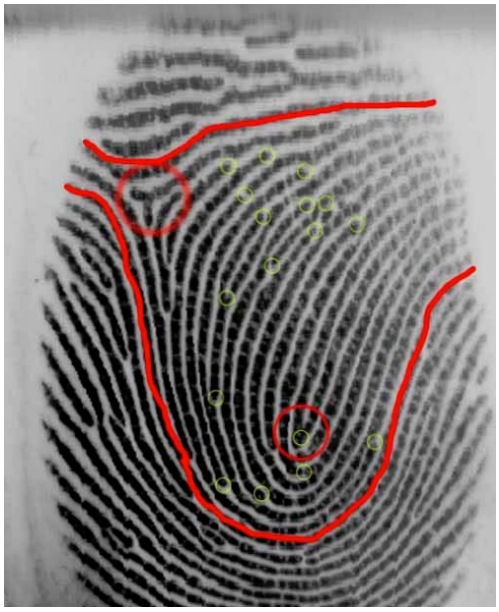

Рис. 1 - Отпечаток пальца

С точки зрения информатики отпечаток пальца это матрица, которую практически невозможно точно повторить. Человек – это живое существо, абсолютно одинаково приложить палец к считывателю не может, само устройство имеет допустимые погрешности ввода, в общем, получаемые матрицы всегда различны. Наша цель использовать их в качестве секретного ключа. Матрицы ведь почти совпадают. Надо как-то нейтрализовать эти погрешности, но таким образом, чтобы сохранить распознавание свой - чужой. И самое главное не хранить эталонный отпечаток, а сделать такую функцию, которая по истинному отпечатку вычисляла бы правильный ключ, а наличие ложного отпечатка не давало бы практически никакой дополнительной информации о ключе. А задача вычисления ключа без истинного отпечатка была бы связана с перебором большого числа вариантов, для которого можно было бы оценить его стойкость.

С помощью такого ключа-отпечатка мы, например, шифруем, индивидуальные секретные ключи пользователя, после чего помещаем их на сервер. Хакер, даже получив доступ к таким зашифрованным ключам, без истинного отпечатка не сможет их восстановить, не осуществляя трудоемкие задачи перебора.

Секретный ключ должен вычисляться по отпечатку пальца в условиях, когда никакой эталонный отпечаток в явном или замаскированном виде в компьютере не хранится.

Есть множество методов распознавания отпечатков пальца, и большинство из них сравнивают с эталоном. Наличие эталонного отпечатка, пусть даже в замаскированном виде, сразу же перечеркивает возможность достижения гарантированной стойкости. Усилия злоумышленника будут направлены не на решение практически неразрешимой переборной задачи, а на добывание эталонного отпечатка. Если эталонный отпечаток найден, то злоумышленник оказывается в тех же условиях, что и законный пользователь.

По этой причине все эти методы, которые сравнивают с эталонным отпечатком, не могут быть применимы для решения поставленной задачи.

4. МЕТОД РАСПОЗНАВАНИЯ ОТПЕЧАТКОВ ПАЛЬЦЕВ БЕЗ ХРАНЕНИЯ ЭТАЛОНА

Если нет эталонного отпечатка, то возможна ли какая-то информация о нем? Нужно найти такую функцию от эталонного отпечатка, с помощью которой при наличии истинного отпечатка можно было бы сравнительно легко вычислить секретный ключ, а при отсутствии истинного отпечатка вычисление ключа потребовало бы трудоемкого перебора,

неосуществимого за реальное время. Открытый “отпечаточный” ключ (информация, которую будем хранить) хранить в сервере или вообще в общедоступном месте в предположении, что потенциальный злоумышленник имеет к нему доступ, а сам эталонный отпечаток нигде не хранить. Тогда истинный пользователь, обладая истинным отпечатком пальца, сумеет вычислить требуемый секретный ключ (конечно, не сам пользователь: за него это сделает программа), а потенциальный злоумышленник, не имея истинного отпечатка пальца, столкнется с неосуществимой задачей.

Разработан новый метод, который решает недостаток выше упомянутых методов (хранение эталонного отпечатка). После сканирования пальца получаем рисунок отпечатка, а из рисунка – матрицу. На матрице отпечатка пальца выделим один фрагмент. Фрагмент - это некоторый ее кусочек, не обязательно квадратный (рис. 2). Например, рассмотрим фрагменты размером n x n ($n < m$) матрицы, размером m x m (m зависит от сканера отпечатка пальца). В нашем примере $m = 128$, $n = 16$.

Рис. 2 - Черным квадратом показан фрагмент.

Попробуем “протащить” выделенный фрагмент по всей матрице (с верхнего левого угла до нижнего правого угла) и посчитать в каждом случае количество несовпадений черно-белых точек (каждый фрагмент со всеми фрагментами). Если все точки совпадают, это значит, что этот показатель равен 0 (это может быть истинное расположение фрагмента), если найдено, например 68 несовпадений, то в этом месте показатель равен 68, и т.д. Когда поиск закончится, берем все несовпадения и отсортируем в порядке убывания. Далее возьмем первые 10 показателей (самые большие несовпадения) и рассчитаем длину между этими фрагментами. Эту информацию сохраним вместо эталонного отпечатка. При распознавании отпечатка будет работать тот же алгоритм, и программа будет сравнивать окончательные цифры (длину между фрагментами), и на основе всей этой информации можно вычислить секретный ключ. Таким образом, у нас есть метод, с которым при наличии истинного отпечатка можно будет легко вычислить ключ, а при отсутствии истинного отпечатка вычисление ключа практически невозможно.

Размер фрагмента n, который мы взяли $n = 16$, неоднозначен. Если взять n меньше, то точность возрастет, но время поиска тоже возрастет, а если n взять больше, то время поиска будет меньше, но снизится точность расчета. Значение можно точно вычислить только опытным путем.

ЗАКЛЮЧЕНИЕ

Таким образом, в статье рассмотрены биометрические методы для управления ключевой информацией. Взяли в основу отпечатки пальца, сделали анализ по существующим методам распознавания отпечатка пальца и предложили новый метод, который основывается на хранении расстояний между фрагментами с наибольшими отличиями, что и поможет нам поднять управление ключами на новый уровень.

ЛИТЕРАТУРА

[1] S. Nanavati. Biometrics- Identity Verification in a Networked World. *John Wiley & Sons, Inc.* New York, 2002.

[2] Ю. Судаков. Биометрическая аутентификация: обзор динамических методов. *МФТИ*. Ст. 4, Москва, 2007

[3] Ежемесячный научно-информационный журнал. В мире науки. *ООО ИД «Медиа-Пресса»*. Ст. 52, Москва, 12-2008.

[4] Wikipedia. http://wiki.oszone.net/index.php/Биометрия._Отпечаток_оальца