ИССЛЕДОВАНИЕ МЕТОДОВ ГЕНЕРАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ ДЛЯ КРИПТОСИСТЕМ С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКИХ ПАРАМЕТРОВ ПОЛЬЗОВАТЕЛЯ

С.А. Барашков, Д.Н. Лясин

Волжский политехнический институт (филиал) ВолгГТУ

В современном мире быстро развивается информационная составляющая общества и большая часть информации требует надежной защиты. На данный момент защита с использованием биометрических параметров пользователя является самой эффективной. Сфера применения биометрических параметров очень широка, как для защиты информации, так и для повышения удобства работы с ней. Но в основном биометрические параметры сейчас используются для аутентификации. Биометрические параметры можно использовать не только для аутентификации, но и в криптографии, для формирования ключа шифрования. Удобство этого метода в том, что этот ключ невозможно потерять и он всегда у пользователя при себе.

Как таковых систем генерации ключевой информации по биометрическим параметрам не существует, существуют системы аутентификации по биометрическим параметрам такие как: «BioLink», «ProSoft Systems», «Anviz», «Sagem», «ZKSoftware», «SONDA Technologies». Однако, их недостатком является направленность на аутентификацию.

На отпечатке пальца можно выделить два типа характеристических точек – разветвление и окончание. Схематично эти точки изображены на *рисунке 1*. После поступления изображения отпечатка начинается его обработка и поиск этих характеристических точек. Распознав тип точки, запоминается ее координата на матрице изображения. Эта информация заносится в массив $Points_i = \{x_i, y_i, type_i, krsort_i\}$, где x_i, y_i – координаты точки на матрице изображения, $type_i$ – тип характеристической точки, $krsort_i$ – критерий сортировки [2].

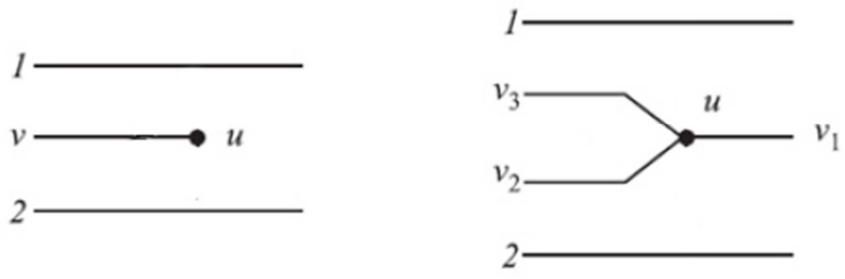

Рисунок 1 – Типы характеристических точек

Тип характеристической точки определяется количеством соседних пикселей того же цвета в окрестностях одного пикселя, *count* – переменная в которой ведется подсчет таких точек. Заполнение переменной типа характеристической точки: $type_i = \begin{cases} 1111, \text{если } count = 1 \\ 1010, \text{если } count = 3 \end{cases}$, 1111 – окончание, 1010 – разветвление. Человек не может всегда прикладывать для сканирования отпечаток пальца точно так же как и в первый раз, поэтому нужно как-то зафиксировать набор характеристических точек. Для этого используется критерий сортировки, он считается после того, как все характеристические точки распознаны и найдены соответствующие им координаты, для каждой точки рассчитывается сумма расстояний до всех характеристических точек. Расчет этого критерия происходит следующим образом: $krsort_i = \sum_{m=0}^{n} \sqrt{(x_i - x_m)^2 + (y_i - y_m)^2}$, где $m \epsilon [0, i) \cup (i, n]$. Получив это значение происходит сортировка массива $Points = sort_{krsort}(Points)$ по возрастанию. Для получения ключа шифрования используется функция хеширования данных $Key = HASH(type_0 \oplus type_1 \oplus \dots \oplus type_{n-1} \oplus type_n)$. В результате мы получаем ключ шифрования, который можно использовать для шифрования и дешифрования данных [1].

На основании проведенного исследования разработана программа, способная выполнять функции системы генерации ключевой информации. Основной задачей программы создание ключа по биометрическому параметру, который в дальнейшем будет использоваться в криптосистемах с симметричным ключом шифрования. Проведенные опыты показали постоянство получения ключа не зависимо от условий подачи входного изображения. Варьировался угол поворота входных данных и масштаб.

Список литературы:

1. Гудков В.Ю. Математические модели изображения отпечатка пальца на основе описания линий // Информатика и ее применения – 2010. – Т.4. Вып. 1. – С. 58-64
2. Трошков М.А. База создания ключей для несимметричной системы шифрования на основе многофакторных биометрических характеристик // INTERMATIC – 2010. – часть 3. – С. 251-253.