Андреев Д. Ю.

Проявление разрядов кодового отклика преобразователя биометрия-код из выходного шума при условии наблюдения расстояния Хэмминга

Определим условия рассматриваемой задачи следующим образом. Пусть для любой кодовой комбинации на выходе преобразователя биометрия-код мы можем узнать расстояние Хэмминга до ключа. Требуется найти ключ, либо уменьшить неопределенность поиска и свести задачу к перебору значений, уменьшив при этом трудоемкость перебора по отношению к полному перебору всех значений.

Для решения задачи предлагается использовать две процедуры, названные «процедурой формирования матрицы» и «процедурой проявки ключа».

Процедура формирования матрицы служит для формирования так называемой «матрицы ключей» - для поиска и накопления кодовых комбинаций, близких к ключу (имеющих небольшое расстояние Хэмминга до ключа).

Процедура «проявки ключа» служит для «проявления» значений разрядов ключа с помощью усреднения значений соответствующих разрядов кодовых комбинаций из матрицы.

Исходя из предположения о случайности выходных кодовых комбинаций, можно сделать заключение о нормальности закона распределения расстояний Хэмминга между произвольно взятой кодовой комбинацией на выходе преобразователя и ключом, причем математическое ожидание расстояния Хэмминга между произвольной кодовой комбинацией и ключом равно половине максимального значения расстояния Хэмминга (равного длине ключа).

В соответствии с определением расстояния Хэмминга, кодовая комбинация с расстоянием Хэмминга, равным нулю, будет совпадать с ключом, а кодовая комбинация с расстоянием Хэмминга, равным длине ключа – с инверсией ключа. Соответственно, по мере увеличения расстояния Хэмминга между ключом и произвольной кодовой комбинацией от нуля до значения, равного математическому ожиданию, число совпадающих бит уменьшается. Симметричная картина, с учетом произведенной инверсии кодовой комбинации, будет наблюдаться при уменьшении расстояния Хэмминга от максимального значения до значения, равного математическому ожиданию.

Таким образом, близость кодовой комбинации к ключу будет убывать по мере приближения расстояния Хэмминга к значению, равному математическому ожиданию, а затем, с учетом инверсии кодовой комбинации, снова увеличиваться по мере приближения к максимальному значению расстояния Хэмминга. Кодовые комбинации с расстоянием Хэмминга, равным нулю и длине ключа, совпадают (с учетом инверсии) с

ключом, кодовая комбинация с расстоянием Хэмминга, равным половине длины ключа, не несет никакой информации о ключе (угадана ровно половина разрядов).

Получаем, что при увеличении отклонения значения расстояния Хэмминга от математического ожидания кодовые комбинации будут иметь большую близость к ключу, и, как следствие, понадобится меньшее их количество для восстановления ключа с заданной точностью при помощи усреднения. Однако, так как расстояния Хэмминга генерируемых случайных чисел располагаются в соответствии с нормальным законом, на поиск подходящих элементов при этом будет затрачиваться большее время.

В данном алгоритме задается некоторое пороговое значение близости - величина минимального отклонения меры Хэмминга от центрального значения (см. рисунок 1) Для проявления ключа используются только те кодовые комбинации, для которых расстояние Хэмминга до ключа удалено от математического ожидания на величину, большую заданного порогового значения, причем кодовые комбинации с расстоянием Хэмминга, большим математического ожидания, инвертируются.

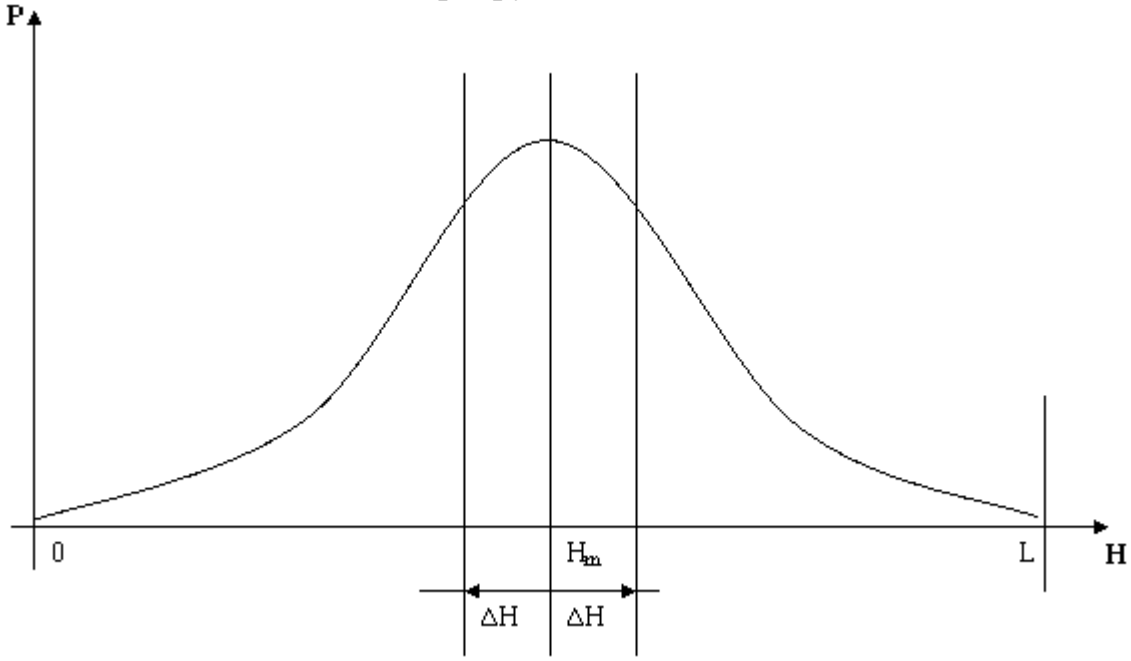

Рисунок 1 – Выбор случайных значений для проявления ключа

На рисунке:

H – расстояние Хэмминга;

P – вероятность появления случайной кодовой комбинации с заданным расстоянием Хэмминга;

L – длина ключа в битах;

H_m – математическое ожидание расстояния Хэмминга множества генерируемых случайных значений (равное L/2);

ΔH – пороговое значение отклонения расстояния Хэмминга.

Суть процедуры формирования матрицы в следующем.

Генерируется случайное длинное число одинаковой с ключом размерности.

В случае, если расстояние Хэмминга меньше центрального отклонения на величину, большую порогового значения, число заносится в матрицу.

В случае, если расстояние Хэмминга превышает центральное отклонение на величину, большую порогового значения, число инвертируется и заносится в матрицу.

Производится генерация следующего числа и повтор процедуры.

При достижении некоторого числа элементов в матрице (в ходе реализации алгоритма число элементов в матрице ограничивалось максимальным временем работы процедуры) производится переход к процедуре «проявки» ключа.

Процедура «проявки ключа» заключается в следующем.

Каждый разряд проявляемого ключа устанавливается в значение, совпадающее с наибольшим количеством соответствующих разрядов элементов матрицы.

Было проведено два эксперимента для различных генераторов псевдослучайных чисел.

В первом случае в качестве генератора кодовых комбинаций использовался стандартный генератор операционной системы Microsoft Windows, доступный при помощи функции rand_s ().

Тестовые исследования реализации вышеприведенного алгоритма, произведенные на ЭВМ с процессором тактовой частотой 900 МГц, дали результаты, представленные графически на рисунке 2. При этом время тестирования составило около 10 секунд. Линии на графике отображают зависимость нормированного количества совпавших бит проявленного ключа от размера матрицы ключей для радиуса области неучитываемых бит соответственно в 4 (нижняя кривая), 8, 12 и 16 (верхняя кривая) бит.

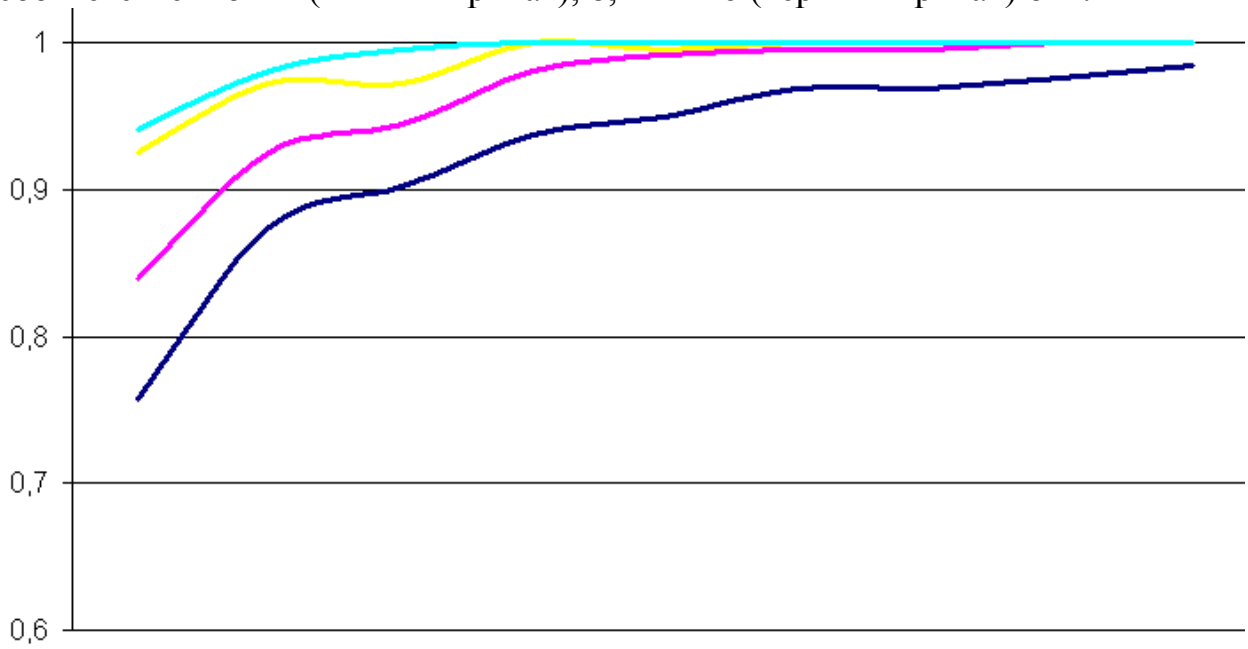

Рисунок 2 – Результаты работы первой реализации алгоритма

Во втором случае в качестве генератора кодовых комбинаций использовалась нейронная сеть, обученная для преобразования биометрических параметров оператора в ключ. Исследования, произведенные на той же платформе, дали результаты, представленные графически на рисунке 3. При этом время тестирования составило около 180 секунд.

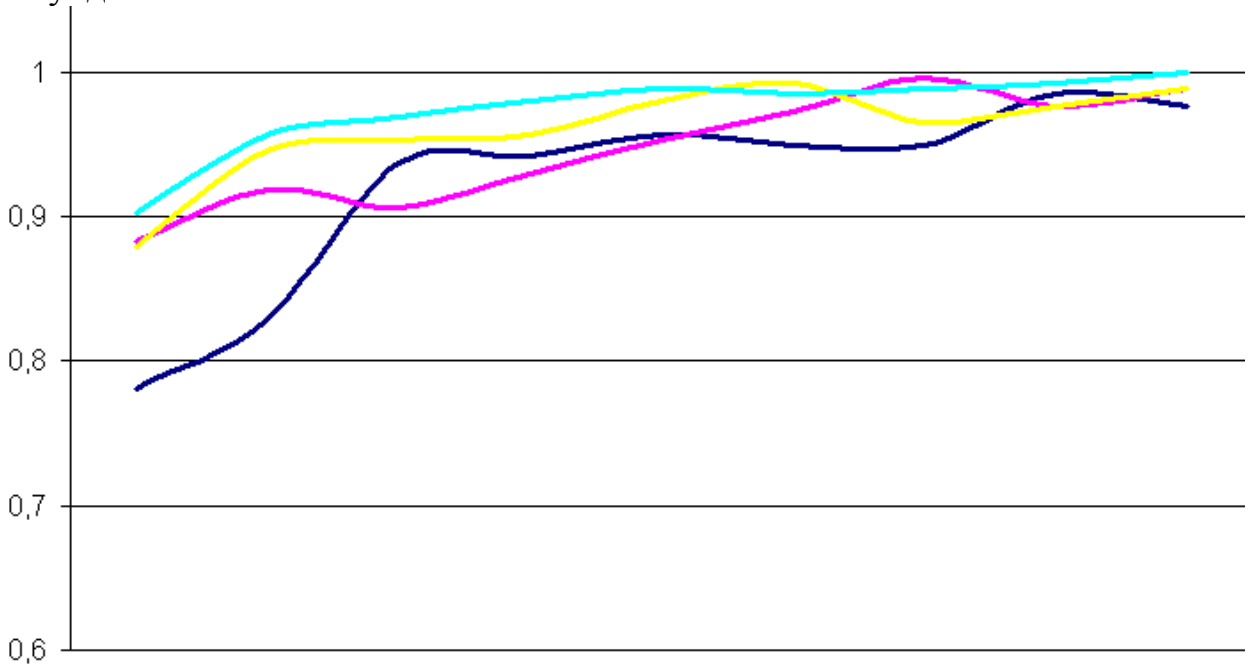

Рисунок 3 – Результаты работы второй реализации алгоритма

Данные, полученные при тестировании, доказывают, что на платформе стоимостью менее 500 $ на сегодняшний день возможно восстановление ключа за несколько секунд.

Сравнивая результаты тестирования различных реализаций атак, можно судить о том, что нейросетевые преобразователи биометрия-код не имеют явных грубых уязвимостей, связанных с неравномерностью распределения случайных выходных значений. Также данные тестирования позволяют судить о том, что на современных ЭВМ общего применения, не предназначенных для выполнения высокопараллельных задач, использование нейронных сетей дает выигрыш около двадцати раз в стойкости к атакам поиска ключа за счет вычислительной сложности.

Приведенный выше алгоритм является наиболее простым и очевидным решением поставленной задачи. Очевидно, что существуют более быстродействующие способы решения, однако, данный алгоритм представляется максимально обобщенным, что позволяет видоизменять его для других возможных вариантов постановки задачи.