Метод надежного хранения биометрических данных на пространственно-распределенных хранилищах

Ю.Н. Кочеров, Э.Е. Тихонов, Д.В. Самойленко

Невинномысский Технологический Институт (филиал) федерального государственного автономного образовательного учреждения высшего образования «Северо-Кавказский федеральный университет»

Аннотация: В статье приведен обзор некоторых методов идентификации личности на основе ее биометрических данных, а также основные принципы реализации этих методов. Также предложен метод надежного хранения биометрических данных на удаленных пространственно-распределенных хранилищах с применением алгоритмов, основанных на системе остаточных классов.
Ключевые слова: методы идентификации, биометрические идентификаторы, система остаточных классов, схемы разделения данных.

Введение

Биометрия вошла в наш обиход, и ее значимость уже почти ни у кого не вызывает сомнений. Все чаще используется биометрическая идентификация, биометрические сканеры.

Под термином биометрические технологии понимаются способы идентификации личности человека по некоторым его биологическим характеристикам.

Любая система контроля и управления доступом (СКУД), основанная на фиксации биометрических данных, состоит из считывающего прибора, позволяющего измерять биометрические характеристики, и алгоритма сравнения полученных биологических характеристик.

В связи с вышесказанным возникает такая насущная проблема, как безопасное хранения биометрических данных человека. Для этого возможно использовать как криптографические, так и некриптографические методы защиты информации. Одним из перспективных методов защиты информации является метод, основанный на пороговом разделении информации.

Алгоритмы сравнения отпечатков пальца

Выделяют три метода идентификации по папиллярному узору:

1) Метод корреляционного сравнения. Суть этого метода заключается в последовательном накладывании изображения, полученного со сканера папиллярного узора на образцы из хранилища информации, и расчета различий между ними.

2) Сравнение по минуциям. Алгоритм по снимкам папиллярного узора формирует плоскость, на которой выделяются минуции (участки папиллярного рисунка кожи, где отдельные линии сливаются, раздваиваются или обрываются). При сравнении оценивается плоскость с выделенными особыми точками и плоскости из хранилища информации. Преимуществом такого алгоритма является скорость работы.

3) Папиллярный узор разбивается на части. Узор в каждой части описывается функцией синуса со своими параметрами, такими как: сдвиг по фазе, частота и амплитуда. Этот алгоритм не требует изображения с высоким разрешением.

Обзор схем разделения данных

Схема разделения данных – криптографическая схема, позволяющая разделить информацию между участниками группы, при этом каждый участник получает ее долю, а исходная информация стирается. Воссоздать информацию может определенная коалиция участников.

Схемы разделения данных подразделяют на идеальную и совершенную.

Схемы разделения данных, в которой доли информации любого запрещенного множества содержат в совокупности нулевую информацию о значении информации, называют совершенными.

Схема разделения данных называется идеальной, если размер части информации равен размеру самой информации.

Среди схем разделения данных особое место занимают схемы, основанные на системе остаточных классов [1–4] (СОК), среди которых выделяются схема Миньотта и схема Асмута-Блума.

Описание схемы Миньота

Схема Миньотта [5] – пороговая схема разделения информации, построенная с применением ряда простых чисел [2]. Позволяет разделить информацию между n участниками схемы обмена данными таким образом, что их могут восстановить любые k участников, но $k-1$ восстановить секрет уже не смогут.

В основе схемы лежит использование (СОК), которая позволяет пользователям, имеющим некоторую часть информации, восстановить ее, причём единственным образом. Рассмотрим обобщенную СОК: пусть $n \ge k$, $p_1, p_2, ..., p_n$, $b_1, b_2, ..., b_n \in Z$. Тогда система уравнений:

$$\begin{cases} x \equiv b_1 \bmod(p_1) \\ x \equiv b_2 \bmod(p_2) \\ ... \\ x \equiv b_n \bmod(p_n) \end{cases}$$

имеет решения в Z тогда и только тогда, когда $b_i \equiv b_j \bmod(m_i, m_j) \forall 1 \le i, j \le n$. Более того, если приведенная система имеет решения в Z, она имеет единственное решение в $Z_{[p_1, p_2, ..., p_n]}$, $[p_1, p_2, ..., p_n]$ определяет наименьшее общее кратное $p_1, p_2, ..., p_n$. В случае, если $(m_i, m_j) = 1 \forall 1 \le i < j \le n$ СОК называют стандартной.

В схеме разделения данных Миньотта применяются специальные ряды чисел, так называемые последовательности Миньотта. Пусть n – целое, такое что $n \ge 2$, $2 \le k \le n$. Тогда (k, n)-последовательность взаимно простых положительных чисел $p_1 < p_2 < ... < p_n$, что $\prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i$. Это утверждение также равносильно следующему $\max_{1 \le i_1 < ... < i_{k-1} \le n} (p_{i_1}, ..., p_{i_{k-1}}) < \min_{1 \le i_1 < ... < i_k \le n} (p_{i_1}, ..., p_{i_k})$.

Разделение информации происходит следующим образом:

1) информация A это целое число, такое, что $\beta < S < \alpha$, где $\alpha = \prod_{i=1}^{k} p_i$, $\beta = \prod_{i=0}^{k-2} p_{n-i}$. То есть информация должна находиться в промежутке $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ и $p_{n-k+2} \cdot \ldots \cdot p_n$;

2) части вычисляются следующим образом: $\alpha_i = S \bmod(p_i)$, для всех $1 \le i \le n$;

3) имея k различных частей $\alpha_1, \ldots, \alpha_k$, можно получить исходную информацию S, используя стандартный вариант китайской теоремы об остатках (КТО) – им будет единственное решение по модулю $p_1, p_2, \ldots, p_k$ системы:

$$\begin{cases} S \equiv \alpha_1 \bmod(p_1) \\ S \equiv \alpha_2 \bmod(p_2) \\ \ldots \\ S \equiv \alpha_n \bmod(p_n) \end{cases}.$$

То есть S можно однозначно восстановить по его остаткам от деления на $p_1, p_2, \ldots, p_k$. Основными способами решения такой системы являются методы, основанные на КТО, Обобщенной полиадической системе (ОПСС), либо совместным применением КТО и ОПСС.

Другой метод разделения данных – это схема Асмута-Блума.

Описание схемы Асмута-Блума

Схема Асмута-Блума [6] – пороговая схема разделения информации, построенная с применением ряда простых чисел. Позволяет разделить информацию между n пользователями таким образом, что его смогут восстановить любые k участников.

В основе этой схемы также лежит использование СОК.

Разделение информации происходит следующим образом:

1) пусть S — некоторая информация, которую необходимо разделить среди участников. Принимается такое простое число q, значение выше S. Принимается ряд из n взаимно простых друг с другом чисел $p_1, p_2, ..., p_k$ таких, что:

– $\forall i : p_i > q$;

– $\forall i : p_i > p_{i+1}$;

– $p_1 \cdot p_2 \cdot ... \cdot p_k > q \cdot p_{n-k+2} \cdot p_{n-k+3} \cdot ... \cdot p_n$

2) генерируете число r и вычисляется $S^{'} = S + q \cdot r$.

3) по формуле $\alpha_i = S^{'} \bmod(p_i)$ рассчитываются части.

4) участникам раздаются $\{q, p_i, \alpha_i\}$.

5) Информация восстанавливается методами, описанными в предыдущем примере.

Из вышесказанного можно сделать вывод, что схема Асмута-Блума является как совершенной, так и идеальной. Поэтому в работе будет применяться она.

Применение схемы Асмута-Блума для разделения биометрических данных

Как говорилось ранее, одним из перспективных алгоритмов сравнения отпечатков пальцев является сравнение по минуциям.

Минуция – это особая точка папиллярного узора, где линии имеют разрыв либо разветвление. Из рассмотренных особых точек могут быть более сложные виды минуций (Рис. 1).

Рис. 1 – Примеры Минуций

Часто используемым алгоритмом сравнения папиллярного узора является метод корреляционного сравнения. Сравнение папиллярных узоров происходит путем многократного сравнения множеств минуций. При проведении процедуры сравнения попарно оцениваются особые точки рисунка из базы данных отсканированного рисунка. В области каждой из минуций проводится поиск особых точек другого отпечатка. Если расстояние между ними является допустимым, то эти особые точки считаются совпавшими. В качестве критерия оценивания близости двух отпечатков пальцев принимается количество пар из минуций, признанных совпавшими. На рис. 2 представлен пример измерения расстояния между некоторыми минуциями.

Рис. 2 – Расстояние между некоторыми минуциями

Поэтому для хранения биометрических данных человека достаточно хранить координаты минуций либо матрицу расстояний между ними.

При использовании схемы Асмута-Блума предлагается передавать на удаленные пространственно-распределенные хранилища данных вычеты координат минуций по заранее заданным основаниям.

Это позволит исключить доступ злоумышленника к частным биометрическим данным, а также восстановить биометрические данные в случае их частичной потери.

Пример реализации алгоритмов

Рассмотрим алгоритм вычисления расстояний между некоторыми минуциями.

Для этого рассмотрим некоторое изображение отпечатка пальца, имеющее разрешение 756x1252.

1) Выделим некоторые минуции и обозначим их точками A, B, C, D.

2) Вычислим координаты этих точек: $A(291,921)$, $B(326,895)$, $C(162,633)$, $D(367,200)$ (Рис. 3).

Рис. 3 –точки для вычисления расстояний

3) Рассчитаем квадраты расстояний между выделенными точками:

– расстояние $AB^2 = (291-326)^2 + (921-895)^2 = 1901$;

– расстояние $AC^2 = (291-162)^2 + (921-633)^2 = 99585$;

– расстояние $AD^2 = (291-367)^2 + (921-200)^2 = 525617$;

– расстояние $BC^2 = (326-162)^2 + (895-633)^2 = 95540$;

– расстояние $BD^2 = (326-367)^2 + (895-200)^2 = 484706$;

– расстояние $CD^2 = (367-162)^2 + (200-633)^2 = 229514$.

Рассмотрим алгоритм (k,n) пространственного разделения координат для $k=3$ и $n=5$. Так как изображение имеет разрешение 756x1252, то S – максимально-возможная координата, следовательно, $S=1252$. Из условий следует, что q –простое число и $q>S$ примем $q=1259$ [7–9].

Из условий: $\forall i: p_i < p_{i+1}$ и $p_1 \cdot p_2 \cdot \ldots \cdot p_k > q \cdot p_{n-k+2} \cdot p_{n-k+3} \cdot \ldots \cdot p_n$ примем $p_1=1277$, $p_2=1279$, $p_3=1283$, $p_4=1289$, $p_5=1291$.

По формуле $(S+rq) \bmod p_i$, где S – координата точки, разделим координаты точек: $\alpha A_1=(614,1244)$; $\alpha A_2=(510,1140)$; $\alpha A_3=(302,932)$; $\alpha A_4=(1279,620)$; $\alpha A_5=(1177,516)$; $\alpha B_1=(649,1218)$; $\alpha B_2=(545,1114)$; $\alpha B_3=(337,906)$; $\alpha B_4=(25,594)$; $\alpha B_5=(1212,490)$; $\alpha C_1=(485,956)$; $\alpha C_2=(381,852)$; $\alpha C_3=(173,644)$; $\alpha C_4=(1150,332)$; $\alpha C_5=(1048,228)$; $\alpha D_1=(690,523)$; $\alpha D_2=(586,419)$; $\alpha D_3=(378,211)$; $\alpha D_4=(66,1188)$; $\alpha D_5=(1253,1086)$.

Восстановить информацию можно, применив КТО, ОПСС, и совместное использование КТО и ОПСС [7,8,10].

Рассмотрим пример восстановления информации с использованием КТО:

1) Преобразуем код числа S, заданного в системе остаточных классов, в позиционную систему счисления. Это можно осуществить в соответствии с выражением:

$$S = \left(\sum_{i=1}^{n} \alpha_i \beta_i\right) \bmod(P).$$

2) Для расчета ортогональных базисов найдем величины P_i, тогда: $P = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5$, а: $P_1 = \frac{P}{p_1} = 2730714902743$; $P_2 = \frac{P}{p_2} = 2726444824709$; $P_3 = \frac{P}{p_3} = 2717944607017$; $P_4 = \frac{P}{p_4} = 2705293196899$; $P_5 = \frac{P}{p_5} = 2701102192721$.

3) Из приближения $(m_i P_i) \bmod (p_i) \equiv 1$ найдем веса базисов: $m_1 = 1061$; $m_2 = 425$; $m_3 = 950$; $m_4 = 950$; $m_5 = 475$

4) Далее вычислим сами базисы $\beta_i = m_i \cdot P_i$:

– $\beta_1 = 1061 \cdot 2730714902743 = 2897288511810323$;

– $\beta_2 = 425 \cdot 2726444824709 = 1158739050501325$;

– $\beta_3 = 950 \cdot 2717944607017 = 2582047376666150$;

– $\beta_4 = 950 \cdot 2705293196899 = 2540270311888161$;

– $\beta_5 = 475 \cdot 2701102192721 = 1283023541542475$;

Подставив разделенные данные, а также рассчитанные значения β_i и P в выражение $S = (\sum_{i=1}^{n} \alpha_i \beta_i) \bmod (P)$, получим исходные координаты точек $A(291,921)$, $B(326,895)$, $C(162,633)$, $D(367,200)$.

Литература

1. Эрдниева Н. С., Использование системы остаточных классов для маломощных приложений цифровой обработки сигналов. // Инженерный вестник Дона, 2013, №2. URL: ivdon.ru/magazine/archive/n2y2013/1621.

2. Бабенко М. Г., Вершкова Н. Н., Кучеров Н. Н., и Кучуков В. А. Разработка генератора псевдослучайных чисел на точках эллиптической кривой // Инженерный вестник Дона, 2012, №4, ч.2. URL: ivdon.ru/magazine/archive/n4p2y2012/1408.

3. Кочеров Ю. Н. и Червяков Н. И., Разработка методов и алгоритмов разделения и восстановления данных в модулярных пороговых структурах для распределенных вычислительных сетей. Ставрополь: Северо-Кавказский федеральный университет, 2016 г., 236 с.

4. Krasnobaev V., Koshman S., Kononchenko A., Kuznetsova K., and Kuznetsova T., The Formulation and Solution of the Task of the Optimum Reservation in the System of Residual Classes, in 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), dec. 2019, pp. 1–4, doi: 10.1109/ATIT49449.2019.9030483.

5. Mignotte M., How to Share a Secret, в Cryptography, mar. 1982, pp. 371–375, doi: 10.1007/3-540-39466-4_27.

6. Asmuth C. and Bloom J., A modular approach to key safeguarding, IEEE Trans. Inf. Theory, T. 29, vol. 2, pp. 208–210, mar. 1983, doi: 10.1109/TIT.1983.1056651.

7. Goldreich O., Ron D., and Sudan M., Chinese remaindering with errors, IEEE Trans. Inf. Theory, T. 46, vol. 4, pp. 1330–1338, jul. 2000, doi: 10.1109/18.850672.

8. Kocherov Y. N., Samoylenko D. V., and Koldaev A. I., Development of an Antinoise Method of Data Sharing Based on the Application of a Two-Step-Up System of Residual Classes, in 2018 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), oct. 2018, pp. 1–5, doi: 10.1109/FarEastCon.2018.8602764.

9. Krasnobaev V., Popenko V., Kuznetsova T., and Kuznetsova K., Examples of Usage of Method of Data Errors Correction which are Presented by the Residual Classes, in 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), dec. 2019, pp. 45–50, doi: 10.1109/ATIT49449.2019.9030512.

10. Iftene S., General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting, Electron Notes Theor Comput Sci, T. 186, pp. 67–84, jul. 2007, doi: 10.1016/j.entcs.2007.01.065.

References

1. Erdnieva N. S. Inzhenernyj vestnik Dona, 2013, №2. URL: ivdon.ru/magazine/archive/n2y2013/1621.

2. Babenko M. G., Vershkova N. N., Kucherov N. N., i Kuchukov V. A. Inzhenernyj vestnik Dona, 2012, №4, ch.2. URL: ivdon.ru/magazine/archive/n4p2y2012/1408.

3. Kocherov Y. N. i CHervyakov N. I., Razrabotka metodov i algoritmov razdeleniya i vosstanovleniya dannyh v modulyarnyh porogovyh strukturah dlya raspredelennyh vychislitel'nyh setej [Development of methods and algorithms for data separation and recovery in modular threshold structures for distributed computing networks], Stavropol': Severo-Kavkazskij federal'nyj universitet, 2016 g., 236 p.

4. Krasnobaev V., Koshman S., Kononchenko A., Kuznetsova K., and Kuznetsova T., The Formulation and Solution of the Task of the Optimum Reservation in the System of Residual Classes, in 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), dec. 2019, pp. 1–4, doi: 10.1109/ATIT49449.2019.9030483.

5. Mignotte M., How to Share a Secret, в Cryptography, mar. 1982, pp. 371–375, doi: 10.1007/3-540-39466-4_27.

6. Asmuth C. and Bloom J., A modular approach to key safeguarding, IEEE Trans. Inf. Theory, T. 29, vol. 2, pp. 208–210, mar. 1983, doi: 10.1109/TIT.1983.1056651.

7. Goldreich O., Ron D., and Sudan M., Chinese remaindering with errors, IEEE Trans. Inf. Theory, T. 46, vol. 4, pp. 1330–1338, jul. 2000, doi: 10.1109/18.850672.

8. Kocherov Y. N., Samoylenko D. V., and Koldaev A. I., Development of an Antinoise Method of Data Sharing Based on the Application of a Two-Step-Up System of Residual Classes, in 2018 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), oct. 2018, pp. 1–5, doi: 10.1109/FarEastCon.2018.8602764.

9. Krasnobaev V., Popenko V., Kuznetsova T., and Kuznetsova K., Examples of Usage of Method of Data Errors Correction which are Presented by the Residual Classes, in 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), dec. 2019, pp. 45–50, doi: 10.1109/ATIT49449.2019.9030512.

10. Iftene S., General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting, Electron Notes Theor Comput Sci, T. 186, pp. 67–84, jul. 2007, doi: 10.1016/j.entcs.2007.01.065.