МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
САНКТ-ПЕТЕРБУРГ
04 марта 2020

ГУАП Государственный университет аэрокосмического приборостроения

ДНИТ Красноярский ДОМ НАУКИ И ТЕХНИКИ

Метрологическое обеспечение инновационных технологий»
«Metrological Support of Innovative Technologies»
ICMSIT-2020

«КОНЦЕПЦИЯ РАЗВИТИЯ БИОМЕТРИЧЕСКИХ СИСТЕМ НА ОСНОВЕ СОВРЕМЕННЫХ СРЕДСТВ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ »

Гладких А.А. д.т.н., профессор, профессор УИ ГА
Волков Ал.К. к.т.н., доцент УИ ГА
Волков Ан.К. старший преподаватель УИ ГА
Саид Б. А. С. аспирант УлГТУ
Юдаев В.В. старший преподаватель УИ ГА

ICMSIT-2020 Metrological Support of Innovative Technologies

ICMSIT-2020 Метрологическое обеспечение инновационных технологий

Актуальность - к обработке сведений цифровой экономики могут быть приняты безусловно достоверные данные и только от легитимных пользователей, что обеспечивается применением биометрических систем, инновационная концепция развития которых базируется на современных средств помехоустойчивого кодирования.

Целью данной работы является развитие новых эффективных алгоритмов помехоустойчивого кодирования в биометрических системах, в наибольшей степени отвечающих современным вызовам.

Для достижения поставленной цели решены следующие задачи:

- дана классификация биометрических систем с учетом их метрологических возможностей при работе в реальном времени;

- показаны возможности биометрии в системе формирования данных криптографических систем с открытым ключом и использованием средств помехоустойчивого кодирования для минимизации ошибок первого рода в ходе восстановления биометрических данных;

- предложена система последовательного турбокодирования с использованием кодека полярного кода и недвоичного избыточного кода при обработке последних методом перестановочного декодирования с использованием когнитивных принципов.

ПРИНЦИП ПОСТРОЕНИЕ КОДОВОГО ВЕКТОРА В СИСТЕМЕ ПОЛЯРНОГО КОДИРОВАНИЯ

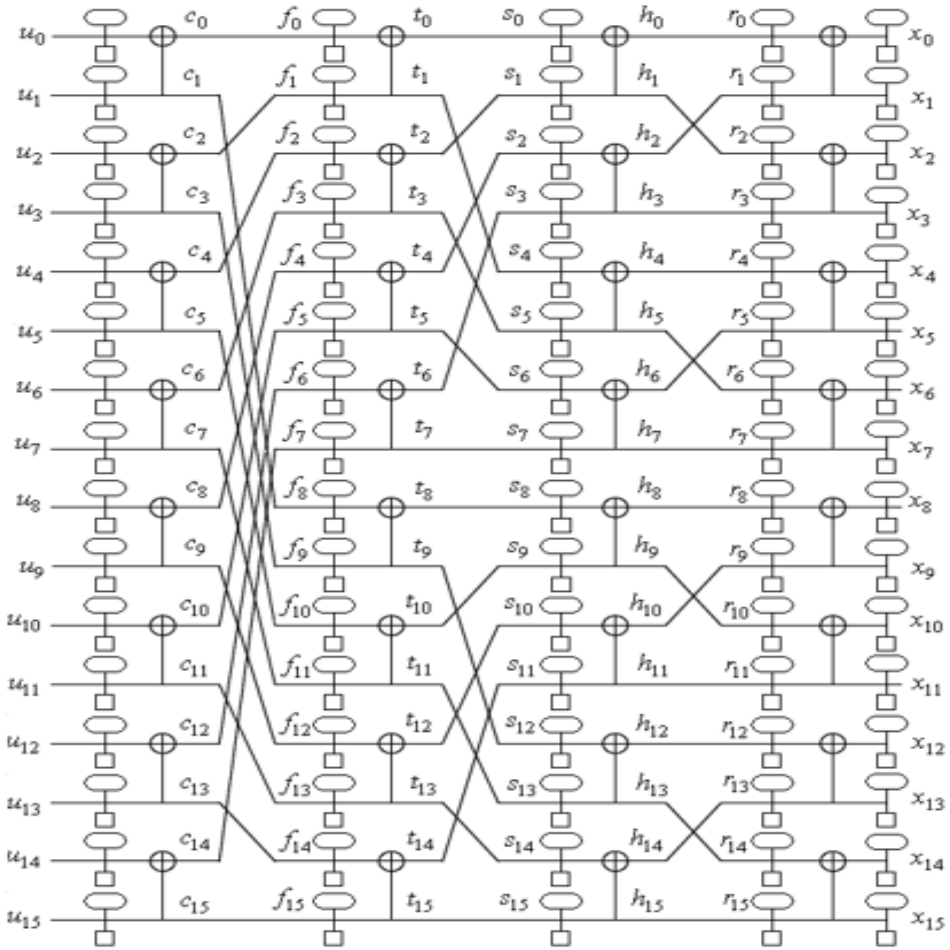

Рис. 1. Функциональная схема формирования кодового вектора полярного кодирования

Оценка параметра Бхаттачария

число перестановок

$$M = m - 1$$

число уровней расчета

$$L = m$$

1 уровень расчета

$$\begin{cases} Z_{r2i} = 2 \cdot Z_{\varepsilon} - Z_{\varepsilon}^{\,2} \\ Z_{r2i-1} = Z_{\varepsilon}^{\,2} \end{cases}$$

2 уровень расчета

$$\begin{cases} Z'_{s2i} = 2 \cdot Z_{h2i} - Z_{h2i}^{\,2}, для\ i = 2j \\ Z_{s2i} = 2 \cdot Z_{h2i-1} - Z_{h2i-1}^{\,2}, для\ i = 2j+1 \\ Z'_{s2i-1} = Z_{h2i}^{\,2}, для\ i = 2j-1 \\ Z_{s2i-1} = Z_{h2i-1}^{\,2}, для\ i = 2j \end{cases}$$

4 уровень расчета

$$\begin{cases} Z_{u2i} = Z_{f_i}, для\ i = j \\ Z_{u2i-1} = Z_{f_{i+7}}, для\ i = j \end{cases}$$

3 уровень расчета

$$\begin{cases} Z^1_{f2i} = 2 \cdot Z_{t2i} - Z_{t2i}^{\,2}, для\ i = 4j \\ Z^2_{f2i} = 2 \cdot Z_{t2i-1} - Z_{t2i-1}^{\,2}, для\ i = 4j+1 \\ Z^3_{f2i} = 2 \cdot Z_{t2i-2} - Z_{t2i-2}^{\,2}, для\ i = 4j+2 \\ Z^4_{f2i} = 2 \cdot Z_{t2i-3} - Z_{t2i-3}^{\,2}, для\ i = 4j+3 \\ Z^1_{f2i-1} = Z_{t2i-1}^{\,2}, для\ i = 4j \\ Z^2_{f2i-1} = Z_{t2i}^{\,2}, для\ i = 4j-1 \\ Z^3_{f2i-1} = Z_{t2i+1}^{\,2}, для\ i = 4j-2 \\ Z^4_{f2i-1} = Z_{t2i+2}^{\,2}, для\ i = 4j-3 \end{cases}$$

В общем виде процедура перестановочного декодирования представляется выражением:

$$PD = \begin{cases} Rn(t) = I(t) + Er(t); \\ Dn = P(t), \end{cases} \Big|_{\max_{S_1;S_2;S_3}},$$

где $I(t)$, $Er(t)$ – стохастические факторы;

$P(t)$ – детерминированная составляющая, характерная только для процедуры перестановочного декодирования.

Когнитивная карта декодера хранит сведения $P(t)$ о перестановках символов кодовых комбинаций, которые определяются априори в ходе обучения декодера, что позволяет уменьшить время декодирования данных на 3 и более порядков в зависимости от параметров кода.

G^1_{sys}	G^2_{sys}	G^3_{sys}	G^4_{sys}	G^5_{sys}
123 – 4567 – 1 123 – 4567	**124 – 3567 – 2** 124 – 5673	**125 – 3467 – 3** 125 – 6734	**126 – 3457 – 4** 126 – 7345	**127 – 3456 – 1** 712 – 3456
134 – 2567 – 1 341 – 2567	**135 – 2467 – 5** 135 – 6724	**136 – 2457 – 5** 613 – 4572	**137 – 2456 – 2** 713 – 4562	**145 – 2367 – 3** 451 – 2367
146 – 2357 – 5 461 – 2357	**147 – 2356 – 3** 714 – 5623	**156 – 2347 – 2** 561 – 2347	**157 – 2346 – 4** 715 – 6234	**167 – 2345 – 1** 671 – 2345
234 – 1567 – 1 234 – 5671	**235 – 1467 – 2** 235 – 6714	**236 – 1457 – 3** 236 – 7145	**237 – 1456 – 4** 237 – 1456	**245 – 1367 – 4** 452 – 3671
246 – 1357 – 5 246 – 7135	**247 – 1356 – 5** 724 – 5613	**256 – 1347 – 3** 562 – 3471	**257 – 1346 – 5** 572 – 3461	**267 – 1345 – 2** 672 – 3451
345 – 1267 – 1 345 – 6712	**346 – 1257 – 2** 346 – 7125	**347 – 1256 – 3** 347 – 1256	**356 – 1247 – 4** 563 – 4712	**357 – 1246 – 5** 357 – 1246
367 – 1245 – 3 673 – 4512	**456 – 1237 – 1** 456 – 7123	**457 – 1236 – 2** 457 – 1236	**467 – 1235 – 4** 674 – 5123	**567 – 1234 – 1** 567 – 1234

Рис. 2 Пример лексикографическая структура когнитивной карты декодера недвоичного кода

ВЫВОД

Применение в процедуре оценки биометрических сведений перестановочного декодирования позволяет сократить время обработки данных, что положительно отражается в условиях использования такой информации в системах реального времени с одновременным решением задач криптографической защиты данных.

Контакты

Гладких Анатолий Афанасьевич
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ульяновский институт гражданской авиации имени Главного маршала авиации Б.П. Бугаева»

E-mail: a_gladkikh@mail.ru
Phone: +7 909 357-78-37