Трошков А.М.
кандидат технических наук, доцент
Ставропольский государственный аграрный университет
Кондрашов А.В.
кандидат технических наук
Ставропольский государственный аграрный университет
Трошков М.А.
кандидат технических наук, доцент
Северо-Кавказский социальный институт

ФОРМИРОВАНИЕ ИНФОРМАЦИОННОГО КОДА ПО СТОМАТОЛОГИЧЕСКОЙ МАТРИЦЕ ДЛЯ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ И КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

Создание современных систем защиты от несанкционированного доступа на основе использования, в качестве полезной информации, статических биометрических характеристик человека (БХЧ) используется в практике принятия решения управлением доступом. Анализ информативных морфогенетических вариантов показывает, что их существует более 200, а используется на практике не более 80, причем в малых аномалиях развития. Поскольку полость рта (РПЧ) имеет генетическую детерминированность и отношение к элементу фенотипа любого человека, то РПЧ может быть использована для решения биометрических и диагностических задач, по идентификации или верификации личности.

Формирование информационного кода по стоматологической матрице происходит поэтапно в следующей последовательности:

1 этап характеризуется сканированием ротовой полости, которая делится на четыре сегмента (рис. 1).

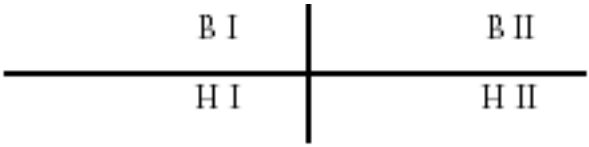

Рисунок 1 – Сегментарная декомпозиция ротовой полости человека

На основании сегментарной декомпозиции происходит сканированное распределение зубов, представленное на рис. 2.

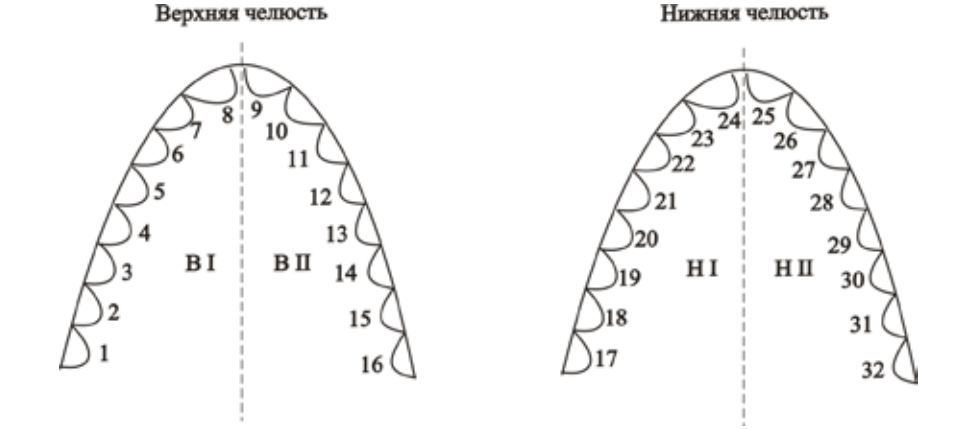

Рисунок 2 – Распределение зубов в сегментах

Исходя из сегментарной декомпозиции и распределения зубов (рис. 1, 2) на втором этапе производится построение стоматологической матрицы зубов человека (рис. 3).

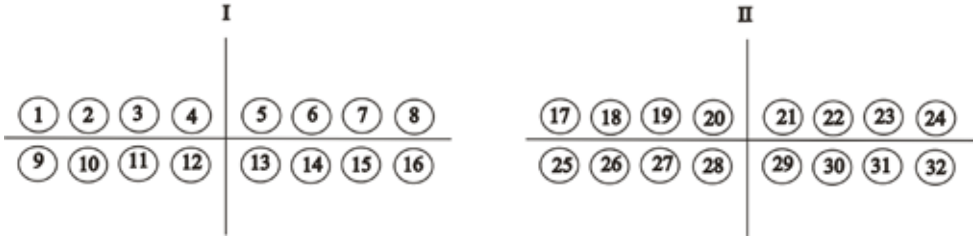

Рисунок 3 – Стоматологическая матрица (I и II)

С учетом формирования матриц I и II развертываем их в единый ряд, представленный на рис. 4.

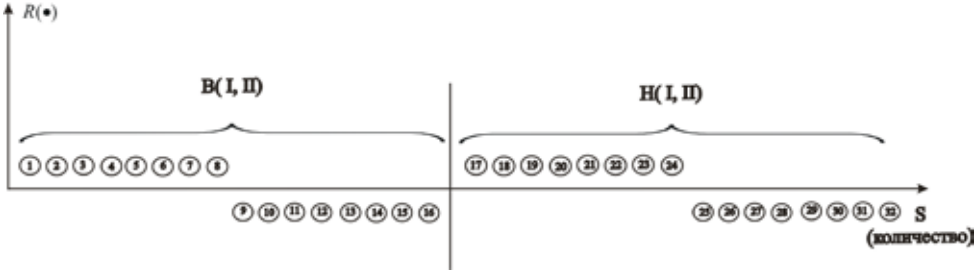

Рисунок 4 – Развернутый единый ряд стоматологической матрицы

На III этапе происходит построение центральной оси развернутого единого ряда стоматологической матрицы, выбор угла развертывания α от $24^\circ - 360^\circ$

и определение шага развертывания D. Если центральная ось и угол выбираются из расчета центральной точки $\mathbf{I}$, 360°, то D определяется из формулы:

$$D = \frac{360^\circ}{\alpha},$$

(формула 1)

Анализ предварительных расчетов показал, что α необходимо выбирать, $\approx 24^\circ$ тогда, используя (ф.1), D=15 шагов. На рис. 5 представлены выбор $\mathbf{I}$ ЦТ, выбор α.

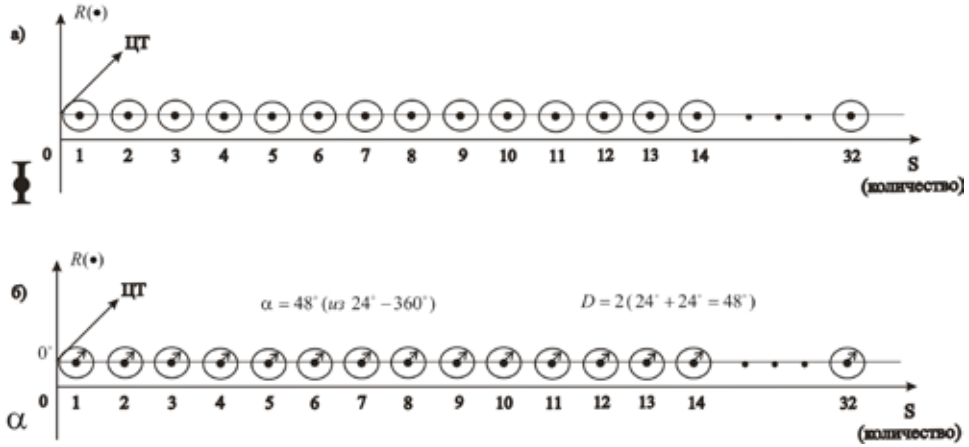

Рисунок 5 – Выбор центральной точки и α

Используя рис. 4 и 5(б) путем наложения реальной картины сканированной полости и расчетной $\mathbf{I}$ ЦТ и α, получаем следующую картину, представленную на рис. 6, как результирующую структуру с проекцией векторов с углом α и размерностью $\rightarrow$.

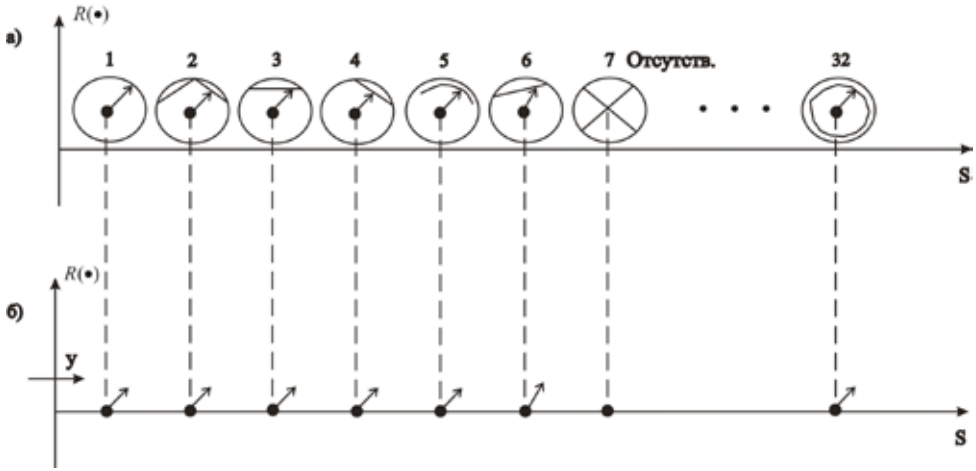

Рисунок 6 – Результирующая структура (а) и ее проекция (б)

На основании полученной проекции 6(б) произведем расчет $R(\bullet)$ – точки соприкосновения с концом зубов R. Расчет R производится в единице измерения «пиксель» с учетом, что 1 пиксель составляет 0,22 мм, тогда R рассчитывается по формуле

$$\underset{\min \to 1 мм}{\overset{\max \to 5 мм}{R(пикс)}} = \frac{y}{0,22} \quad [пикс] \tag{2}$$

Ограничение в формуле 2 по M : $\max R = 5$ ì , $\min R = 5$ ì .

Четвертый этап характеризуется позиционированием стоматологической матрицы, представленной в табл. 1.

Таблица 1 – Позиционирование стоматологической матрицы

<table>
<tr><th>N зуба</th><th>R [пиксель]</th><th>Q номер позиции</th><th>Расчет позиции</th></tr>
<tr><td>1</td><td>22 (max)</td><td>175</td><td rowspan="5">а)
R
1 мм 5 мм
min max

б)
R
4,5 пикс 22 пикс

Шаг позиционирования 0,1 пикс, отсюда .

$Q = {}^{22}/_{0,1} - {}^{4,5}/_{0,1} = 220 - 45 = 175$ позиций</td></tr>
<tr><td>2</td><td rowspan="3">.

.

.</td><td rowspan="3">.

.

.</td></tr>
<tr><td>3</td></tr>
<tr><td>4</td></tr>
<tr><td>5</td><td>4,5 (min)</td><td>1</td></tr>
<tr><td>.
.
.</td><td></td><td></td></tr>
<tr><td>32</td><td></td><td></td><td></td></tr>
</table>

В табл. 1 вводятся ограничения М: max Q=22 пикс, min Q= 4,5 пикс, шаг=0,1 пикс.

На этом же этапе производится кодирование результатов позиционирования стоматологической матрицы двоичным исчислением с количеством разрядов $n = 8$, представленное в табл. 2.

Таблица 2 – Кодирование результатов позиционирования

Q позиция	Код (двоичное исчисление)
1. (4,5 пикс)	00000001
2. (4,6 пикс)	00000010
. . .	. . .
175. (22 пикс)	11111111

На основании присвоенных кодов (табл. 2) размерности векторов (рис. 6б) развертывается цифровой информационный код (рис. 7).

Рисунок 7 – Развертывание цифрового информационного кода

Поскольку от шага D зависит угол поворота α , то необходимо ввести кодирование D и код D размещать перед ЦИК (рис. 8).

Рисунок 8 – Размещение шага D перед информационной частью ЦИК

Однако использование биометрического параметра стоматологическая матрица имеет недостатков, которыми не следует пренебрегать:

вероятность ложного пропуска (FAR);

вероятность ложного отказа (FRR);

большое время идентификации, аутентификации;

сложность и индивидуальность технических средств.

Перечисленные недостатки ведут к снижению безопасности, уменьшению удобства пользования системой, дискретизации системы, снижению эффективности функционирования биометрической системы.

Одной из характеристик оценки биометрической системы используют сравнительное биометрическое тестирование:

$$S_{тест} = \frac{FAR(P_{л.пр})}{FRR(P_{л.отк})}$$

(формула 3)

В России кроме Русского биометрического общества (основано в 2002 году), независимых центров биометрического тестирования не существует. Поэтому модели, способы, методы, устройства оценивать в России практически некому. Таким образом, достоверность биометрической информации, меры защиты от подделок, муляжей и биометрических шаблонов в настоящее время очень актуальны. Стандарты для биометрических технологий различны и еще не совершенны. Анализ существующей защиты делится на две группы :

технические;

организационные.

Техническая защита имеет уровень программного обеспечения, либо уровень считывающего устройства. Организационная защита состоит лишь в простой организации процесса аутентификации таким образом, чтобы затруднить или исключить возможность подделки.

Исходя из этого, можно сделать вывод о несовершенстве защиты биометрической системы. Предлагаемые системы биометрической защиты сводятся к следующим:

мультибиометрия (перекрестная) сводится к применению нескольких параметров (рис. 8);

Рисунок 8 – Мультибиометрия

многофакторная аутентификация использует совокупность методов аутентификации и других систем защиты (рис. 9).

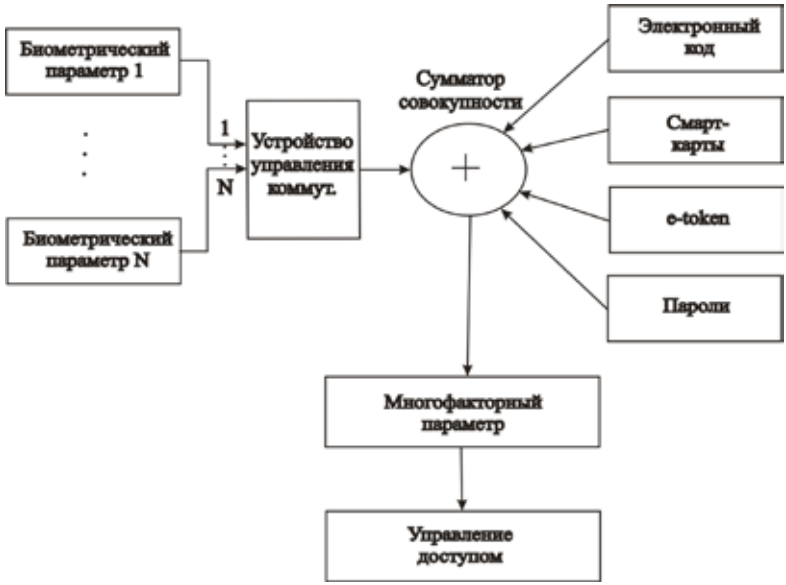

Рисунок 9 – Многофакторная аутентификация

Однако, мультибиометрия и многофакторная аутентификация усложняют работу

информационных средств и увеличивают время процедуры аутентификации, кроме того отсутствует защищенность информации биометрических характеристик и параметров.

Для устранения этих недостатков, а также повышения защищенности биометрических характеристик и параметров предлагаются следующие способы защиты. Одним из способов повышения защищенности биометрических характеристик, в том числе и стоматологической матрицы, является кодирование биометрических параметров с последующей криптографией. С этой целью биометрические системы идентификации (аутентификации) вычленяют индивидуальные особенности человека, которые находятся во множественном пространстве биометрических параметров и представлены в этом пространстве векторами биометрических признаков $S \in R^N$, это пространство определяет две области: S^+ – область биометрических параметров пользователей и S^- – область биометрических параметров претендентов на них. Через регулятор построения эталонных значений производится формирование эталонных биометрических параметров Y_n Из области S^- формируются претендентские биометрические параметры X_n При дальнейшей идентификации (аутентификации) происходит сталкивание $Y_n \oplus X_n$, результаты столкновений переходят в область сравнения. Этот алгоритмический процесс представлен на рис.

Рисунок 10 – Алгоритмический процесс биометрической идентификации (аутентификации)

Анализ процессов, представленный на рис. 10, показывает, что высока вероятность угрозы эталонным биометрическим параметрам Y_n в области формирования и области сравнения. Поэтому предлагается криптографическая защита на этих этапах. Для этого формируется кодирование пакетов по отдельным биометрическим параметрам (рис. 11).

Рисунок 11 – Формирование кодированных биометрических пакетов

Каждый пакет несет определенную кодируемую информацию, например, пакет №1 – анкетные данные пользователя, пакет №2 – идентификатор (выбор биометрического направления), пакеты №3 – №N – коды биометрических параметров (отпечатки пальцев, зрительный анализатор, слуховой анализатор, фрагменты антропометрии, стоматологической матрицы, ногтевой пластины, кровотока, объема конечностей и т.д.). Далее пакеты формируют единый цифровой информационный код (ЦИК), который больше подвержен угрозам.

Исходя из этого, для повышения информационной безопасности ЦИК, применяют традиционные методы криптографии, а именно, перестановки в пакетах (рис. 12).

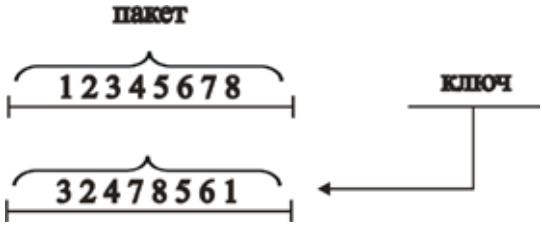

Рисунок 12 – Метод перестановки в пакетах

Далее сформированный пакет (блок) остается в едином цифровом информационном коде, к которому применяют метод блочного шифрования (рис. 13).

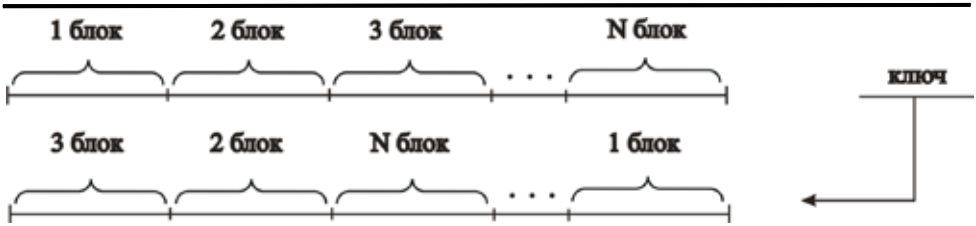

Рисунок 13 – Метод блочного шифрования

Таким образом, ЦИК будет зашифрован методами перестановки и блочного шифрования, что существенно повысит защиту биометрической информации.

Литература

1. Трошков А.М., Трошков М.А. Кодирование и информационная защита биометрических параметров ротовой полости человека для ограничения доступа к информационным ресурсам. // Материалы международной НПК СКСИ. – Ставрополь, 2008.

2. Трошков А.М., Трошков М.А., Филимонов А.А., Кондрашов А.В. Биометрические характеристики человека и их аутентификационные признаки – база создания защиты и ограничения доступа к информационным ресурсам агропромышленного комплекса. // Вестник АПК Ставрополья. – 2011. – № 3 (3). – с. 124-129.

3. Трошков А.М., Трошков М.А., Свидетельство о государственной регистрации программы для ЭВМ № 2012617031 «Информационная система аутентификации личности по биометрическим характеристикам». Заявка № 2012614575. Зарегистрировано в Реестре программ для ЭВМ 6 августа 2012.

4. Брюхомицкий Ю.А. Вероятностный метод классификации биометрических параметров личности. // Материалы X Международной научно-практической конференции «Информационная безопасность». Часть 1 – Таганрог. Издательство ТТИ ЮФУ, 2008. – 318с.