УДК 004.056.53

С.М. Гончаров, А.В. Первак

Генерация ключевой пары на основе 3-мерной геометрии лица с использованием дифференциально-геометрического представления

Предложен алгоритм формирования ключевых строк на основе трёхмерных биометрических образов человеческого лица, представленных при помощи аппарата дифференциальной геометрии. Рассмотрена схема применения алгоритма в задачах аутентификации.

Ключевые слова: биометрия, криптография, генерация ключа, аутентификация, трёхмерная геометрия лица, FMTD, MDS.

Биометрические системы аутентификации по геометрии лица имеют особое значение по следующим причинам:

1. Такие системы не требуют прямого физического контакта с пользователем.
2. Снятие изображений лиц при помощи камер не представляет никаких технических трудностей.

Однако даже при использовании трёхмерных изображений лиц у систем биометрической аутентификации существует ряд проблем, а именно:

1. Данные хранятся в открытом виде – имея на руках базу данных эталонных значений, появляется возможность сделать муляж биометрического признака.
2. Невозможна анонимная аутентификация.
3. Полученные биометрические образцы из-за своей «шумности» нельзя использовать в криптографии.

Для решения этих проблем было предложено извлекать из биометрического образца уникальную ключевую последовательность, которую впоследствии можно использовать в системе аутентификации.

Для того чтобы построить такую систему, для начала необходимо подобрать конкретное представление человеческого лица, пригодное для цифровой обработки и проведения расчётов. Их существует достаточно много [1], однако мы рассмотрим три.

Облако точек. В данном методе лицо будет представляться трёхмерным облаком точек – множеством $\{p_1, p_2 ... p_m\}$, в котором p_k – это просто координаты (x, y, z) каждой точки, а m – число всех точек (рис. 1).

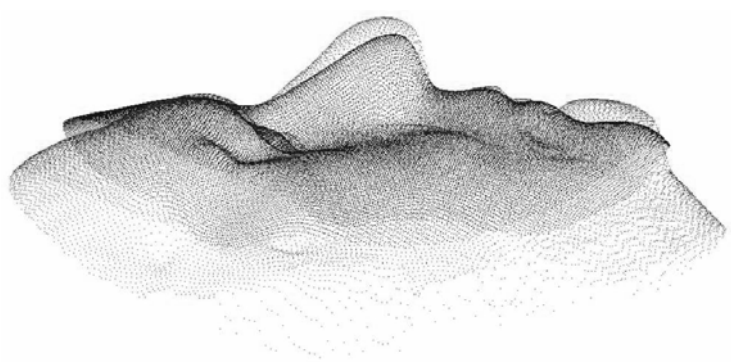
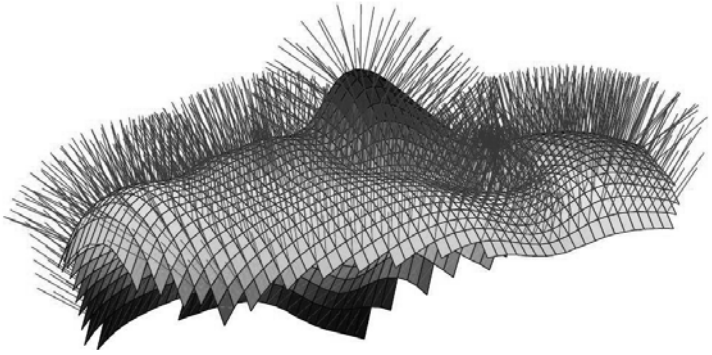


Рис. 1. Представление лиц облаками точек

Метод представления *полем нормалей*. Для каждой трёхмерной точки на поверхности лица рассчитывается вектор нормали. Математически представление лица как поля нормалей имеет вид $\{\vec{\mathbf{n}}_1, \vec{\mathbf{n}}_2, ..., \vec{\mathbf{n}}_m\}$, где $\vec{\mathbf{n}}_k$ – векторы нормалей во всех точках поверхности (рис. 2).

Алгоритмы категории *методов дифференциально-геометрического представления* оперируют с инвариантами двумерных поверхностей. Классическим примером такого инварианта является так называемая первая квадратичная форма поверхности (или метрика, или метрический тензор).

Дифференциально-геометрическое представление является, по сути, расширением представления полем нормалей и более привлекательно на фоне других методов в силу его высокой устойчивости к произвольности в положении головы пользователя или выражения его лица. Точнее, главная математическая идея выбранного представления состоит в предположении, что человеческое лицо



моделируется именно как деформируемая поверхность, все трансформации которой тем не менее происходят не более чем *изометрически* (расстояния между любыми двумя точками не изменяются) [2].

Рис. 2. Представление лица полем нормалей

Из курса дифференциальной геометрии известно, что множеству изометрических поверхностей можно поставить в соответствие инвариантную величину – метрический тензор (или метрика, или первая квадратичная форма). Найти метрику можно по формулам:

$$\mathbf{g}_{ij} = \begin{pmatrix} \mathbf{X}_1 \cdot \mathbf{X}_1 & \mathbf{X}_1 \cdot \mathbf{X}_2 \\ \mathbf{X}_1 \cdot \mathbf{X}_2 & \mathbf{X}_2 \cdot \mathbf{X}_2 \end{pmatrix}, \quad (1)$$

где $\mathbf{X}_1 = (1, 0, z_x)$, $\mathbf{X}_2 = (0, 1, z_y)$, z_x, z_y – компоненты поля нормалей к поверхности лица.

Вычисленный метрический тензор необходимо преобразовать в вид, максимально удобный для хранения в цифровом виде и последующего использования для сравнения с метриками других лиц. В задачах обработки трёхмерных изображений для подобных целей используется алгоритм *MDS* (multi–dimensional scaling) [3], основная идея которого заключается в максимальном сокращении объёма данных о моделируемом объекте при минимизации возможно возникающих погрешностей вычисления. Давая конечное представление поверхности в виде величин, называемых инвариантными к изгибаниям каноническими формами (bending–invariant canonical form), этот алгоритм является, по сути, ядром вычислительной части нашей системы распознавания. Рассмотрим его подробнее.

Пусть нам дано представление поверхности в виде его облака точек $\{p_1, p_2 ... p_n\}$ и задана функция расстояний, порождающая матрицу расстояний:

$$D(p_i, p_j) = \boldsymbol{\delta}_{ij}. \quad (2)$$

Для удобства вычисления принято пользоваться не самой матрицей расстояний, а другой, вычисляемой по формуле

$$\boldsymbol{\Delta}_{ij} = (\boldsymbol{\delta}_{ij})^2. \quad (3)$$

Далее матрица $\boldsymbol{\Delta}$ обрабатывается следующим образом:

$$\mathbf{B} = -\frac{1}{2}\mathbf{J}\boldsymbol{\Delta}\boldsymbol{\Delta}, \quad (4)$$

где $\mathbf{J} = \mathbf{I} - \frac{1}{n}\mathbf{U}$; $\mathbf{I}$ – единичная матрица размером $n \times n$; $\mathbf{U}$ – матрица размером $n \times n$, состоящая целиком из единиц.

Первые m собственных векторов $\vec{\mathbf{e}}_i$, соответствующие m наибольших собственных чисел матрицы **B**, используются как координаты вложения

$$x_i^j = e_i^j, \; 1 = \overline{1, n}, \; 1 = \overline{1, m}, \quad (5)$$

где x_i^j – j-я компонента вектора $\vec{\mathbf{x}}_j$.

Множество точек $\vec{\mathbf{x}}_i$, полученное при помощи алгоритма MDS, называется *инвариантной к изгибаниям канонической формой*. Если m = 3, то пространство вложения – трёхмерное и каноническая форма представляет собой не что иное, как некоторую поверхность в этом пространстве. К таким формам могут быть применены такие же методы сравнения, какие используются в распознавании поверхностей твёрдых тел.

Таким образом, открытым остаётся лишь вопрос об алгоритме нахождения матрицы расстояний. Решение этой задачи относится к области реализации алгоритма, известного как FMTD (fast marching on triangulated domains) [4].

Подробно алгоритм описан в [4], а на рис. 3 приведён пример его применения к поиску расстояний на поверхности лица от одной исходной точки до всех остальных. Чёрные изолинии показывают области, одинаково удалённые от начальной точки.

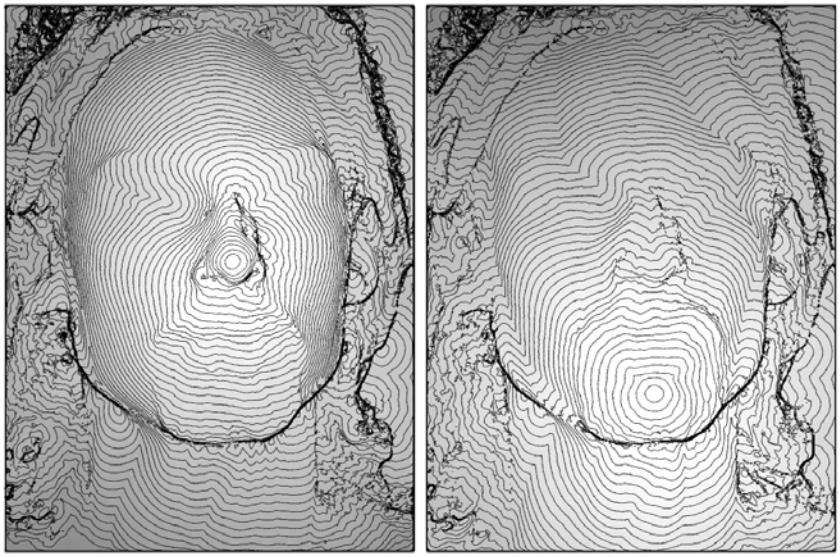


Рис. 3. Применение алгоритма FMTD к расчёту расстояний на поверхности лица

Итак, биометрическая система некоторым специальным аппаратным методом снимает с поверхности лица человека производные z_x, z_y, на основе которых вычисляется метрический тензор $\mathbf{g}_{ij}$. Из него посредством алгоритма FMTD вычисляется матрица расстояний $\boldsymbol{\delta}_{ij}$, из которой в свою очередь при помощи алгоритма MDS получается каноническая форма поверхности.

Следующим шагом является вычисление так называемых *сигнатурных моментов поверхности* [5]. Конкретнее, моментом сигнатуры (p, q, r) поверхности в трёхмерном евклидовом пространстве называет величина

$$M_{pqr} = \sum_i \left(x_i^1\right)^p \left(x_i^2\right)^q \left(x_i^3\right)^r, \tag{6}$$

где суммирование производится по всем точкам поверхности.

Величина $p+q+r$ называется *порядком* момента.

Чтобы произвести обычное сравнение двух лиц в представлении их канонических форм, следует составить последовательность чисел, называемую вектором сигнатурных моментов поверхности:

$$\left(M_{p_1q_1r_1} \ldots . M_{p_Kq_Kr_K}\right). \tag{7}$$

Теперь на основе вектора моментов можно получать ключевую последовательность. Основная идея реализации этой процедуры состоит в том, чтобы сравнивать элементы вектора моментов каждого пользователя с элементами специальной хранящейся в системе последовательностью, составленной на основе некоторой обучающей базы лиц пользователей (так называемый пороговый вектор). Теперь опишем этапы работы системы подробнее.

Процедура регистрации нового пользователя (будем обозначать относящиеся к нему параметры индексом i):

1. Случайным образом генерируется секретная строка пользователя $\mathbf{u}_i$ длины L.

2. К секретной строке применяется помехоустойчивое кодирование, в результате чего мы получаем кодированную строку $\mathbf{c}_i = C_e(\mathbf{u}_i)$ длины K (поскольку сущность идеи помехоустойчивого кодирования вообще состоит в добавлении в информацию избыточности, очевидно, что K будет больше L).

3. Пользователь предъявляет системе свою биометрическую характеристику (лицо), по которой система сначала строит вектор моментов $\mathbf{f}_i$, и на основании его и порогового вектора $\boldsymbol{\mu}$ строится ключевая строка $\mathbf{b}_i$ (длина которой k будет зависеть от качества снятия характеристики, но, очевидно, должна быть больше K) по формуле

$$\mathbf{b}_{i,t} = \begin{cases} 1, \mathbf{f}_{i,t} \geq \boldsymbol{\mu}, \\ 0, \mathbf{f}_{i,t} < \boldsymbol{\mu}, \end{cases}, \quad t = \overline{1, L}. \tag{8}$$

4. Строится так называемый вектор надёжности $\mathbf{r}_i$, выражающий пригодность к использованию каждого извлечённого бита:

$$\mathbf{r}_{i,t} = \frac{\left|\boldsymbol{\mu}_t - \boldsymbol{\mu}_{i,t}\right|}{\left(\sigma_i\right)_t}. \tag{9}$$

5. Среди всех элементов вектора $\mathbf{b}_i$ выбираются K таких, чтобы соответствующие им значения вектора надёжности $\mathbf{r}_i$ были наибольшими. Так мы получаем бинарный вектор надёжности $\mathbf{x}_i$;

6. *Первый вспомогательный вектор* $\mathbf{w}_i$ строится как последовательность индексов наиболее надёжных элементов вектора $\mathbf{b}_i$ (тех его значений, которые попали в бинарный вектор надёжности). Он состоит из целых чисел.

7. *Второй вспомогательный вектор* строится как сумма

$$\mathbf{v}_i = \mathbf{c}_i \oplus \mathbf{x}_i. \tag{10}$$

8. *Третий вспомогательный вектор* – это значение некоторой криптографической хеш-функции от секретной строки

$$\mathbf{h}_i = HASH\left(\mathbf{u}_i\right). \tag{11}$$

9. Пара $\mathbf{X}_i = \left(\mathbf{w}_i, \mathbf{h}_i\right)$ сохраняется в системе как данные о пользователе;

10. Вектор $\mathbf{v}_i$ выдаётся пользователю как его открытый ключ.

Процедура аутентификации:

1. Пользователь предъявляет системе свои биометрические характеристики, на основании которых строится вектор особенностей $\mathbf{f}_i$, и открытый ключ $\mathbf{v}_i$.

2. По формуле (8) строится ключевая строка $\mathbf{b}'_i$.

3. Система при помощи сохранённого в своей базе вспомогательного вектора $\mathbf{w}_i$ выбирает из вектора $\mathbf{b}'_i$ элементы в бинарный вектор надёжности $\mathbf{x}'_i$.

4. Секретная строка пользователя находится по формуле

$$\mathbf{u}'_i = C_d\left(\mathbf{v}_i \oplus \mathbf{x}_i\right). \tag{12}$$

5. Аутентификация будет считаться пройденной при выполнении условия

$$HASH\left(\mathbf{u}'\right) \equiv \mathbf{h}_i. \tag{13}$$

В качестве алгоритма помехоустойчивого кодирования обычно применяют последовательность кодов БЧХ и Рида–Соломона.

Были проведены предварительные эксперименты, в которых исследовалась работа описанных алгоритмов. Качество реализованной системы позволило вычислять сигнатурные моменты вплоть до 12-го знака после запятой, в связи с чем информативными оказались 220 первых из них. Таким образом, удалось получать ключи длиной 220 бит. Более качественные системы обычно позволяют получать ключи длиной до 408 бит [6]. В эксперименте использовались только 63 первых бита последовательностей.

Среднее время сканирования каждого пользователя – 2 с. Для предварительных экспериментов, для которых не проводились специальные исследования по повышению эффективности алгоритма, лучшее значение для ошибки первого рода – 5, второго рода – 10%.

Ключи были исследованы на случайность частотным методом. 95% сгенерированных последовательностей удовлетворили критерию.

Литература

1. Gökberk B. Three dimensional face recognition // Ph.D. Thesis [Электронный ресурс]. – Режим доступа: http://www.vanderberk.com/docs/gokberk_phdthesis_2006.pdf, свободный (дата обращения: 20.04.2012).

2. 3D Face Recognition without Facial Surface Reconstruction / A. Bronstein, M. Bronstein, R. Kimmel, A. Spira [Электронный ресурс]. – Режим доступа: http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2003/CIS/CIS-2003-05.pdf, свободный (дата обращения: 20.04.2012).

3. Bronstein A. Numerical geometry of non-rigid objects: embedding problems [Электронный ресурс]. – Режим доступа: http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2007/PHD/PHD-2007-07.pdf, свободный (дата обращения: 21.04.2012).

4. Spira A. An efficient solution to the eikonal equation on the parametric manifolds / A. Spira, R. Kimmel // Interfaces and Free Boundaries. – 2004. – № 6. – P. 315–327.

5. Elad M. Content based retrieval of VRML objects – an iterative and interactive approach / M. Elad, A. Tal, S. Ar // Proc. EG Multimedia. – 2001. – № 39. – P. 97–108.

6. Privacy Enhancing Technology for a 3D-Face Recognition System / X. Zhou, T. Kevenaar, E. Kelkboom et al. [Электронный ресурс]. – Режим доступа: http://subs.emis.de/LNI/Proceedings/Proceedings108/gi-proc-108-001.pdf, свободный (дата обращения: 21.04.2012).

Гончаров Сергей Михайлович
Канд. физ.-мат. наук, доцент, зав. каф. «Безопасность информации и телекоммуникационных систем» (БИТС) Морского Государственного университета им. адм. Г.И. Невельского (МГУ им. Г.И. Невельского)
Тел.: +7-914-707-29-93
Эл. почта: sgprim@smtp.ru, goncharov@msun.ru

Первак Андрей Владимирович
Аспирант каф. БИТС МГУ им. Г.И. Невельского
Тел.: +7-924-232-08-69
Эл. почта: pervak1989@mail.ru

Goncharov S.M., Pervak A.V.
Key pair generation based on 3D–face geometry using differential–geometric representation.

The key sequences forming algorithm based on differential geometry 3D–biometric images of human face is proposed. The application of the algorithm in authentication tasks is performed.
Keywords: biometrics, cryptography, key sequence generation, authentication, 3D face geometry, FMTD, MDS.
