5. Marushko, Y. Using Ensembles of Neural Networks with Different Scales of Input Data for the Analysis of Telemetry Data / Y. Marushko // Proc. of the XV Intern. PhD Workshop OWD 2013 (Wisla, 19–22 Oct. 2013). – Gliwice: Silesian University of Technology, 2013. – P. 386–391.
6. Parikh, D. An ensemble-based incremental learning approach to data fusion / D. Parikh, R. Polikar // IEEE Transactions on Systems, Man and Cybernetics – Part B: Cybernetics. – 2007. – Vol. 37. – № 2. – P. 437–450.

Материал поступил в редакцию 25.11.15

MARUSHKO E.E. Using ensembles of neural networks for prediction of spacecraft corrective propulsion system telemetry parameters

Issues related to intellectual processing of complex poorly formalized tasks in the field of the analysis of telemetry data are considered. Methods of combining of neural networks into ensembles based on weighing for forecasting tasks are described in detail. Possibility of additional training of the neural network ensemble is analyzed.

УДК 004.93

Загородняя Д.И.

МЕТОД ИДЕНТИФИКАЦИИ ЛИЦ ПО ХАРАКТЕРНЫМ ТОЧКАМ КОНТУРА

Введение. Стремительное развитие вычислительной техники и снижение ее стоимости обусловили расширение области применения систем видеонаблюдения не только на больших объектах (аэропорты, супермаркеты, банки), но и на таких, как остановки общественного транспорта, парки, скверы, площади, придомовые территории и тому подобное.

В связи с этим возникает задача систематизации и автоматизации обработки видеоданных, например для поиска субъектов в потоке людей, распознавания лиц или других объектов, отслеживания, перемещения объектов. Задачи, упомянутые выше, требуют слишком больших вычислительных ресурсов при условии непосредственного анализа всей информации, поступающей с камер видеонаблюдения. Поэтому такие системы не имеют достаточной оперативности.

Для того чтобы сократить объем данных, который обрабатывается, и соответственно, повысить оперативность работы всей системы видеонаблюдения, в данной работе предложено применить иерархические методы контурной сегментации на основе вейвлет-анализа [1]. Особенностью этих методов является возможность выделить на изображении объекты или детали объектов с нужной для цели обработки детализацией. Также предлагается перейти к идентификации лиц по форме головы человека, используя для этого информацию только о характерных точках контура лица.

Выделение характерных точек можно осуществить следующими методами (которые имеют некоторые недостатки) [2]:

- дифференциальный (нельзя регулировать количество выделенных характерных точек, низкая помехоустойчивость),
- полигональный (сложность и высокие вычислительные затраты),
- интерполяционный (низкая точность).

На основе проведенного анализа методов в данной работе разработан метод выделения характерных точек на основе вейвлет-анализа функции кривизны.

В случае если распознавание по форме головы не обеспечивает необходимого результата, то предусматривается переход на другие уровни детализации.

Предлагаемый подход. Задача автоматического распознавания пространственных объектов относится к сложным задачам комплексного типа. Структура системы распознавания представлена на рисунке 1, на котором изображение поступает из видеодатчика на кадровый накопитель, после этого изображение проходит предыдущую обработку для улучшения его качества и уменьшения объема видеоинформации; осуществляется локализация области лица и проводится контурная сегментация. Выделяются характерные точки контура и на основе информации только о характерных точках контура строится идентификационный вектор, который позволит классифицировать объекты при заданных условиях [3].

Точки контура, которые передают смысл фигуры, – находятся на участках значительной кривизны контура и называются характерными точками контура. Также установлено, что при соединении таких точек отрезками суть фигуры сохранится (теорема Аттнива). Поэтому можно переходить к выделению признаков для распознавания изображений, используя только информацию о характерных точках [2, 4].

Функция кривизны – это дифференциальная функция координат контура [5, 6]. Для дискретного случая кривизна определяется формулами [7]:

$$z(s_i) = x(s_i) + iy(s_i), \quad (1)$$

$$\Phi(s_i) = arctg\left[\frac{y(s_i) - y(s_{i-1})}{x(s_i) - x(s_{i-1})}\right], \quad (2)$$

$$k(s_i) = \Phi(s_i) - \Phi(s_{i-1}), \quad (3)$$

где s_i i-й элемент дуги.

Рис. 1. Структура системы видеонаблюдения

А для полярной системы координат кривизна определяется следующим образом:

$$k_i = \sqrt{\bar{x}_i^{-2} + \bar{y}_i^{-2}}, \quad \theta_i = arctg\left(\frac{\bar{y}_i}{\bar{x}_i}\right), \quad (4)$$

$$\bar{x}_i = x_i - \bar{x}, \quad \bar{y}_i = y_i - \bar{y}, \quad (5)$$

где $(x_i, y_i) \in X$ – упорядоченное множество точек контура изображения в декартовой системе координат, $\bar{x}$, $\bar{y}$ – средняя точка изображения контура, k_i – размер кривизны, которая отвечает углу θ_i.

Однако, в меру дифференциальной природы, сама функция кривизны имеет низкую помехоустойчивость: любые максимумы и минимумы отмечаются как характерные точки, за счет чего выделяется большое количество таких точек. Поэтому, для выхода из данной ситуации, предложено использовать вейвлеты Хаара, как самые простые вейвлеты, которые хорошо зарекомендовали себя в прак-

***Загородняя Диана Ивановна**, аспирант кафедры информационно-вычислительных систем и управления, факультет компьютерных информационных технологий, Тернопольский национальный экономический университет.*
Украина, 46009, г. Тернополь, Тернопольская область, ул. Львовская, 11.

тических заданиях обработки дискретных сигналов.

Вейвлеты Хаара представляют собой кусково-постоянные функции, которые принимают два значения {-1; +1} и заданны на конечных интервалах разных масштабов [8].

Вейвлет-преобразование функции кривизны в базисе Хаара заключается в линейном превращении функции вектора k парной размерности 2π в другой вектор H согласно следующим соотношением [3]:

$$H_j = \sum_{i=j-a}^{j-1} k_i \cdot 1 + \sum_{i=j}^{j+a} k_i \cdot (-1), \qquad (6)$$

где $j \in [-\pi + a; \pi - a)$, $2a$ – длина вейвлета Хаара.

В зависимости от значения параметра a будет выделяться разное количество характерных точек: чем меньшее значение параметра a – тем больше будет характерных точек.

Для идентификации формы головы был выбран структурно-статистический метод [2], так как он обеспечивает инвариантность к геометрическим превращениям, высокую помехоустойчивость и не требует значительных вычислительных затрат.

Выражение для вычисления идентификационного вектора имеет вид [2]:

$$\mu_p = \iint_A \rho^p Q(\rho, \varphi) \psi(x \cap A), \qquad (7)$$

где A – множество вещественных чисел; X – подмножество вещественных чисел $x(\rho, \varphi)$ координат характерных точек контура фигуры в полярной системе координат; ψ – мера на множестве вещественных чисел; ρ – порядок момента; Q – множество характерных точек контура:

$$Q(\rho, \varphi) = \begin{cases} 1, \rho = \rho_i, \varphi = \varphi_i; i = 1, \ldots, J \\ 0, \rho \neq \rho_i. \end{cases}$$

J – количество характерных точек контура объекта.

Учитывая, что мера Лебега в полярной системе координат является площадью треугольника, можно записать формулу (7) в дискретном виде:

$$\mu_p = \left| \sum_{i=0}^{J} \rho_i^{*(p+2)} \sin(\Delta\varphi_i) \right|, \qquad (8)$$

где $\rho_i^* = \sqrt{\rho_i \rho_{i+1}}$ – среднее геометрическое радиус-векторов, $\Delta\varphi_i = \varphi_{i+1} - \varphi_i$ – разница фаз между i-й и (i+1)–й характерными точками.

Это выражение берется по модулю, поскольку знак выражения зависит от направления обхода характерных точек, а нас интересует только абсолютное значение. Для обеспечения инвариантности к масштабу проведели нормирование радиус-векторов, использовав коэффициент $\rho = \sqrt{\frac{S}{2\pi}}$, где S – площадь фигуры.

Тогда выражение (8) будет иметь вид: $C_p = \left| \sum_{i=0}^{J} \rho_{i0}^{*(p+2)} \sin(\Delta\varphi_i) \right|$, где $\rho_{i0}^* = \frac{\rho_i^*}{\rho}$.

В случае, когда $\Delta\varphi_i$ достаточно мало, то есть достаточно много характерных точек, можно считать, что $\sin(\Delta\varphi_i) \approx \Delta\varphi_i$. Тогда получим: $C_p = \left| \sum_{i=0}^{J} \rho_{i0}^{*(p+2)} \Delta\varphi_i \right|$. Само значение Ср используется в качестве вектора признаков.

Эксперименты. Для проведения экспериментов работы описанного метода использованы изображения из базы изображений ORL [9], которая состоит из десяти изображений для каждого из 40 разных лиц. Для каждого лица изображения были сделаны в разное время, с измененным освещением, измененной мимикой (открытыми или закрытыми глазами, с улыбкой или без нее), измененными чертами лица (очки или без очков).

На рис. 2 приведен пример изображения из базы ORL, а также выделенный контур формы головы. Количество точек контура – 233.

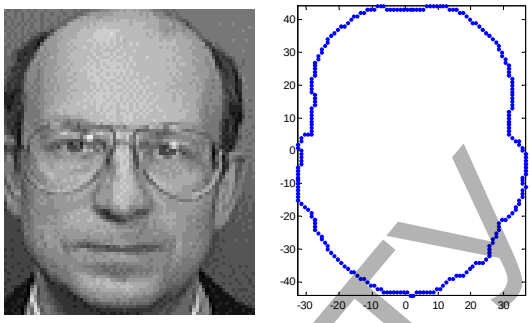


Рис. 2. Изображения из базы ORL и его контур

График функции кривизны представлен на рис. 3 для изображения контура формы головы из рис. 2. По оси абсцисс установлено значение угла, который находится в диапазоне $(-\pi; \pi)$, а по оси ординат – значения функции кривизны k.

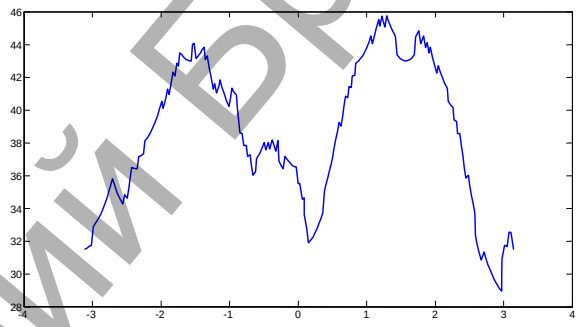


Рис. 3. Функция кривизны

В первом столбце таблицы 1 приведены примеры функции, которая образовывается в результате наложения вейвлета Хаара согласно соотношению (6) на функцию кривизны из рис. 3. В таком случае характерные точки находятся на пересечении графика с осью абсцисс.

Некоторые характерные точки находятся рядом друг с другом, что в свою очередь не несет смыслового наполнения (кардинальных изменений формы головы), поэтому, предлагается при вычислении идентификационного вектора учитывать только одну характерную точку, когда расстояние между характерными точками меньше параметра a. С учетом данной поправки, такие характерные точки, которые удовлетворяют данному условию, обведены в кружки, а расстояние a от характерной точки обозначено сплошной линией.

Для визуальной наглядности во втором столбце таблицы 1 представлен контур изображения лица с нанесенными на него и последовательно соединенными характерными точками, выделенными описанным методом.

В третьем столбце таблицы 1 указана длина вейвлета Хаара a для каждого конкретного случая и соответствующее количество выделенных характерных точек (J), а также рассчитанные значения C_p идентификационного вектора.

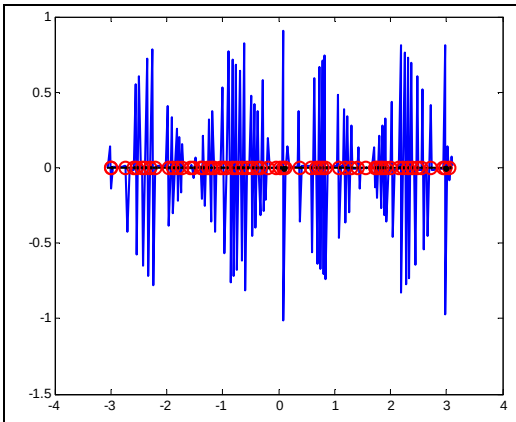
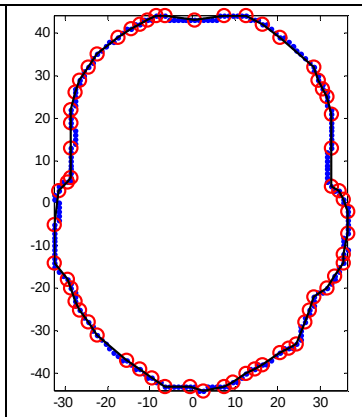
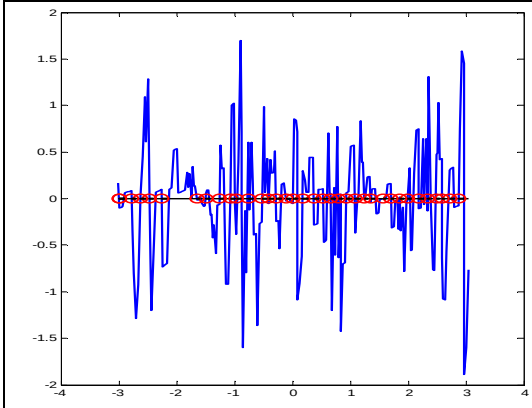
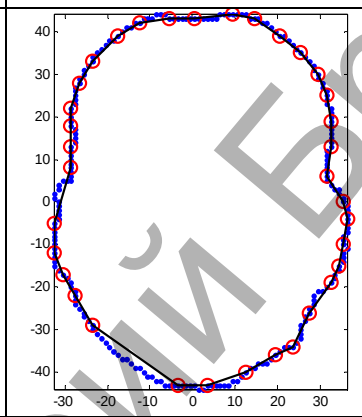
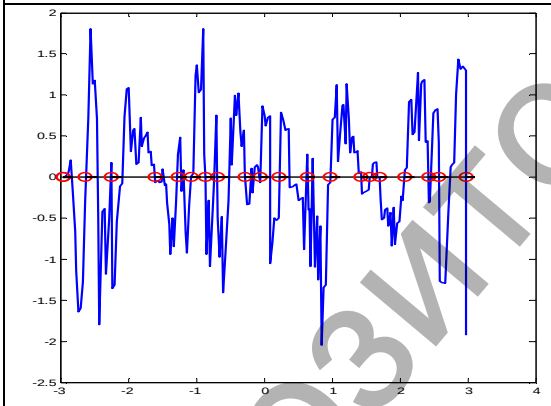
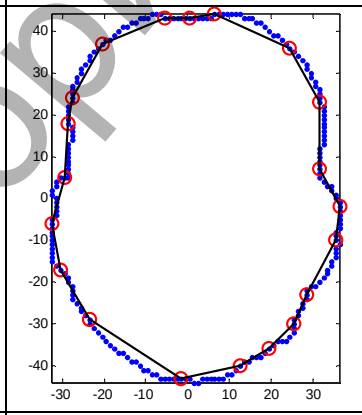
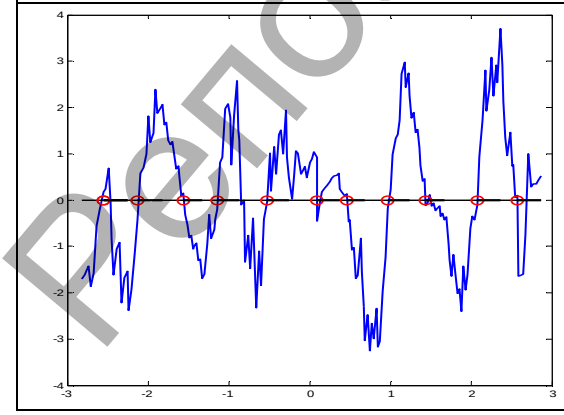
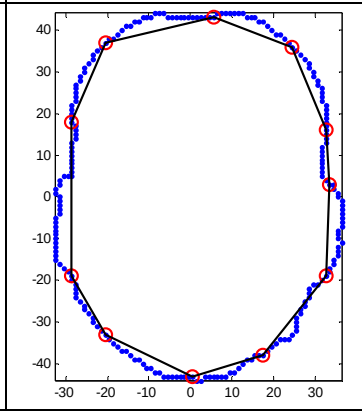
Заключение. Предложенный метод выделения характерных точек на основе вейвлет-анализа функции кривизны позволил устранить недостатки дифференциального и интерполяционного методов благодаря регуляризирующим свойствам и низкой вычислительной сложности.

Использование данного метода дало возможность регулировать детализацию выделения характерных точек.

Предложено осуществлять идентификацию лиц, используя структурно-статистический метод, который базируется только на информации о характерных точках контура.

Предложенная методика идентификации лиц позволяет повысить быстродействие работы системы видеонаблюдения за счет уменьшения объема обрабатываемой информации.

Таблица 1. Примеры работы метода выделения характерных точек контура с регуляризирующим свойством

		α =1 J=61 C1 = 18.1165415896 C2 = 26.3943845578 C3 = 38.8296080684 C4 = 57.6329614961 C5 = 86.2350323116 C6 = 129.9765046331 C7 = 197.1961129633 C8 = 300.9485303866 C9 = 461.7214762318 C10 = 711.7399301868
		α =3 J=35 C1 = 18.1776031321 C2 = 26.5620245146 C3 = 39.1773192075 C4 = 58.2784847845 C5 = 87.3660901664 C6 = 131.8916626829 C7 = 200.3699819765 C8 = 306.1363758523 C9 = 470.1280293504 C10 = 725.2934234978
		α =5 J=20 C1 = 18.2653010321 C2 = 26.7967078616 C3 = 39.6555130973 C4 = 59.1578268260 C5 = 88.9046863087 C6 = 134.5129442142 C7 = 204.7695178972 C8 = 313.4576181975 C9 = 482.2511539824 C10 = 745.3094482086
		α =10 J=11 C1 = 18.6899241881 C2 = 27.9889287101 C3 = 42.1911847904 C4 = 63.9986873516 C5 = 97.6513576557 C6 = 149.8232588032 C7 = 231.0502016254 C8 = 358.0079482905 C9 = 557.1539062152 C10 = 870.5573502377

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Полякова, М.В. Морфологический метод контурной сегментации изображений на основе репагулярного вейвлет-преобразования / М.В. Полякова, В.Н. Крылов // Труды Одесского политехнического университета – 2006. – Вып. 1(25). – С. 98–103.
2. Крылов, В.Н. Вторичные преобразователи сигналов зображений / В.Н. Крылов, М.В. Максимов – Одесса: Астропринт, 1997. – 176 с.
3. Zahorodnia, D. Structural Statistic Method Identifying Facial Images by Contour Characteristic Points / D. Zahorodnia, Y. Pigovsky, P. Bykovyy, V. Krylov, I. Paliy, I. Dobrotvor // Proceedings of the 8th

IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015). – Warsaw (Poland), 2015. – P. 293–297.
4. Ding, Ian-Jiun Compression for the Feature Points with Binary Descriptors / Ian-Jiun Ding, Szu-Wei Fu, Ching-Wen Hsiao, Pin-Xuan Lee, Yen-Chun Chen // Proceedings of the 19th International Conference on Digital Image Processing. – 2014. – Taiwan. – P. 651–656.
5. Daguang, Jiang. Comparion and Study of Classic Feature Point Detection Algorithm / Jiang Daguang, Yiy Junkai // Proceedings of the 2012 International Conference on Computer Science and Service System. – 2012. – P. 2307–2309.
6. Schimid, C. Evaluation of Interest Point Detectors / C. Schimid, R. Mohr, C. Bauckhane // International Journal of Computer Vision, 2nd ed. – Vol. 37. – 2000. – P.151–172.
7. Прэт, У. Цифровая обработка изображений: в 2-х книгах / Прэт У.; пер. с англ. Д.С. Лебедев. – М.: Мир, 1982. – Кн. 2 – 480 с., ил.
8. Демьянович Ю.К. Введение в теорию вэйвлетов. Курс лекций / Ю.К. Демьянович, В.А. Ходаковский - Санкт-Петербург, 2007р. – 49 с.
9. База изображений: AT&T Laboratories Cambridge. – Режим доступа: http://www.cl.cam.ac.uk/research/dtg/attarchive/facesatglance.html.

Материал поступил в редакцию 08.01.16

ZAHORODNIA D.I. Method of Face Identification Based on Contour Characteristic Points

This paper proposes a method for characteristic points detection based on the wavelet analysis of the curvature function, which allowed the detail regulation of the characteristic point's allocation. It is proposed to implement person's identification using the identification vector, which is based only on the contour characteristic points. The proposed method of person's identification allows increasing of video surveillance system performance by reducing the size of information to be processed.

УДК 003.26:51:004(075.8)

Виссия Х.Е.Р.М., Галибус Т.В., Гафуров С.В., Каганович Д.М.

ЗАЩИТА МОБИЛЬНЫХ ПРИЛОЖЕНИЙ НА ОСНОВЕ РАЗДЕЛЕНИЯ СЕКРЕТА

В настоящее время использование мобильных технологий стало практически универсальным и наиболее удобным способом своевременного доступа к информации и управления ею. Все чаще важные конфиденциальные данные хранятся и обрабатываются на мобильных устройствах, что требует наличия соответствующих защитных механизмов, специализированных под нужды обеспечения безопасности мобильных платформ. Наиболее высоким уровнем защиты должны обладать при этом мобильные устройства, которые используются в корпоративном секторе, поскольку данные, хранящиеся на таких устройствах, являются наиболее уязвимыми.

В данной работе рассмотрена разработанная авторами система аутентификации для мобильной платформы Android, в основе которой лежит полиномиальная модулярная СРС[1], описанная в стандарте СТБ 34.101.60 [10] и работе [2]. В сравнении со стандартной системой аутентификации, при использовании предложенного метода нет необходимости в хранении кода аутентификации (паттерн/PIN/пароль) на устройстве пользователя [5]. Кроме того, стандартная система безопасности Android подвержена ряду известных уязвимостей, например, CVE-2015-3860 [4], которая позволяет злоумышленнику получить доступ к устройству пользователя, минуя этап аутентификации. Предложенный нами метод аутентификации не использует данных стандартных системных сервисов, за счет чего является более устойчивым к подобного рода атакам.

Таким образом, в рамках предложенного метода гарантируется, что доступ к ключу имеется только у аутентифицированного пользователя. Это достигается за счет хранения ключа в разделенном виде (в качестве участников разделения секрета выступают устройство и пользователь). Предложенная система защиты пользовательских ключей в мобильных приложениях является первой системой на основе разделения секрета, обладает хорошей встраиваемостью и может быть легко адаптирована для использования с существующими протоколами безопасности (SSL/TLS и т.п.).

Математические алгоритмы в основе аутентификации

1. (2, 2)-пороговая модулярная СРС

Рассмотрим (2, 2)-пороговую СРС [10], [2]. Алгоритм разделения секрета в этом случае принимает следующий вид:

1. Сгенерировать случайные попарно различные неприводимые многочлены $p_0(x), p_1(x), p_2(x); p_i(x) \in F_2[x], \deg p_i(x) = l+1, i = \overline{0,2}$;
2. Сгенерировать случайный равномерно распределенный одноразовый ключ $k(x) \in F_2[x], \deg k(x) = l$ и вычислить промежуточный секрет $S(x) = s(x) + kp_0(x)$;
3. Дилер публикует $p_i(x), i = \overline{0,2}$;
4. Дилер вычисляет частичные секреты $s_i(x) = S(x) \bmod p_i(x), i = \overline{1,2}$ и передает их участникам.

Алгоритм восстановления секрета имеет вид:

1. Участники передают вычисляющему устройству (дилеру) секреты $s_i(x), i = \overline{1,2}$;
2. Дилер вычисляет промежуточный секрет $S(x)$:

$$S(x) \equiv s_1(x)p_2(x)p_2^{-1}(x)_{p_1(x)} + \\ + s_2(x)p_1(x)p_1^{-1}(x)_{p_2(x)} \bmod p_1(x)p_2(x),$$

где $p_i^{-1}(x)_{p_j(x)} := p_i^{-1}(x) \bmod p_j(x)$.

3. Участники восстанавливают секрет $s(x) = S(x) \bmod p_0(x)$.

2. Генерация приватного ECDSA ключа

Стандарт ANSI X9.62[1] генерации приватного ECDSA не учитывает опасность использования ключей с малым весом Хемминга в NAF-

Виссия Херман Элизабет Мария Рене, *начальник филиала ИУП "Байлекс Малтимедиа", e-mail: h.vissia@byelex.com.*
Гафуров Сергей Владимирович, *начальник отдела филиала ИУП "Байлекс Малтимедиа".*
Каганович Дмитрий Михайлович, *студент кафедры информационных систем управления Белорусского государственного университета, сотрудник филиала ИУП "Байлекс Малтимедиа".*
Беларусь, 220028, г. Минск, ул. Маяковского, 111.
Галибус Татьяна Васильевна, *доцент кафедры информационных систем управления Белорусского государственного университета.*
Беларусь, 220013, г. Минск, пр. Независимости, 4.

[1] Схема разделения секрета