УДК 004.056.5 (045)

ВЫДЕЛЕНИЕ ХАРАКТЕРНЫХ ФРАГМЕНТОВ НА ИЗОБРАЖЕНИИ ЛИЦА ЧЕЛОВЕКА

Валериян Швец, Татьяна Нимченко, Виталий Васянович

Развитие информационных технологий тесно затрагивает и вопросы информационной безопасности частью, которой есть системы контроля и управления доступом на объекты информационной деятельности. Системы контроля и управления доступом для работы используют биометрическую идентификацию по изображению лица человека. Однако как показывает практика система контроля и управления доступом имеет один существенный недостаток – возможность подмены злоумышленником изображения реального человека его портретом, то есть попытка выдать портрет за реального человека, что может привести к проникновению злоумышленника на объект информационной деятельности. В статье рассматривается реализация детектора лица человека на изображении для возможности его реализации непосредственно контроллером видеокамеры и выделение характерных фрагментов в программном обеспечении системы с целью повышения надежности идентификации.

Ключевые слова: *информационная безопасность, идентификация, системы контроля и управления доступом, биометрическая идентификация, изображение лица.*

Введение. Современные системы контроля и управления доступом (СКУД) на объектах информационной деятельности используют биометрическую идентификацию по изображению лица человека. Это связано с тем, что традиционные средства идентификации личности во многих случаях оказываются недостаточно удобными. Распознавание лиц представляет собой бесконтактный и, возможно, наиболее естественный способ установления личности. Хотя для этого существует немало биометрических методов (например, использование отпечатков пальцев, изображений зрачка и радужной оболочки глаза, геометрии руки, особенностей голоса), все они в той или иной мере опираются на готовность пользователя сотрудничать с системой. В то же время распознавание лиц может быть осуществлено даже без ведома испытуемого.

Анализ проблемы. Как показывает практика, СКУД имеет один существенный недостаток – возможность подмены злоумышленником изображения реального человека его портретом, то есть попытка выдать портрет за реального человека (рис. 1) [1], что может привести к проникновению злоумышленника на объект информационной деятельности.

Одним из методов устранения данного недостатка получение изображения с нескольких камер с последующим формированием 3D портрета [1, 2]. Однако 3D распознавание является достаточно трудоёмким и дорогостоящим методом и поэтому возможно не все пользователи захотят его применять.

Авторами предлагается более дешевый метод устранение недостатка, описанного выше, а именно – анализ траекторий движения характерных точек на изображении лица человека, получаемых с уже используемых камер наблюдения.

а)

б)

Рис. 1. Подмена изображения реального человека портретом

Для реализации этого метода необходимо решить следующие задачи:

– детектирование лица человека на изображении и желательно чтобы это делала видеокамера на основе встроенных микроконтроллеров;

– выделение характерных фрагментов (областей) на изображении лица человека (глаза, нос, рот и т.д.);

– выделение контрольных точек на характерных фрагментах (областях) лица человека и последующий анализ траекторий их движения;

– получение ответа «портрет» или «реальный человек» по результатам анализа траекторий движения контрольных точек.

Решение этих задач не должно вносить значительных временных задержек, увеличивать объемы оборудования и его стоимость.

В статье рассматривается решение задачи детектирования лица человека на изображении и выделение характерных фрагментов.

Решение задачи. Реализацию задачи предложено осуществить в два этапа, на первом из которых происходит детектирование лица человека на изображении, тем самым сужая область поиска характерных областей; на втором – собственно поиск характерных областей на локализованном лице человека.

Детектирование лица на изображении. Корректное детектирование и выделение лица на изображении является основой для последующего анализа траекторий контрольных точек. Нельзя сказать, что эта задача решается впервые. Есть ряд программных продуктов OpenGL, OpenCV, MatLab в которых детекторы лица реализованы.

Авторами была проанализирована работа детекторов указанных программных продуктов и выявлены их недостатки. Детекторы MatLab не могут работать в реальном масштабе времени, детекторы OpenGL работают в операционной среде Windows и имеют закрытый программный код, детекторы OpenCV работают в операционной среде Windows, поддерживают только камеры с интерфейсом USB и не поддерживают работу «дешевых» WEB-камер (камеры не всех производителей поддерживаются OpenCV). Работа детекторов в операционной среде Windows делает невозможной их работу на аппаратном обеспечении видеокамер.

Детекторы лица можно реализовать, используя алгоритмы, приведенные в табл. 1.

Не смотря на недостаток первого алгоритма, он был взят для реализации детектора, потому что видеокамера СКУД передает информацию об изображении в цветовой схеме YC_bC_r, а это дает возможность переложить функции детектирования лица по цвету на контроллер видеокамеры. Для этого используется свойство хроматических компонент цветового пространства YC_bC_r видеокамеры для цветных изображений (цвет лица имеет постоянный оттенок, который не совпадает с цветом фона). В результате для цветных изображений лиц людей образовывается довольно компактный эллипс, содержащий информацию о местоположении лица на портрете (пиксели, которые лежат внутри эллипса определяются как «лицо», а пиксели, которые лежат за его пределами – как «не лицо») (рис. 2). По полученному эллипсу можно определить и координаты лица на изображении.

Таблица 1

Алгоритмы локализации лица

Алгоритм	Преимущества	Недостатки
Поиск по цвету	Высокая скорость обнаружения, возможность селекции по цвету кожи, не требует обучения, возможность реализации в самой видеокамере	Вероятность ложного обнаружения составляет от 10% до 15%
Корреляционные методы	Высокая Точность обнаружения	Крайне низкая скорость работы, требуется большая обучающая выборка с жесткими условиями съемки. Работа под управлением Windows.
Поиск по характерным точкам лица	Высокая точность и скорость обнаружения для изображений лиц крупным планом	Низкая точность и скорость обнаружения для изображений с несколькими лицами. Работа под управлением Windows.

Применяя данный метод, получаем оконтуренное лицо на изображении (рис. 3).

Поиск характерных областей на локализованном лице человека. Для поиска характерных областей, а именно областей глаз, носа и рта, используется метод интегральных проекций [4].

Метод интегральных проекций состоит из двух этапов: превращения цветного изображения лица в черно-белое (двух цветное, пиксель принимает два значения 0 или 1) изображение для построения интегральных проекций областей лица и выделения контрольных областей.

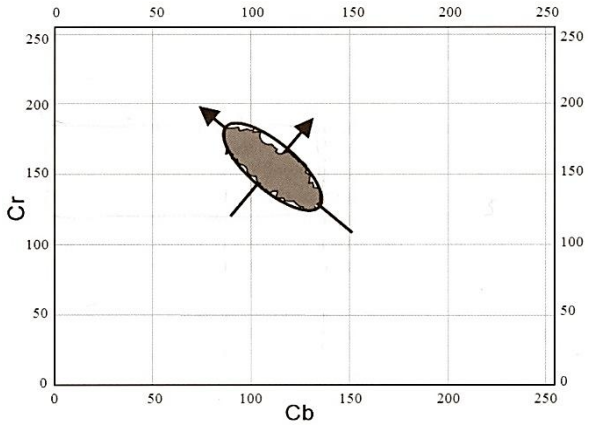

Рис. 2. Распределение хроматических компонент для изображения лица

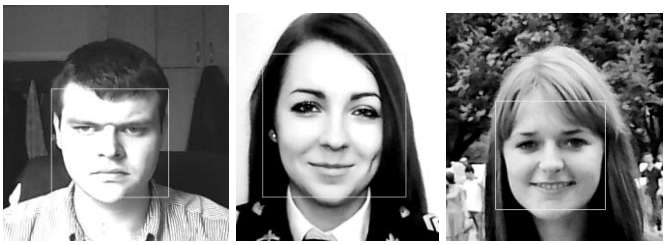

Рис. 3. Результат работы детектора по цвету лица человека на изображении

После преобразования цветного изображения лица в черно-белое, полученное изображение подвергается интегральному анализу. В результате проведения интегрального анализа, на выходе получаем график интегральной функции, который включает в себя четкие минимумы. Эти минимумы будут соответствовать местонахождениям характерных областей на изображении (рис. 4). Вторые производные интегральной функции будут давать характерные линии, которые будут проходить через самые темные участки изображения (рис. 4).

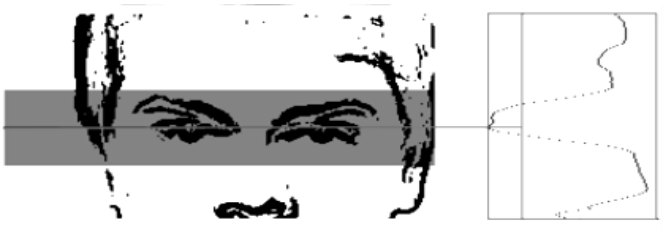

Рис. 4. Результат проведения интегрального анализа

Анализ метода интегральных проекций черно-белого изображения показал, что около 40% изображений имеют минимумы, которые вызывают нахождение ложных фрагментов на изображении лица. Для уменьшения ложных минимумов авторами предлагается преобразовывать изображение в оттенки серого (пиксель принимает значения от 0 до 255) с последующим ограничением снизу для проведения интегрального анализа.

Построение графика интегральной функции осуществляется по следующему алгоритму:

1. Изображения представляются в виде матрицы, элементы которой являются значениями оттенков серого каждого пикселя изображения.

2. Экспериментальным путем выбирается пороговое значение для анализа изображения (пороговое значение выбирается таким образом, чтобы график интегральной функции имел наиболее четкие минимумы).

3. Осуществляется горизонтальный и вертикальный интегральный анализ изображения. При горизонтальном интегральном анализе элементы каждой строки матрицы сравниваются с пороговым значением. На выходе получаем количество пикселей, значения которых превышают пороговое значение, в каждой строке. При вертикальном интегральном анализе вместо элементов строк матрицы сравниваются элементы ее столбцов.

4. Осуществляется построение графиков интегральной функции на основании полученных результатов горизонтального и вертикального интегрального анализа.

Результат горизонтального и вертикального интегрального анализа, а так же графики интегральных функций приведены на рис. 5 и 6. Экспериментально установлено, что при пороге равным 100 можно полностью устранить ложные минимумы.

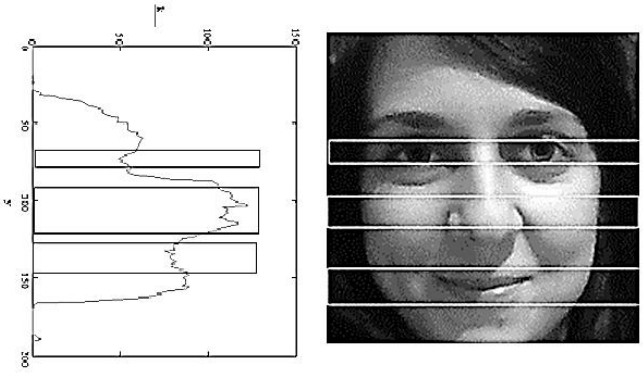

Рис. 5. Горизонтальный интегральный анализ и график интегральной функции

Вертикальный и горизонтальный интегральный анализ дает возможность уменьшить погрешность и более четко определить характерные области (глаза, рот и нос).

На рис. 7 представлен результат по выделению характерных фрагментов на изображении лица человека для последующего анализа траекторий движения контрольных точек.

Как видно из рисунка на различных изображениях достаточно точно выделяются характерные фрагменты лица человека.

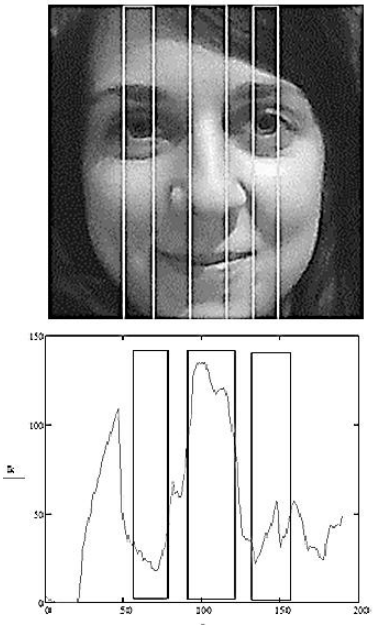

Рис. 6. Вертикальный интегральный анализ и график интегральной функции

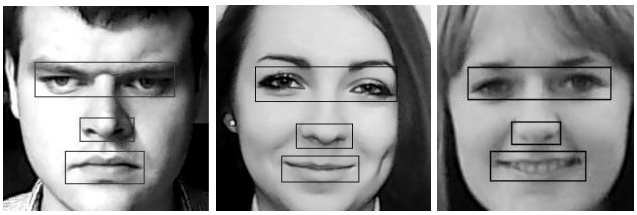

Рис. 7. Характерные фрагменты на изображении лица

Выводы. В работе предложен метод по повышению надежности распознавания человека в СКУД. Перечислены задачи для реализации предложенного метода. Проанализированы алгоритмы локализации лица. Выбран и проверен в работе детектор выделения лица по цвету. Реализован метод выделения характерных фрагментов на изображении лица человека. Реализация этих методов необходима для анализа траекторий контрольных точек на изображении.

ЛИТЕРАТУРА

[1]. 3D программа распознавания лиц [Электронный ресурс] − 2012. Режим доступа: http://www. youtube.com/watch?v=sXMV2TD8WYP.

[2]. Манолов А.И. Некооперативная биометрическая идентификация по 3D-моделям лица с использованием видеокамер высокого разрешения [Электронный ресурс] / А.И. Манолов, А.Ю. Соколов // Труды 19-й Международной конференции по компьютерной графике и зрению "ГрафиКон 2009", (Москва, 5 – 9 октября 2009 г.). – М.: МАКС ПРЕСС, 2009. – Режим доступа: http://gc2009. graphicon.ru/en /proceedings.

[3]. F Zuo, P H. N. de With. Fast Human Face Detection Using Successive Face Detectors with Incremental Detection Capability. In: Proc. International Conference on Visual Communications and Image Processing, Santa Clara, p. 831-841, 2003.

[4]. Лукьяница А.А., Шишкин А.Г. Цифровая обработка видеоизображений / А. А. Лукьяница, А. Г. Шишкин. - М.: "Ай-Эс-Эс Пресс", 2009. − 518 с.

[5]. Гонсалес Р. Цифровая обработка изображений в среде MATLAB / Р. Гонсалес, Р. Вудс, С. Эддинс. М.: "Техносфера", 2006. − 616 с.

REFERENCES

[1]. 3D facial recognition software [Electronic resource] - 2012. Mode of access: http://www.youtube.com / watch?v=sXMV2TD8WYP.

[2]. Manolov A. I. Non-cooperative biometric identification based on 3D models of faces using video cameras high resolution [Electronic resource] / A.I. Manolov, A.Y. Sokolov // Proceedings of the 19th International conference on computer graphics and vision GraphiCon 2009" (Moscow, 5 - 9 October 2009)., M.: MAKS PRESS, 2009., Mode of access: http://gc2009.graphicon.ru/en/proceedings.

[3]. F Zuo, P H. N. de With. Fast Human Face Detection Using Successive Face Detectors with Incremental Detection Capability. In: Proc. International Conference on Visual Communications and Image Processing, Santa Clara, p. 831-841, 2003.

[4]. Lucanica A.A., Shishkin A., Digital image and video processing / A.A. Lucanica, A., Shishkin. - M: "I-Es-Es Press", 2009, 518 p

[5]. Gonzalez R. Digital image processing in MATLAB / R. Gonzalez, R. Woods, S. Eddins. M: "Technosphere", 2006, 616 p.

ВИДІЛЕННЯ ХАРАКТЕРНИХ ФРАГМЕНТІВ НА ЗОБРАЖЕННІ ОБЛИЧЧЯ ЛЮДИНИ

Розвиток інформаційних технологій тісно зачіпає і питання інформаційної безпеки, частиною якої є системи контролю і управління доступом на об'єкти інформаційної діяльності. Системи контролю та управління доступом для роботи використовують біометричну ідентифікацію по зображенню обличчя людини. Однак, як показує практика, система контролю і управління доступом має один істотний недолік - можливість підміни зловмисником зображення реального людини його портретом, тобто спроба видати портрет за реального людини, що може призвести до проникнення зловмисника на об'єкт інформаційної діяльності. У статті розглядається реалізація детектора обличчя людини на зображенні для можливості його реалізації безпосередньо контролером відеокамери і виділення характерних фрагментів в програмному забезпеченні системи з метою підвищення надійності ідентифікації.

Ключові слова: інформаційна безпека, ідентифікація, системи контролю та управління доступом, біометрична ідентифікація, зображення особи.

THE SELECTION OF CHARACTERISTIC FRAGMENTS IN THE IMAGE OF A HUMAN FACE

The development of information technology is closely touches on the issues of information security part, which is the control system and access control objectives for information and activities. Control systems and access control for use biometric identification by the image of a human face. However, as practice shows, the control system and access control has one major drawback is the possibility of an attacker tampering with the image of a real person his portrait, that is, the attempt to present a portrait of a real person, which can lead to the penetration of the attacker on the object information activities. The article discusses the implementation of the detector of the human face in the image to the possibilities of its implementation directly by the controller of the camera and the selection of characteristic fragments in the software system to improve the reliability of the identification.

Index terms: information security, identification, access control systems and access control, biometric identification, a facial image.

Швец Валеріян Анатолійович, кандидат технічних наук, доцент, доцент кафедри засобів захисту інформації Національного авіаційного університету.
E-mail: hvan@nau.edu.ua

Швец Валериян Анатольевич, кандидат технических наук, доцент, доцент кафедры средств защиты информации Национального авиационного университета.
Valerian Shvets, PhD, Associate Professor of the Academic Department of of information security tools National Aviation University.

Німченко Тетяна Васильовна, кандидат технічних наук, доцент кафедри засобів захисту інформації Національного авіаційного університету.
E-mail: fiona54@ukr.net
Нимченко Татьяна Васильевна, кандидат технических наук, доцент кафедры средств защиты информации Национального авиационного университета.
Tatyana Nimchenko, PhD, Associate Professor of the Academic Department of information security tools National Aviation University.

Васянович Віталій Васильович аспірант кафедри засобів захисту інформації Національного авіаційного університету.
E-mail: vasianovichv@ukr.net
Васянович Виталий Васильевич аспирант кафедры средств защиты информации. Национального авиационного университета.
Vitaly Vasyanovych, postgraduate student of the Department of information security tools National aviation University.

УДК 003.26.09: 004.056.55

САМОТЕСТУВАННЯ ТА КОНТРОЛЬ ЦІЛІСНОСТІ КЛІЄНТСЬКОГО КОДУ МЕРЕЖНОГО ІНФОРМАЦІЙНОГО РЕСУРСУ

Денис Самойленко

Для убезпечення інформації від несанкціонованого доступу при мережній організації комунікації необхідно реалізовувати засоби перевірки якими програмними засобами було сформовано запит на її одержання. Існуючі засоби дозволяють реалізовувати захист та перевірку на справжність пасивних об'єктів шляхом включення до них цифрових «водяних» знаків. У статті розглянуто ряд способів автоматичного контролю цілісності клієнтського коду мережних інформаційних ресурсів. Показано низьку ефективність способів, побудованих на аналізі HTML коду ресурсу, рекомендовано реалізовувати розподілені засоби самотестування. Запропоновано методику одержання псевдо-поліморфного коду, використовуючи динамічну заміну елементів однакової семантики. Методика випробувана на ряді популярних браузерів, відзначено особливості та застереження щодо її використання. Реалізація запропонованих заходів дозволить покращити інформаційну безпеку мережних ресурсів.

***Ключові слова**: інформаційна безпека, мережні ресурси, захист даних, самотестування, цілісність.*

Постановка проблеми у загальному вигляді. Розвиток інформаційних технологій, трансформація способів спілкування, прискорення обмінних процесів призвели до формування нового типу комунікаційних відносин – інформаційного суспільства. Пріоритетність розвитку суспільства саме такого типу зазначається у відповідному Законі України [1]. Як правило, відображенням особи (фізичної чи юридичної) у інформаційному просторі виступає мережний інформаційний ре-