пользователем пароль также зашифровывается и сравнивается с хранящимся зашифрованным значением. Дважды неправильно ввод пароля – отказ в обслуживании и блокировка абонента, затем регистрация в журнале защиты попытки НСД.

Генерация ключей. Для каждого пользователя генерируются личные ключи – для его последующей аутентификации и для передачи (хранения) информации высокой степени секретности соответственно ее владельцу. Схема генерации и рассылки ключей может базироваться на одном из популярных протоколов ключевого соглашения при условии выполнения требуемой криптостойкости P. Генерация гаммы может осуществляться через реализацию алгоритмов формирования последовательности псевдослучайных чисел (например, ANSI X9.17), которых разработано достаточно много. Опубликованные в известных работах наборы псевдослучайных чисел не могут гарантировать надежность криптопреобразований $P_{зад}$. В дальнейшем планируется разработка оригинальных алгоритмов формирования последовательности псевдослучайных чисел.

Применение подобных схем криптопреобразований дает удовлетворительные характеристики надежности для сохранения конфиденциальности информации различной степени секретности при организации многоуровневого контроля доступа.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Горковенко Е.В.* Методология защиты при нормативном контроле доступа к информации. Управление защитой информации. – М.: ВНИИПВТИ. Том 11. 2007. №4. – С.427-432.

2. СТРК 1073-2002 «Средства криптографической защиты информации» // Общие технические требования. – Астана: Госстандарт РК, 2002.

3. *Бияшев Р.Г., Горковенко Е.В.* Шифраторы информации с заданной криптостойкостью. // Труды международной научно-практической конференции «Состояние, проблемы и задачи информатизации в Казахстане», КазНТУ им. К. Сатпаева. – Алматы, 2004. – С.27-37.

4. Анализ состава ключевой информации в соответствии с длиной шифруемого пакета // Раздел 1 промежуточного отчета «Разработка технологий по информационной безопасности (криптографическая защита информации на основе нетрадиционных подходов)», номер госрегистрации №0103РК00120, инвентарный номер №0204РК00016. – Алматы: ИПИУ, 2004. – С.14-25.

УДК 681.034

Д.П. Рублёв, В.М. Фёдоров, А.Б. Чумаченко, О.Б. Макаревич

УСТАНОВЛЕНИЕ АВТОРСКИХ ПРАВ ПО НЕОДНОРОДНОСТЯМ ЦИФРОВЫХ ОБРАЗОВ*

Одной из актуальных задач защиты информации является разработка методов защиты от копирования мультимедийных данных и как несанкционированного использования аппаратуры для их создания, так и производства контрафактной продукции. Это связано с массовым переходом на цифровые технологии получения, обработки, отображения и хранения мультимедиа информации. Благодаря этому практически полностью устранены изначально присущие аналоговым уст-

* Работа выполнена при поддержке грантов РФФИ №08-07-00253-а, № 08-07-00117а.

ройствам записи недостатки, а именно зависимость от наличия расходных материалов, их качества, существенная ограниченность возможностей для пользователя по редактированию получаемых записей, неизбежное ухудшение качества записей при копировании и ограниченный срок их хранения. Однако эти же преимущества дают возможность неограниченного тиражирования медиазаписей и затрудняют выявление источника контрафактных копий. Наиболее распространенным методом защиты от несанкционированного копирования является использование цифровых водяных знаков (ЦВЗ). Метод заключается во встраивании в защищаемый объект невидимых меток ЦВЗ путём модификации области данных.

Методы ЦВЗ начали разрабатываться сравнительно недавно, в связи с чем имеется ещё много неясных проблем, требующих своего разрешения. Применение ЦВЗ подразумевает использование вычислительных ресурсов и специального программного обеспечения для их встраивания. Во многих случаях осуществить встраивание ЦВЗ непосредственно при создании цифровых мультимедийных данных затруднительно, так как связано с необходимостью модификации внутреннего ПО устройства записи.. Таким примером является, например, использование неспециализированных цифровых фотокамер либо записи на цифровой магнитофон. Так как встраивание стойких водяных знаков необратимо модифицирует контейнер, то при требовании целостности контейнера их применение также невозможно.

В то же время, применение ЦВЗ не всегда является необходимым, так как уникальные характеристики элементов и узлов устройств записи также оказывают влияние на создаваемые образы. В связи с тем, что в цифровом тракте параметры элементов в штатном режиме ошибок не вносят, идентификацию необходимо производить по параметрам аналоговых узлов до оцифровки сигнала включительно.

Идентификация цифрового образа даже одной природы, например, цифрового изображения, существенно зависит от источника и применяемых алгоритмов постобработки. В случае фотокамер можно выделить следующие аппаратные свойства на основе которых возможно проведение идентификации: Объектив и система крепления (байонет) (формирует среднеустойчивые признаки), фильтр размытия (формирует средне- и высокочастотные устойчивые признаки), модуль светочувствительной матрицы (формирует устойчивые признаки всех частот) [1,2,3]. Для сканеров изображений таковыми являются дефекты и неоднородности светочувствительных элементов линейки сканера, отклонения перемещения каретки сканера от линейного, неравномерность засветки и прижатия к стеклу оригинала и т.д. Для цифровых микрофонов и диктофонов первой группой признаков являются отклонения от средней АЧХ-микрофона, внутренние наводки на аналоговую часть, отклонения характеристик АЦП, нестабильность генераторов тактовой частоты и т.д.

Кроме того, качество полученного изображения в значительной степени определяется также применёнными алгоритмами постобработки изображения, так в цифровых камерах, оказывающим наибольшее влияние на полученное изображение, являются алгоритмы восстановления изображения из мозаичной структуры сенсора [4], повышения контурной резкости и шумоподавления. В большинстве наиболее распространённых фотокамер нижнего ценового сегмента алгоритмы постобработки являются неотключаемыми. В цифровых сканерах получаемое изображение может проходить двухуровневую обработку – в самом сканере на основе калибровочных кривых, подавления следов пыли и на уровне драйвера, где осуществляется субъективное повышение качества изображения. В большинстве наиболее распространённых фотокамер нижнего ценового сегмента алгоритмы постобработки являются неотключаемыми.

Ввиду того, что алгоритмы постобработки являются общими иногда для всех моделей одного производителя, для выявления экземплярно-уникальных признаков необходимо проводить идентификацию по параметрам аналогового участка, т.е. по первому классу признаков. Авторами была исследована возможность идентификации по полученным с них цифровых изображений фотокамер и сканеров по имеющемуся цифровому изображению цифровой фотокамеры либо сканера, при помощи которого оно было получено.

В фотокамерах светочувствительные элементы расположены либо в узлах тетрагональной решётки в соответствии со структурой Байера, либо гексагональной решётки, благодаря которым учитываются особенности человеческого зрения, а именно большая разрешающая способность в яркостной области и максимум чувствительности в жёлто-зелёной области спектра. Каждый элемент матрицы обладает максимумом чувствительности в области только одной цветовой компоненты, а недостаток цветового разрешения частично компенсируется применением эвристик в алгоритмах восстановления (интерполяции) отсутствующих значений. При этом восстановленное изображение изначально характеризуется пониженной разрешающей способностью в области цветности. При этом используется только один светочувствительный сенсор, перед которым размещен решетчатый цветовой фильтр, в английской терминологии color filter array (CFA). Такая решетка Байера использует своеобразное расположение фильтров трех цветов, расположенных согласно схеме, показанной на рис. 1, где R, G и B соответственно фильтры красного, зеленого и синего цветов. Число пикселей с фильтрами зелёного цвета в два раза больше числа пикселей красного и синего, что связано с особенностями спектральной чувствительности глаза человека, максимум которой приходится на жёлто-зелёную область.

G	R	G	R	G	R
B	G	B	G	B	G
G	R	G	R	G	R
B	G	B	G	B	G
G	R	G	R	G	R
B	G	B	G	B	G

Рис. 1. Модель Байера (CFA)

В большинстве случаев, встречающихся на практике, требуется установить принадлежность изображения конкретной фотокамере, при этом изображение доступно, как правило, только в формате компрессии с потерей качества. Случаи, когда доступным может быть RAW- изображение, подвергнутое только коррекции пиксельных дефектов и вычитанию темнового кадра, либо компрессированное (обычно в формате TIFF) изображение, прошедшее все ступени внутрикамерной обработки, кроме компрессии с потерей качества, встречаются значительно реже, что объясняется тем, что их получение возможно только в камерах, начиная с верхнего ценового диапазона любительских камер [2].

Сигнал $s(x, y)$, получаемый с отдельного светочувствительного элемента матрицы, может быть рассмотрен как:

$$s(x, y) = B(x, y) + tD(x, y) + tG(x, y)I(x, y) + n,$$

где $B(x, y)$ – ток смещения,

$D(x, y)$ – темновой ток,

$G(x, y)$ – чувствительность элемента,

$I(x, y)$ – световой поток на элементе,

n — неучтённые шумовые составляющие.

Компенсация тока смещения и темнового тока пикселя составляющих $B(x, y)$ и $D(x, y)$ осуществляется при внутренней первичной обработке, зачастую ещё до формирования выходного изображения, подвергающегося в дальнейшем компрессии, соответственно идентификация камер на основе данных компонент затруднена. Некомпенсированной является компонента $G(x, y)$, которая отражает неодинаковую чувствительность элементов и вносит, таким образом, мультипликативную неоднородность [5]. Как показали эксперименты, разброс чувствительности светочувствительных элементов достаточен для проведения идентификации камер на его основе.

Ввиду того, что в фотокамерах в целях повышения чувствительности плотность цветных светофильтров перед элементами невелика, а также учитывая интерполяционный способ восстановления цветов, в наибольшей степени неоднородности проявляются в яркостной области изображения. Соответственно, целесообразно полноцветные изображения предварительно переводить в градации “серого” и дальнейшую обработку осуществлять над чёрно-белым изображением. Ввиду мультипликативного характера неоднородности, вносимой компонентой $G(x, y)$, получение карты распределения неоднородностей производилось усреднением на множестве кадров. Снижение количества кадров, необходимых для получения усреднённых значений неоднородностей пикселей может быть достигнуто предварительным выделением из изображения высокочастотной части (шумов) [1]. Для этих целей были рассмотрено применение вейвлет-фильтров и фильтра Винера. Критерием эффективности фильтра являлось отсутствие следов, коррелированных с низкочастотной структурой изображения в полученной ВЧ-составляющей. Наилучшие показатели были получены при использовании двумерного фильтра Винера с размерностью окна от 3x3 до 7x7.

Для идентифицируемой камеры находится усреднённое значение неоднородностей W_{apprx} чувствительностей пикселей. Идентификация камеры по имеющемуся изображению I_q производится по значению коэффициента корреляции яркостной составляющей изображения и W_{apprx}.

Исследования метода проводились на основе выборок изображений, полученных с 5 камер. Каждая выборка была сформирована 300 различными изображениями, полученными с одной фотокамеры в максимальном разрешении без какой-либо постобработки, 200 из которых использовались на этапе построения карты неоднородностей и 100 на этапе тестирования. Ввиду различной разрешающей способности фотокамер для построения карты неоднородностей использовался центральный участок кадра размером 1024x1024 пикселя.

В ходе экспериментов метод позволил верно классифицировать все изображения, при этом разница оценок математических ожиданий коэффициентов корреляции составила 2 порядка при неперекрывающихся распределениях. Модификации данного метода позволяют также производить идентификацию цифровых микрофонов [6].

Для идентификации сканеров данный подход должен быть изменён вследствие специфики получения изображений со сканеров. В фотокамерах применяется двумерная светочувствительная матрица, в то время как в наиболее распространённых планшетных сканерах – линейка светочувствительных элементов, механически перемещаемая вдоль изображения. Планшетные сканеры построены по принципу плоской развертки, при которой считываемый оригинал располагается на плоском подвижном или неподвижном держателе и при сканировании осуществляется построчное считывание изображения. В качестве приемников в большинстве сканеров используются линейные ПЗС, на которые объектив или линза проецирует изображение строки. Наиболее распространена схема, в которой чувствительные к каждой цветовой компоненте элементы формируют три светочувствительные линейки. Таким образом, несмотря на то, что идентификация как сканеров, так и фотокамер производится на основе двумерных матриц яркости, идентифицирующие признаки сканера и фотокамеры существенно отличаются. Как показали проведённые исследования, построение образа неоднородностей по аналогично применяемому для идентификации камер неэффективно. Основной источник коррелированного шума, вносимого сканером в направлении движения сканирующей каретки, – неоднородность элементов ПЗС- либо CIS-линейки, выражающаяся в повышенном уровне шума, отклонении цветового оттенка и т.д. В эту же категорию попадают искажения, вносимые неравномерностью засветки оригинала. Данные неоднородности проявляются в виде вертикальных линий, областей и т.д., соответствующих отдельным пикселям светочувствительной линейки. Источниками шума, вносимого сканером в направлении, перпендикулярном движению сканирующей каретки, являются нестабильная интенсивность света лампы, неплотное прижатие оригинала к стеклу, наводки на электронные компоненты. В данной работе была исследована возможность идентификации сканеров на основе неоднородностей светочувствительных линеек.

Идентификация сканеров производилась аналогично идентификации фотокамер. Для двух сканеров на основе ПЗС-линеек было получено по 65 различных изображений, 32 из которых формировали выборку для формирования отпечатка сканера, а 33 – тестовую выборку. На первом этапе идентификации создавался идентифицирующий отпечаток сканера. Для этого из каждого полноцветного немасштабированного изображения, полученного с идентифицируемого сканера, производилось выделение высокочастотной составляющей цветовых компонент с последующим усреднением по всем изображениям выборки:

$$\bar{I}_{HF_{RGB}} = \frac{\sum_{k=1..n} I_{k_{RGB}} - Wiener(I_k)}{n},$$

и находилась оценка математического ожидания значения каждого столбца пикселей:

$$\mu_{j\,RGB} = \frac{\sum_{i=1..height} RGB(i,j)}{height}.$$

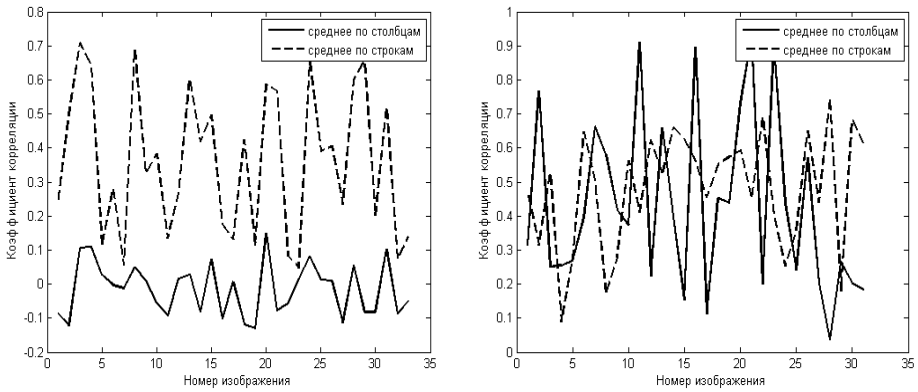
Автокорреляция полученной одномерной матрицы является отпечатком сканера:

$$ID_{RGB} = ifft(fft(\mu_{RGB}) \cdot conj(fft(\mu_{RGB}))) \cdot$$

Для установления принадлежности изображения сканеру, отпечаток которого имеется, из изображения производится выделение ВЧ-области и далее находится значение ID_{RGB}. Далее для сформированной матрицы строится автокорреляционная функция и находится коэффициент корреляции с имеющимся отпечатком сканера. Значения коэффициента корреляции по строкам и столбцам полученного отпечатка сканера и двух выборок изображений, одна из которых получена при помощи этого же сканера, приведены на рис. 2 и 3.

Сканирование проводилось на основе при разрешении 300 dpi при оптическом разрешении сканеров 1200 dpi, так как наибольший интерес представляет идентификация сканеров на основе оригиналов низкого качества. В частности, для сканеров таковыми являются оригиналы, содержащие типографский растр, регулярные структуры с периодом, сопоставимым с разрешением сканера.

Таким образом, разница коэффициентов корреляции позволяет идентифицировать сканер в варианте выбора одного из нескольких и разрешении в 300 dpi. Проведённые исследования показали, что на точность классификации при низких разрешениях значительное влияние оказывают регулярные структуры в изображении, по масштабу сопоставимые с разрешением сканирования (типографский растр). Также была установлена возможность идентификации сканеров по признакам, вносимым в изображение работой механической части и алгоритмами постобработки изображения.

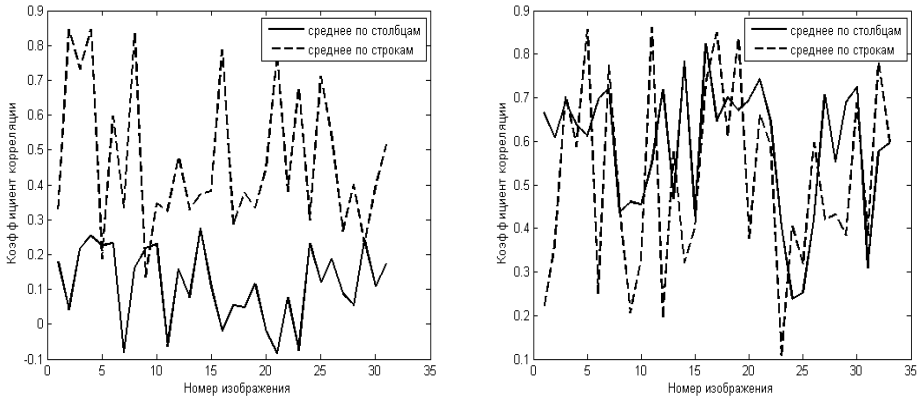


а б

Рис. 2. Корреляция отпечатка сканера №1 и отпечатков изображений из выборки, полученной при помощи сканера №1 (а) и сканера №2 (б)

В дальнейшем будет исследована возможность идентификации по признакам пространственной и частотной областей, вносимым нестабильностью светового

потока лампы подсветки, работой механической части сканера, аддитивными шумами сенсоров ПЗС-линейки.



а б

Рис. 3. Корреляция отпечатка сканера №2 и отпечатков изображений из выборки, полученной при помощи сканера №2(а) и сканера №1 (б)

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Jan Lukáš, Jessica Fridrich, and Miroslav Goljan* Determining Digital Image Origin Using Sensor Imperfections. Proceedings of the SPIE-2005, Vol. 5685, pp. 249-260.

2. *Mehdi, K.L. Sencar, H.T. Memon, N.* Blind source camera identification. International Conference on Image Processing, 2004, Vol. 1, pp. 709- 712.

3. *Lukáš J., Fridrich J., and Goljan M.*: "Determining Digital Image Origin Using Sensor Imperfections", Proc. SPIE Electronic Imaging, Image and Video Communication and Processing, San Jose, California, January 16–20, 2005, pp. 249–260.

4. *Kharrazi, M., Sencar, H. T., and Memon, N.*: "Blind Source Camera Identification", Proc. ICIP' 04, Singapore, October 24–27, 2004. pp. 312-317.

5. *Рублёв Д.П., Чумаченко А.Б.* Идентификация цифровых фотокамер по карте светочувствительности матрицы // XIII Всероссийская научно-практическая конференция "Проблемы информационной безопасности в системе высшей школы". – М.: МИФИ, 2007. – С. 78-79.

6. *Рублёв Д.П., Чумаченко А.Б., Макаревич О.Б., Фёдоров В.М.* Идентификация цифровых микрофонов по неидеальностям тракта записи // Известия ЮФУ. Технические науки. Тематический выпуск "Информационная безопасность". – Таганрог: Изд-во ТТИ ЮФУ, 2007. – С. 84-92. №1(76).

УДК 681.324

Ю.А. Брюхомицкий

КЛАССИФИКАЦИЯ НЕСТАЦИОНАРНЫХ ВЕРОЯТНОСТНЫХ БИОМЕТРИЧЕСКИХ ПАРАМЕТРОВ ЛИЧНОСТИ*

Применяемые в настоящее время динамические биометрические системы идентификации (БСИ) личности (по голосу, рукописному и клавиатурному почеркам) основаны на анализе индивидуальных особенностей динамики подсознатель-

*Работа выполнена при поддержке грантов РФФИ: № 08-07-00117а; № 06-07-96609-р_юг_а, 06-07-89010-а.