УДК 681.322.067

И. З. Климов, доктор технических наук, профессор, ИжГТУ имени М. Т. Калашникова
Р. Бустами, магистрант, ИжГТУ имени М. Т. Калашникова

ИССЛЕДОВАНИЕ И РАЗРАБОТКА АЛГОРИТМА ШИФРОВАНИЯ ОПРЕДЕЛЕННОЙ ОБЛАСТИ ИЗОБРАЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА ВИОЛЫ – ДЖОНСА

В настоящее время фотографирование на мобильный телефон с последующим сохранением в облаке результатов широко распространено, что, в свою очередь, привело к попыткам несанкционированного доступа к таким данным. Существенную роль в этом процессе играет халатность самих участников. Облачные системы в настоящее время широко используются, так как скорость интернета возросла, и в мобильных телефонах, таких как I-phone и android, такие возможности, как правило, заложены. Поэтому пользователи, как и мультимедиа, кроме стандартных возможностей таких средств используют свои мобильные телефоны для фотосъемки и создания видеоинформации.

Кроме того, селфи становится популярной тенденцией, позволяющей создать видеоизображение с собственного мобильного телефона. Камера такого телефона должна быть разработана специально с увеличенными пикселами. Это связано, в частности, с тем, чтобы полученные цифровые изображения подходили для просмотра на персональном компьютере и даже для печати.

Недавно актрисы Голливуда, предполагая, что облако, созданное компанией Apple.inc достаточно защищено, сохраняли свои фотографии в Я-облако, которое подключается автоматически с мобильного телефона [1]. Однако хакерам удалось взломать защиту системы Apple, что фактически привело к вторжению в частную жизнь. Ко всему прочему оказалось, что после того, как фотографии просочились в СМИ, практически ничего сделать нельзя из-за отсутствия юридических основ для возврата фотографий.

Аналогичная проблема возникает при попадании мобильного телефона в чужие руки. Если даже мобильный телефон защищен паролем, этого недостаточно, так как злоумышленник может получить доступ к данным с помощью карты памяти.

Другая опасность состоит в массовом использовании цифрового изображения в других аспектах. Так, часто сканируют фото для использования в различных документах, которые при попадании в чужие руки приводят к различным злоупотреблениям.

Предлагается метод защиты цифровой фотографии, в частности селфи. В сооветсвии с Оксфордским словарем под селфи понимается фотография самого себя с помощью смартфона или веб-камеры и отправка фотографии с помощью социальных медиа. При этом возникает, естественно, возможность вторжения посторонних в частную жизнь владельца селфи.

В настоящей статье предлагается метод шифрования только наиболее важной области фотографии. Для селфи такой областью является особо важная область пикселов, представляющая лицо или его часть. При такой операции лицо должно обнаруживаться автоматически для последующего дешифрования. Основываясь на этой идее, очевидно, можно сократить время обработки для шифрования и дешифрования изображения и обеспечить наилучшую конфиденциальность фотографий.

Для обнаружения лица в фотографии использован алгоритм Виолы – Джонса [2]. Для шифрования данных использованы стандартные алгоритмы DES и ГОСТ [3, 4, 5, 6] с одноразовым блокнотом с помощью хаоса [7].

В эксперименте выделено четыре основных шага. Первый шаг – обнаружение лица с помощью алгоритма Виолы – Джонса.

Прежде всего на этом шаге цифровое изображение преобразуется в значение пиксела. Далее лицо обнаруживается алгоритмом Виолы – Джонса (рис. 1). Координаты пикселов (x, y), а также длина обнаруженной части сохраняются в базе данных.

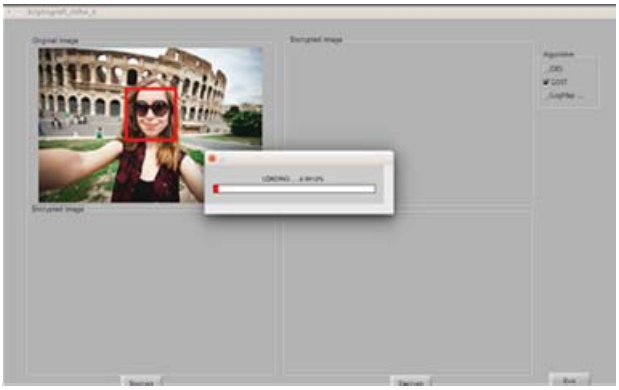

Рис. 1. Первый шаг – обнаружение лица алгоритмом Виолы – Джонса

Второй шаг – подготовка выбранного изображения для шифрования выделенного блока алгоритмами DES или ГОСТ. Для этого значение пиксела преобразуется в двоичные данные длиной 64 бит и используется 64-битный ключ для DES и 256-битный ключ для ГОСТ (рис. 2).

Третий шаг – процесс шифрования и дешифрования (рис. 3). Работа с подготовкой шифрования зависит от используемого криптографического алгоритма – DES, ГОСТ или логистическая карта One time pad.

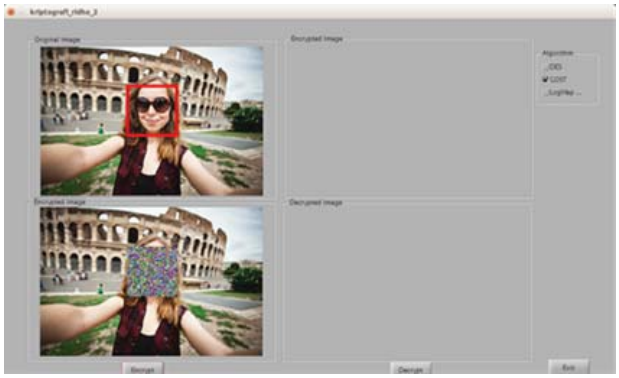

Рис. 2. Результат шифрования изображения путем перестановки пикселов

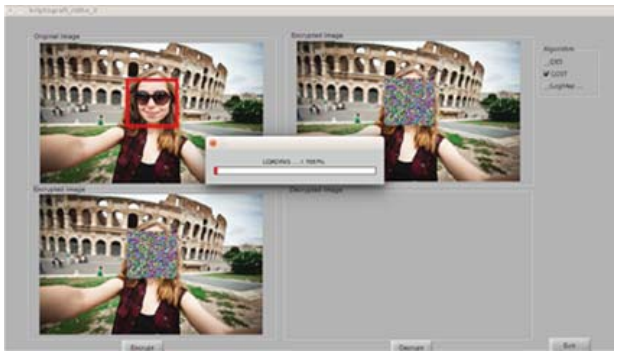

Рис. 3. Загрузка координат в шифрованные изображения для процесса дешифрования

Заключительным этапом является сбор и перестановки в изображении (рис. 4). На этом шаге после процесса шифрования или дешифрования пикселы, которые уже зашифрованы или расшифрованы, должны быть собраны и перестроены в основное изображение. Координаты точки и длина берутся из базы данных.

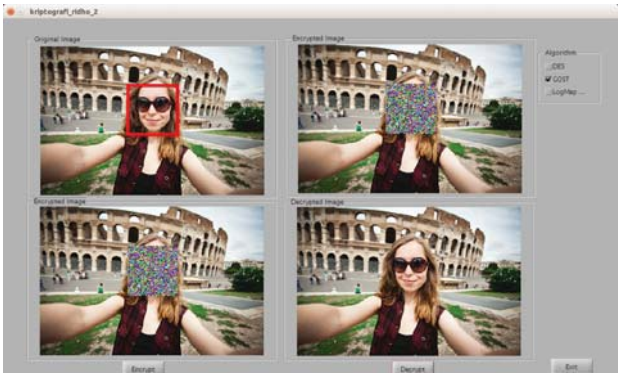

Рис. 4. Результат дешифрования процесса и перестановки пикселов

Для реализации симуляции использован Matlab 2012. Разработан также графический пользовательский интерфейс. На первом этапе мы просто загружаем селфи. После этого программа непосредственно обнаруживает объект шифрования. Для дешифрования процесса кроме ключа необходимо знать характер зашифрованной информации.

Графический пользовательский интерфейс для моделирования работает в среде Matlab 2012 с операционной системой Linux. Спецификация оборудования Intel сердечника i3-2356M 1,40 ГГц, ОЗУ 3,87 ГБ. Изображения с форматом .bmp (33×73 пикселов, 24 бит глубина) была испытана, использовано шифрование и дешифрование с алгоритмами Des, ГОСТ и логистической картой Logistic map. Результаты рассчета среднего времени обработки приведены в таблице.

Сравнение времени обработки между DES, ГОСТ и Logistic map – One time pad

Алгоритмы	DES	ГОСТ	Logistic map – One time pad
Скорость обработки, пиксел/сек.	4,8150	5,5313	8,5702
Шифрование обработки, пиксел/сек.	124,7029	183,2866	0,098226
Дешифрование обработки (второй) (33×73 пикселов, 24 бит глубина)	244,5134	371,2706	0,0865

Полученные результаты показали, что алгоритм Виолы – Джонса успешно обнаруживает лицо на фотографии.

Разработанный метод может быть реализован также с помощью алгоритма блочного шифрования или криптографии, основанной на хаосе. Оба стандарта – ГОСТ и Des – медленнее (время обработки – до получаса), чем алгоритм logistic map – one time pad.

Библиографические ссылки

1. *Cooper G.* Jennifer Lawrence nude photos leak : The risks of cloud storage. – URL: http://www.telegraph.co.uk/technology/technology-video/11067666/Jennifer-Lawrence-nude-photos-leak-the-risks-of-cloud-storage.html (дата обращения: 20.10.2014).

2. *Viola P.*, *Jones M. J.* Rapid Object Detection using a Boosted Cascade of Simple Features // Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. – 2001. – Vol. 1. – Pp. 511–518.

3. Federal Information Standards Publication 46-3. Digital Encryption Standard (DES). Gaitherenburg: U.S. DEPARTMENT OF COMMERCE / National Institute of Standards and Technology, 1999. – 22 с.

4. ГОСТ ССР 28147–89. Алгоритм криптографического преобразования. – М. : Изд-во стандартов, 1990. – 26 с. – Системы обработки информации. Защита криптографическая.

5. *Шнайер Б.* Прикладная криптография : Протоколы, алгоритмы, исходные тексты на языке Си. – С. 370–454.

6. *Bustami R.* Research and Development of the Encryption Algorithm in Specific Area of Digital Image // Приборостроение в XXI веке – 2015.

7. *Bustami R*. Implementation Image Encryption Algorithm with One-time Pad and Pseudo-random Chaos in Java // Приборостроение в XXI веке – 2015.

Получено 25.07.2016