рами 1 и 2 позволяет оценить относительную ширину СП. Таким образом, анализ трех первых коэффициентов ДПФ энергетического спектра позволяет принять решение о наличии или отсутствии значительной СП и оценить ее относительную ширину. Решение о наличии значительной СП позволяет перейти к пороговому обнаружению ее положения на дискретной оси частот.

Оценки среднего и дисперсии квадратов модуля коэффициентов ДПФ с номерами 1 и 2

№ линии	q^2_c	$\delta_\Delta = 0{,}1$		$\delta_\Delta = 0{,}2$		$\delta_\Delta = 0{,}4$		$\delta_\Delta = 0{,}6$	
		среднее	дисперсия	среднее	дисперсия	среднее	дисперсия	среднее	дисперсия
1	0	$6{,}7\cdot10^{-3}$	$4\cdot10^{-5}$	–	–	–	–	–	–
	5	0,568	$2\cdot10^{-3}$	0,517	$1{,}2\cdot10^{-3}$	0,34	$7{,}1\cdot10^{-4}$	0,153	$4{,}4\cdot10^{-4}$
	10	0,728	$1\cdot10^{-3}$	0,661	$6{,}2\cdot10^{-4}$	0,434	$5{,}6\cdot10^{-4}$	0,195	$4{,}8\cdot10^{-4}$
	100	0,939	$3{,}7\cdot10^{-5}$	0,851	$1{,}1\cdot10^{-4}$	0,556	$5{,}2\cdot10^{-4}$	0,249	$5{,}9\cdot10^{-4}$
	1000	0,965	$1{,}5\cdot10^{-5}$	0,874	$1\cdot10^{-4}$	0,572	$5{,}4\cdot10^{-4}$	0,256	$6{,}1\cdot10^{-4}$
2	0	$6{,}1\cdot10^{-3}$	$3{,}8\cdot10^{-5}$	–	–	–	–	–	–
	5	0,513	$1{,}8\cdot10^{-3}$	0,34	$9{,}6\cdot10^{-4}$	0,035	$2{,}1\cdot10^{-4}$	0,018	$1{,}1\cdot10^{-3}$
	10	0,658	$1\cdot10^{-3}$	0,435	$8{,}4\cdot10^{-4}$	0,044	$2{,}7\cdot10^{-4}$	0,022	$1{,}1\cdot10^{-3}$
	100	0,851	$2{,}1\cdot10^{-4}$	0,561	$8{,}7\cdot10^{-4}$	0,056	$3{,}8\cdot10^{-4}$	0,027	$1{,}1\cdot10^{-3}$
	1000	0,875	$2\cdot10^{-4}$	0,576	$9{,}1\cdot10^{-4}$	0,058	$3{,}9\cdot10^{-4}$	0,028	$1{,}2\cdot10^{-3}$

Провалы в обнаружении, обусловленные флуктуациями спектральной плотности СП, могут быть ликвидированы специальной обработкой решений, предусматривающей инверсию решений порогового обнаружения в сравнительно узких интервалах между превышениями порога. Для блоковой обработки, т. е. при использовании n_p ШПС, оценка энергетического спектра, поступающая на анализ определения СП, будет характеризоваться значительно меньшим уровнем флуктуаций дискретных линий по сравнению с рассмотренным случаем оценок спектра на минимальном интервале. Дисперсия флуктуаций дискретных линий уменьшиться в n_p раз.

Таким образом, усреднение приводит к значительному уменьшению быстрых (флуктуационных) изменений оценки энергетического спектра.

Получено 13.09.2016

Библиографические ссылки

1. *Комарович В. Ф.*, *Сосунов В. Н.* Случайные помехи и надежность КВ-связи. – М. : Связь, 1977. – 136 с.

2. *Тузов Г. И.*, *Поставной В. И.*, *Мудров О. И.* Исследование влияния режекции спектров сложных частотно-фазоманипулированных сигналов на их корреляционные свойства // Радиотехника. – 1988. – № 10. – С. 30–33.

3. Там же.

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

Защита информации от третьих сторон и обеспечение конфиденциальности данных является одной из задач криптографического обеспечения. В настоящей работе авторами предложен результат создания и технической реализации алгоритма шифрования определенных частей цифровых изображений. Разработка выполнена для широко используемых в настоящее время четырехсимметричных блочных алгоритмов: *Data Encryption Standart* [1], Государственный стандарт 28147–89 [2], Международный алгоритм шифрования данных [3, 4, 5], *Ron Code 5* [6, 7]. В настоящее время в современных симметричных блочных алгоритмах используются по крайней мере четыре режима реализации криптографических процессов [8]: режим электронной шифровальной книги (*Electronic Code Book*), режим сцепления блоков шифра (*Cipher Chaning Book*), режим обратной связи по шифру (*Cipher-Feedback*) и режим обратной связи по выходу(*Output-Feedback*). Так как каждый из режимов имеет свои преимущества и недостатки, то решается задача исследования работы алгоритмов в разных режимах. Экспериментальные исследования выполнены на языке программирования *Java* с целью возможного использования результатов выполненных исследований в реальных приложениях.

Выполнен анализ гистограммы исходного (рис. 1) и шифрованного изображения (рис. 2). На рис. 3 приведены гистограммы исходного изображения и шифрованного изображения по алгоритмам DES, GOST,

IDEA и RC5. Выполнены расчеты дисперсии случайной величины оригинальных и шифрованных изображений для различных режимов и алгоритмов шифрования (рис. 4). Анализ позволяет сделать вывод, что гистограммы зашифрованного изображения довольно однородны и существенно отличаются от гистограмм исходного изображения, следовательно, не позволяют целенаправленно использовать любой ключ для атаки с целью раскрытия изображения.

Алгоритмы DES, GOST, IDEA и RC5 были протестированы для 20 размеров шрифтов изображений и для каждого из 10 различных изображений. На рис. 5 представлены сравнения среднего времени обработки графического изображения различными алгоритмами. Анализ таких зависимостей позволяет сделать вывод, что алгоритм DES работает медленнее, чем другие алгоритмы, и увеличение числа пикселов исходного изображения также увеличивает время обработки.

Рис. 1. Оригинальное изображение

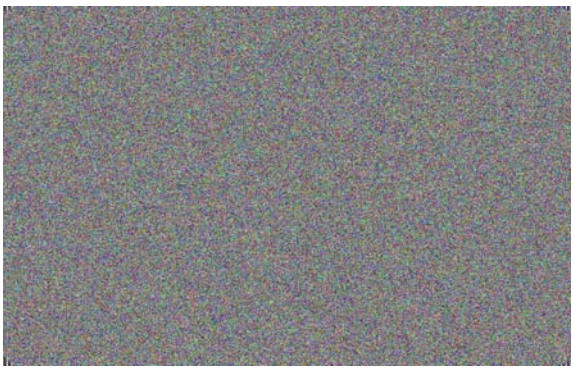


Рис. 2. Шифрованное изображение

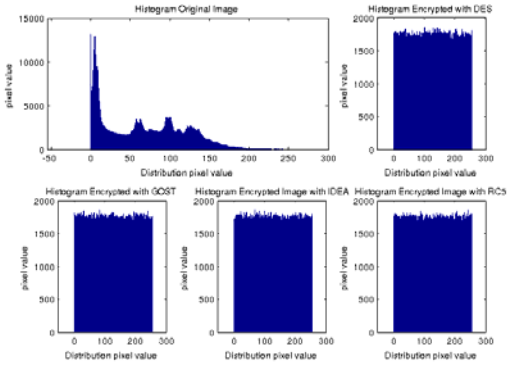


Рис. 3. Гистограммы оригинального и шифрованного изображений с DES, GOST, IDEA и RC5

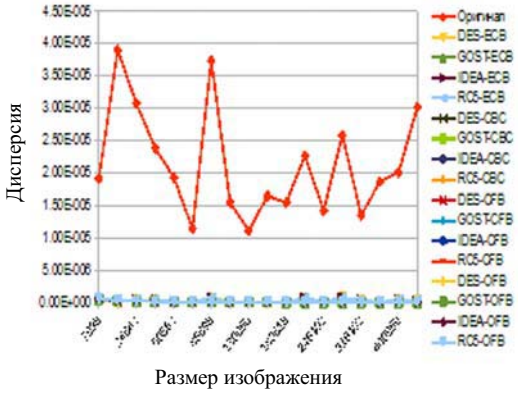


Рис. 4. Дисперсия случайной величины оригинальных и шифрованных изображений в любых режимах и алгоритмах

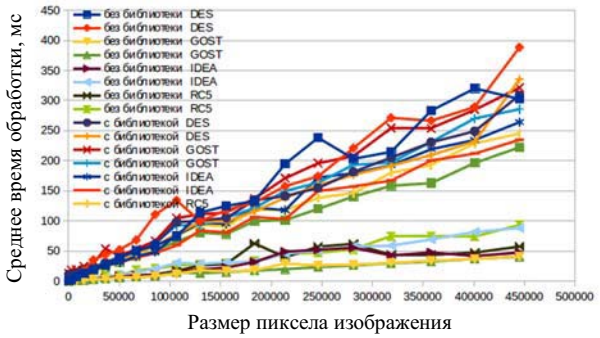


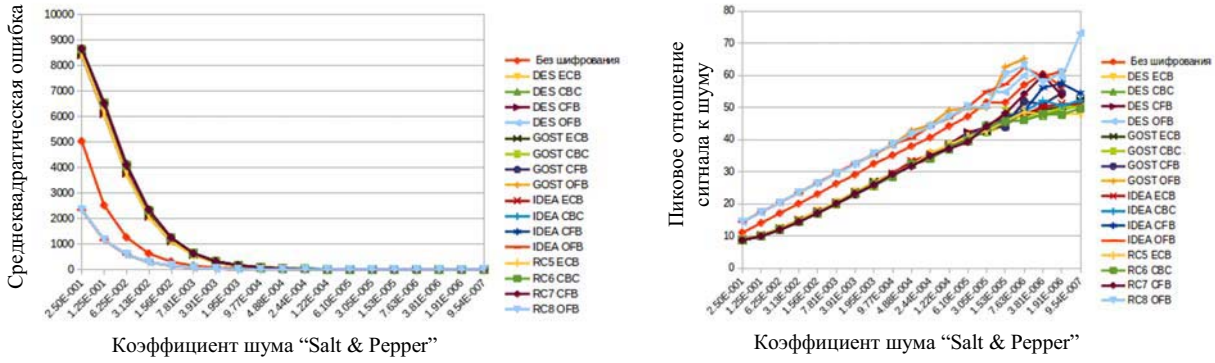
Рис. 5. Зависимость среднего времени обработки шифрования и дешифрования без библиотеки и с библиотекой

Выполнено сравнение среднего времени обработки с библиотекой и без библиотеки. Показано, что для алгоритма DES скорость обработки может быть снижена при использовании библиотеки (см. рис. 5).

Выполнено исследование зависимости ошибки дешифрования от шумов типа «соль», «перец» и гауссова шума. Выполненные расчеты показали (рис. 6), что OFB-режим имеет меньшую ошибку по сравнению с другими используемыми режимами. Показано, что режим OFB обепечивает меньшую ошибку, чем исходное изображение с «солью» в шуме, особенно в условиях низкой плотности шума. Такая ошибка определяет качество изображения в зависимости от пикового отношения сигнала к помехе (PSNR). Численные значения приведены на рис. 6, *а* и *б*.

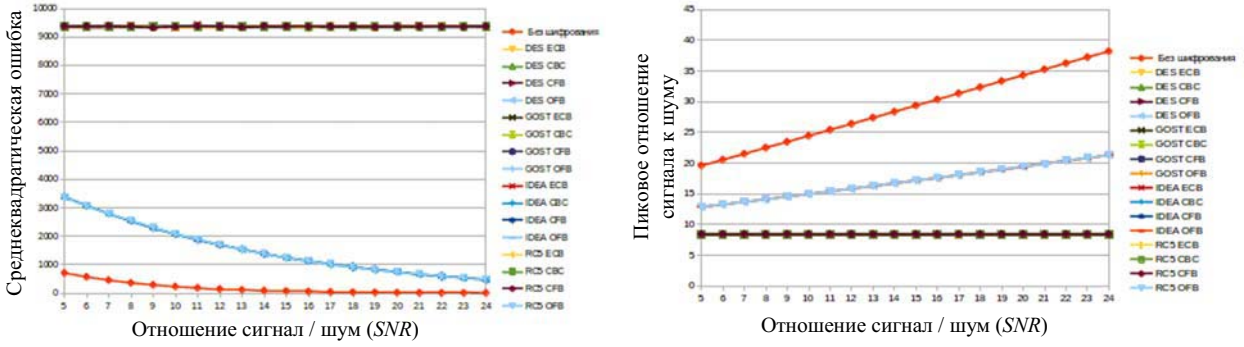
На рис. 7, *а* и *б* приведены результаты исследования зависимости среднеквадратических ошибок и пиковых отношений сигнала к шуму. В частности показано, что в режиме OFB изображения могут быть восстановлены, но их качество все равно далеко от исходного изображения с гауссовым шумом.

Выполнен анализ шифрования части изображения – практически закрытие части образа, который имеет меньшую площадь, чем исходное изображение. В этой части использованы паспорта с фотографией документа, когда необходимо зашифровать только часть фотографии (рис. 8, *а* и *б*).



а *б*

Рис. 6. Графические среднеквадратические ошибки (*а*); графические пиковые отношения сигнала к шуму «соль» и «перец» (*б*)



а *б*

Рис. 7. Графические среднеквадратические ошибки (*а*); графические пиковые отношения сигнала к гауссову шуму (*б*)

а *б*

Рис. 8. Оригинальное изображение (*а*); расшифрованное изображение (*б*)

Результаты вычисления дисперсии показаны на рис. 9. На рис. 9, *а* приведены такие результаты всего изображения, а на рис. 9, *б* – для части изображения. Показано, что шифрование части изображения дает бóльшую ошибку, чем для исходного изображения.

На рис. 10 приведены значения среднего времени обработки части изображения и полного изображения. Результаты позволяют сделать вывод, что шифрование части изображения сокращает время обработки. Полученное значение выигрыша представляет интерес для практической реализации метода.

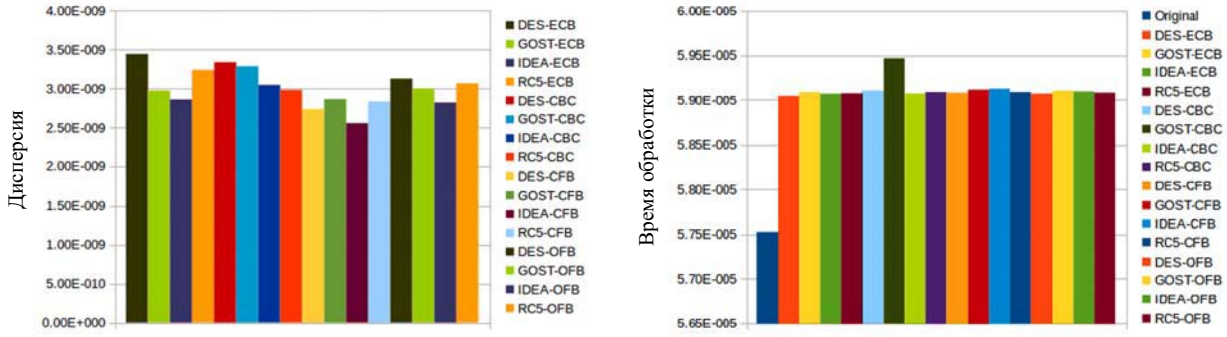
Выполнен анализ влияния аддитивного шума на операцию шифрования и дешифрования.

Анализ результатов рис. 11 показывает, что шифрование делает качество изображения ниже, если в зашифрованном изображения мы добавляем шум типа «соль» и «перец».

На рис. 12 приведены результаты вычислений MSE и PSNR. Показано, что качество изображения деградирует после расшифровки, и использование режима OFB дает лучшее качество обработки. Такой результат подтверждается анализом среднеквадратических ошибок (рис. 12, *а*).

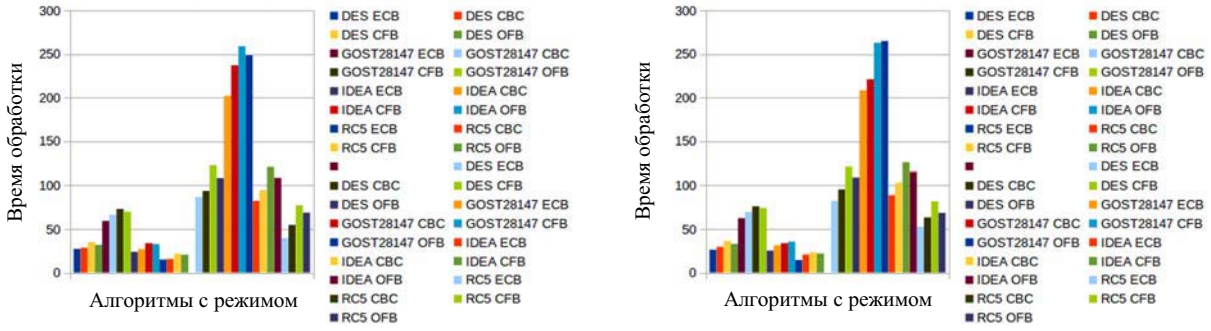
Основным результатом выполненных исследований является решение задачи повышения эффективности операции для шифрования изображения.

Алгоритм ГОСТ в 2.7^38 раз более, чем IDEA и RC5 для защиты от атаки грубой силы. Это объясняется тем, что алгоритм ГОСТ имеет самую большую длину ключа (256 бит) из рассмотренных стандартов шифрования. Так, в алгоритме DES (длина ключа 64 бит) возникает проблема с перебором. Однако задача может быть решена путем использования Triple DES (TDES), который в 5,7^25 раз более, чем TDES. При этом ключ можно увеличить в 2 раза (128 бит).



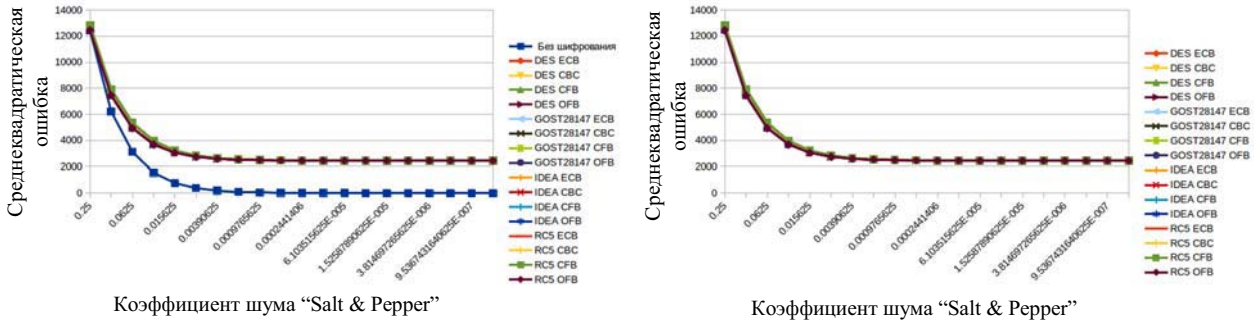
а *б*

Рис. 9. Дисперсия случайной величины части пикселов области (*а*) и всех пикселов области (*б*)



а *б*

Рис. 10. Среднее время обработки всей области и ее части: *а* – шифрование; *б* – дешифрование



а *б*

Рис. 11. Графические среднеквадратические ошибки (*а*); графические пиковые отношения сигнала к шуму (*б*)

Снижение дисперсии изображения от 4,4^5 до 5,99^5 после шифрования показало, что шифрованное изображение не имеет статистическую информацию (распределение частоты), как в обычных изображениях. Корреляция смежных пикселов также уменьшается после процесса шифрования, т. е. зашифрованное изображение имеет небольшую корреляцию в смежных пикселах не только в горизонтальном направлении, но и по вертикали и диагонали.

Время обработки алгоритмов имеет различные значения для каждого алгоритма. При использовании библиотеки время обработки примерно одинаково для каждого алгоритма. Но при шифровании без библиотеки или по собственному сценарию время можно существенно уменьшить, особенно для алго-

ритмов ГОСТ, IDEA и RC5, причем сокращение может достигать от 0,1 до 0,4 раза.

Доказано, что реализация режима OFB позволяет достигнуть лучших результатов для шифрования изображения, так как такой режим позволяет получить лучшее качество изображения при наличии шумов в шифрованном изображении. Получено достаточно высокое качество шифрования при наличии гауссова шума (PSNR = 11) и для шума типа «соль» и «перец» (PSNR = 18).

Все алгоритмы, режимы, а также тип формата (.png и .bmp) могут быть реализованы в шифрованной части изображения. Показано, что при шифровании изображения можно сократить время обработки до 50 % от шифрования всей площади без снижения безопасности. Пользователь может оперировать областью защиты. Однако дисперсия и корреляция не снижаются по сравнению с шифрованием всей области изображения.

Получено 25.07.2016

Библиографические ссылки

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

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

3. *Lai X.*, *Massey J.* A proposal for a new block encryption standard // Advances in Cryptology EUROCRYPT '90 Proceedings. – Springer-Verlag, 1991. – Pp. 389–404.

4. *Lai X.*, *Massey J.*, *Murphy S.* Markov ciphers and differential cryptanalysis // Advances in Cryptology EUROCRYPT '91 Proceedings. – Springer-Verlag, 1991. – Pp. 17–38.

5. *Lai X.* Detailed description and a software implementation of the IPES cipher // unpublished manuscript. – 1991.1995. – Vol. 20, No. 1. – Pp. 146–148.

6. *Rivest R. L.* The RC5 Encryption Algorithm // K. U. Leuven Workshop on Cryptographic Algorithms. – Springer-Verlag, 1995.

7. *Шнайер Б.* Прикладная криптография : Протоколы, алгоритмы, исходные тексты на языке Си. – С. 277–294.

8. *Hook D.* Beginning cryptography with Java (1st Ed.). – Birmingham : Wrox Press Ltd., 2005. – 484 p. – ISBN 978-0-7645-9633-9.