Университет ИТМО, факультет программной инженерии и компьютерной техники
Двухнедельная отчётная работа по «Информатике»: аннотация к статье

Дата прошедшей лекции	Номер прошедшей лекции	Название статьи/главы книги/видеолекции	Дата публикации (не старше 2021 года)	Размер статьи (от 400 слов)	Дата сдачи
11.09.2024	1	Number Systems for Deep Neural Network Architectures: A Survey	11.07.2023	~7000	25.09.2024
25.09.2024	2	Noise-Resistant Image Encryption Scheme for Medical Images in the Chaos and Wavelet Domain	07.03.2021	~8000	09.10.2024
	3				
	4				
	5				
	6				
	7				

Выполнил(а) Решетников С.Е, № группы P3108, оценка _____
Фамилия И.О. студента — не заполнять

Прямая полная ссылка на источник или сокращённая ссылка (bit.ly, tr.im и т. п.)
http://ray.yorksj.ac.uk/id/eprint/8168/1/Noise-Resistant_Image_Encryption_Scheme_for_Medical_Images_in_the_Chaos_and_Wavelet_Domain.pdf

Теги, ключевые слова или словосочетания (минимум три слова)
Medicine, Fast images encryption, Noise-resistant encryption

Перечень фактов, упомянутых в статье (минимум четыре пункта)
1. AES малоэффективен для шифрования изображений из-за большого количества раундов вычислений (также было упомянуто про DES, но он ведь небезопасен, разве нет?)
2. В шифровании активно используются хаотические системы т.к. они чувствительны к входным данным (подтверждение в статье на рисунке 4(b))
3. Система шифрования тем более надёжна, чем на более «низком»(«глубоком») уровне она шифрует данные
4. Любая криптосистема становится надёжнее, если содержит в себе confusion-diffusion механизм
5. Кубическо-логистическая карта (CLM) — последовательность задаваемая формулой $x_{n+1} = \phi x_n(1 - x_n)(2 + x_n)$, позволяет генерировать хаотичные значения из интервала (0;1), очень чувствительные к начальным параметрам.
6. Битовые плоскости содержат различное количество информации, при чём некоторые значительно больше остальных (в приведённом в статье примере 8-ая битовая плоскость (Most Significant Bit) содержала 50% информации об изображении, тогда как 1-ая (Least Significant Bit) — 0.3%)
7. Краткое описание алгоритма шифрования: извлекаем битовые плоскости → в битовых плоскостях с 5-ой по 8-ую перемешиваются писели, в остальных — нет (в угоду скорости) → применяется дискретное вейвлет-преобразование для каждой битовой плоскости → ко всем LL дианазонам применяется XOR с случайным 2-d сигналом, остальные диапазоны остаются неизменны т. к. в них мало данных (в угоду скорости) → обратное вейвлет-преобразование → формируем 3 группы по 3 изображения (ещё 2 мы генерируем случайным генератором) → раскладываем все изображения на битовые плоскости → как-то формируются 3 изображения-шифра (сущая магия)

Позитивные следствия и/или достоинства описанной в статье технологии (минимум три пункта)
1. Скорость работы алгоритма
2. Низкий коэффициент корреляции входных и выходных данных (стремится к 0), что говорит о надёжности шифрования
3. Шифрование на низком уровне (уровень битов), что обеспечивает его более высокую надёжность
4. Представленная технология устойчива к зашумлению данных
5. Без потерь

Негативные следствия и/или недостатки описанной в статье технологии (минимум три пункта)
1. Нет возможности автоматической коррекции ошибок, а при утрате какой-либо большой части зашифрованных данных изображение
2. Нужно передавать 3 изображения, что увеличивает вероятность повреждения данных
3. Описанный алгоритм действителен для монохромных изображений с глубиной 8 бит (возможно стоит шифровать каждую цветовую компоненту отдельно, но в статье об этом ни слова)