ЛР 6. Шифр с управляемыми подстановками

Реализовать шифр *с управляемыми подстановками*. Зашифровать и расшифровать сообщение. При этом надо определить то количество раундов шифрования (при выбранных параметрах алгоритма шифрования), которое превращает исходное изображение в шумоподобное (проверка с помощью тестов).

На основе всего проделанного надо проанализировать полученные результаты и основные свойства данного алгоритма шифрования.

Для выполнения данной ЛР надо:

1. ***индивидуально выбрать*** черно/белое изображение (*полутоновое*) - исходное открытое сообщение ***M***. Размер цифрового изображения взять *порядка* **512 × 512** пикселей (или более);
2. для последующего шифрованиясообщение ***M*** разбить на блоки **B**i, ***индивидуально выбрать*** битовый размер ***S***блоков **B**i (можно кратный одному байту, но необязательно), а также выбрать битовый размер ***r***подблоков ***в*** (на которые разбиваются блоки **B**i);
3. с учетом выбранного битового размера подблоков ***в***, выбрать количество таблиц прямой подстановки для шифрования. Создать таблицы прямой подстановки и соответствующие им таблицы обратной подстановки. Таблицы подстановки генерируются случайным образом и являются *секретным ключом* к шифру. При генерации таблиц подстановки обязательно проверить на замену числа «на себя самого», а также соблюсти критерий размножения битовых ошибок (заведомо устранить слабые ключи);
4. составить структуры алгоритмов *прямого и обратного преобразований* для шифра с управляемыми подстановками, удовлетворяющую индивидуальному заданию;
5. для исходного цифрового изображения выполнить тест на корреляцию, тест на «решетчатость», построить гистограмму распределения яркости пикселей. Привести все примененные расчетные соотношения и соответствующие графики. Проанализировать полученные результаты и сделать (написать в отчете) ***аргументированные*** выводы на этот счет;
6. выполнить один раунд шифрования. Построить результат шифрования-«картинку», по ней визуально оценить насколько хорошо/плохо просматриваются контуры изображения (контуры на зашифрованном цифровом изображении не должны просматриваться), визуально оценить «степень похожести» изображения на шум. Затем выполнить тест на корреляцию и тест на «решетчатость» (привести соответствующие графики), построить гистограмму распределения яркости пикселей полученного изображения. Сделать (написать) соответствующие ***аргументированные*** выводы на этот счет;
7. выполнить 2-й раунд шифрования. Построить результат шифрования-«картинку», по ней оценить визуально, насколько хорошо/плохо просматриваются контуры изображения и т.д. Выполнить для результата шифрования указанные выше тесты. Сделать (написать) соответствующие ***аргументированные*** выводы на этот счет. НАДО *выполнить столько раундов шифрования*, чтобы шифруемое черно/белое цифровое изображение превратилось в шумоподобное. Продемонстрировать это на соответствующей «картинке» и на графических тестах. Для каждого раунда шифрования - своя «картинка»-изображение и свои результаты тестирования;
8. выполнить и продемонстрировать правильность расшифрования цифрового изображения;
9. оценить влияние количества выбираемых таблиц подстановки при моделировании обработки на требуемое количество *раундов шифрования* (требуемое для получения шумоподобного цифрового изображения).

В отчете надо представить структуру алгоритмов шифрующего/дешифрующего преобразований (с описанием их работы).

Сделать (написать) соответствующие ***аргументированные*** общие выводы ***по всем выполненным пунктам*** работы.