для красных – 5,39. Визуальное восприятие также дает некоторую разницу, поэтому цветовой контраст по WCAG, применительно к контрастности с текстом, позволяет лучше показать насколько тона безопасной цветовой гаммы выдают неоднозначные параметры визуального различия цветов для их использования в веб-сервисах.

Таким образом, стандартная оценка цветового различия двух цветов между собой по показателю ΔE_{1976} в настоящее время не является однозначной. Безопасная гамма, несмотря на существенную разницу в уровнях квантования, не является гарантией однозначного воспроизведения цветов, и для некоторых тонов требуется более существенная корректировка с учетом визуального восприятия. Количественная оценка цветового контраста по WCAG в сравнении с цветностью текста позволяет лучше контролировать цвета между собой.

ЛИТЕРАТУРА

1. Джадд Д., Вышецки Г. Цвет в науке и технике. – М.: Мир, 1978. – 592 с.

2. Проверка цветового контраста [Электронный ресурс] / Сайт Aspose. – URL: https://products.aspose.app/html/ru/contrast-checker.

УДК 004.1

А.В. Кизино, маг.; О.А. Новосельская, доц.
(БГТУ, г. Минск, РБ)

АЛГОРИТМ РЕАЛИЗАЦИИ ИСКАЖЕНИЯ ШИФРОТЕКТСА

Подстановочные шифры (или шифры подстановки) – это криптографические методы, при которых каждое символ сообщения заменяется другим символом или знаком в соответствии с некоторыми правилами [1]. Самый распространенный метод расшифровки такого шифротекста – статистический анализ. Т.е. соотношение вероятностей появления символов в шифротексте с известной вероятностью символов в натуральном (естественном языке) [2]. Для шифров, использующих знаки для замены букв существует проблема сохранения порядка и ритма, т.е. визуально можно определить некоторые слова и расшифровать текст. Для затруднения расшифровки и анализа зашифрованного текста можно использовать алгоритм искажения входного текста.

Алгоритм искажения шифротекста подразумевает изменения входного текста, по средству внесения в него дополнительных символов, которые, предполагается, смогут изменить статистическое распределение символов в натуральном тексте и создать ложные вероятности, из-за чего при анализе текста будет сложнее вычленить определенные

символы, опираясь исключительно на статистическую вероятность их появления. Также полагается, что данный метод будет эффективным для использования в защитных изображениях, генерирующихся на основе помещенных в них данных, тем самым скрывая основное сообщение, изменяя его визуальный ритм.

Реализация данного метода проходит в несколько этапов. Для начала определяется количество мешающих (шумовых) символов исходя их языка, который используется в исходном сообщении. Рекомендуется использовать количество мешающих символов равное или меньше, чем символов в выбранном алфавите, тем самым вероятности появления символов будут приближены к натуральным показателям. Следующим этапом является определение процента зашумленности текста. Чем больше зашумляющих символов будет вмешано вы текст, тем сильнее видоизменится защитное изображение, однако это повлечет искусственное уменьшение вероятности появления основных символов, что так же моет стать подозрительным для криптоаналитика. Малое количество мешающих символов плохо будет изменять защитные изображения. Процент зашумления рекомендуется выбирать исходя из метода и вида шифрования, которым в последующем будет шифроваться текст. Так как подстановочные шифры зачастую базируются на таблицах соответствия или словарях, то при использовании данного метода, все мешающие символы должны восприниматься как полноценные символы и должны также находится в словарях и таблицах наравне с основным алфавитом. После начинается процесс добавленния символов в текст. Путем осаждения случайных символов в текст, который на данном этапе воспринимается как массив знаков, исходный тест видоизменяется, увеличиваясь в размерах. Этой особенностью можно воспользоваться, для увеличения начального текста до необходимого размера, если такие требования есть. Конечный текст подвергается стандартному шифрованию в соответствии с выбранным методом. Процесс дешифрования происходит следующим образом. Текст дешифруется в соответствии с правилами выбранного метода. На выходе, после дешифровки, пользователь получает сообщение с осажденными во время шифрования символами. Строка подвергается очистке, которая подразумевает удалении шумовых символов, которые заведомо известны. Таким образом после этих этапов пользователь получает исходное изображение.

Для тестирования данного метода были использованы два текста на русском и английском языке. Каждый текст содержал 3000 символов, тесты проходили на 50, 66 и 75 процентах зашумленности.

Для русского алфавита был сгенерирован мешающий алфавит размером в 33 символа, а для английского – 26 символов.

Первая серия тестов была на оценку изменения вероятности появления основных символов в тексте. В данных тестах оценивалась схожесть статистического распределения вероятностного появления символов натуральном тексте. На рис. 1 показан график распределения символов в тексте на русском языке в сравнении с эталонным распределением.

Рисунок 1 – График распределения символов в тексте на русском языке

Полученное распределение сравнивалось с эталонными показателями Тесты показали, что статистическое распределение в тексте после изменения сохраняют свои тенденции, что говорит о том, что нельзя утверждать, что метод изменяет статистическое появление основного алфавита. Данное суждение подтвердилось и при исследовании текста на английском языке.

Во время проведения тестов, был замечет факт, что при правильной настройке соотношения количества мешающих символов по отношению к основному тексту, то вероятность появления мешающих символов становится схожей с показателями натурального алфавита, тем самым в тексте появляется набор символов с одинаковыми или схожими вероятностями появления. Такие результаты были достигнуты при 50% зашумленности текста. На рис. 2 отображен график распределения вероятностей появления мешающих и основных символов, сгруппированных по вероятностям.

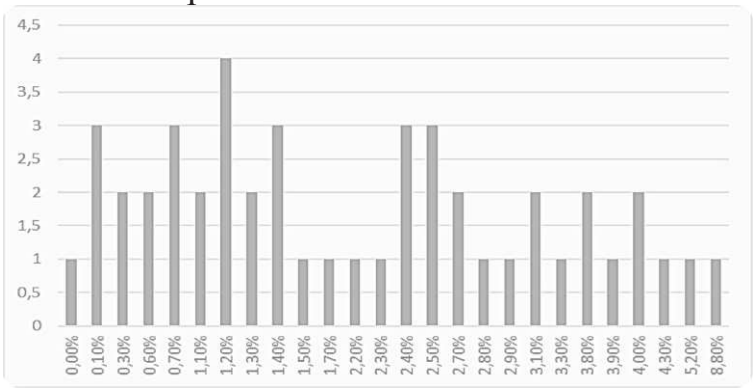
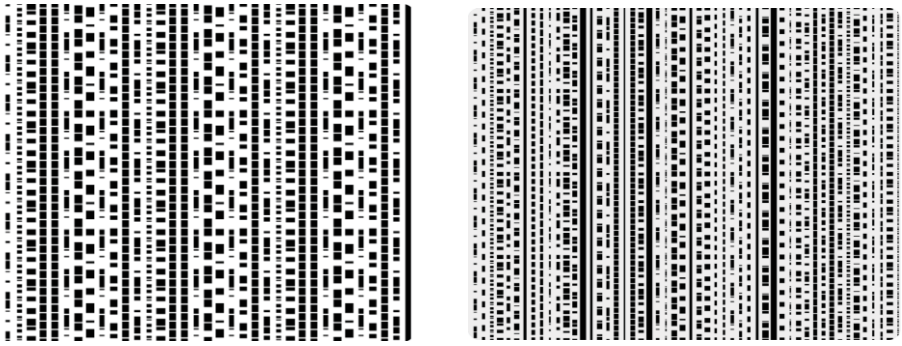


Рисунок 2 – График распределения вероятностей появления всех символов

Из графика видно, что в распределении есть как символы, вероятность появления которых встречается один раз, так и группы из двух и более символов с одинаковой вероятностью появления.

Таким образом можно говорить, что метод создает побочные вероятности, которые потенциально могут усложнить процесс анализа зашифрованного сообщения.

Следующая серия тестов была нацелена на анализ защитных изображений. Целью анализа был анализ ритма и характера рисунка до и после изменения сообщения, а также оценка возможности определения основной информации в рисунке при помощи визуального анализа. Для тестов были использованы сообщения, состоящие из 30 символов. До искажения текста в изображении были очевидно заметны повторяющиеся знаки, которые соответствовали повторяющимся символам в сообщении. После изменения исходного сообщения, рисунок стал более хаотичным, ритм исходного сообщения не прослеживается. На рис. 3*а*, 3*б* представлены изменения защитного изображения при шифровании строки «Hello world».



а *б*

Рисунрк 3 – Защитное изображение
а – до изменения исходного сообщения; б – после изменения

Исходя из результатов тестов, описанных выше, рассматриваемый метод применим для изменения шифротекста. Метод имеет практическую ценность при использовании его в защитных изображениях, так как позволяет существенно исказить конечный результат, при этом сохранив исходную информацию. Метод является достаточно легким в реализации и не требует больших вычислительных мощностей, что позволяет использовать его как дополнительную защиту данных в шифровании информации.

ЛИТЕРАТУРА

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: учебное пособие. – Гелиос АРВ, 2002. – 480 с.

2. Долгов В.А., Анисимов В.В. Криптографические методы защиты информации. – ДВГУПС, 2008. – 155 с.