УДК 621.391

МАСКИРОВАНИЕ ИЗОБРАЖЕНИЙ

Д.А.НАРЕЙКО, О.Г.ШЕВЧУК

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 02 апреля 2020

Аннотация.Рассмотрено матричное маскирование изображений с использованием уникальных квазиортогональных матриц Мерсенна (QES), а так же двумерное Стрип-преобразование изображения. Показано, что стрип-методимеет большее быстродействие по сравнению сметодом поблочного маскирования (QES).

Ключевые слова: маскирование, стрип-метод, метод поблочного маскирования, кватерион, матрицы Мерсенна.

Введение

Термин "маскирование" в настоящее время используется в различных областях человеческой деятельности, таких как биология, военное дело, химия, психология, технологии управления базами данных, цифровая обработка изображений. Сегодня данный термин также используется в области защиты изображений от несанкционированного доступа.

Маскирование – это процесс преобразования цифровой визуальной информации с малым сроком актуальности к шумоподобному виду с целью защиты от несанкционированного доступа [1]. Полученный после обработки изображения массив данных называется маскированной визуальной информацией или маскированным изображением.

Существующие методы маскирования изображений можно разделить на два основных вида [2]:

1. Криптографическое маскирование или маскирование с использованием криптографических примитивов, к данному виду относится метод поблочного маскирования [3].

2. Матричное маскирование, например Стрип метод [4].

Широкое распространение социальных сетей привело к необходимости использования различных методов маскирования фотоснимков для защиты данных в режиме реального времени.

Цель работы – анализ эффективных методов маскирования для оценки возможности их использования в режиме реального времени.

Метод поблочного маскирования изображений

Метод поблочного маскирования изображений (Quaternion Encryption Scheme, QES) основан на применении кватернионов – гиперкомплексных чисел четвертого ранга имеющих скалярную и векторную часть, которая является вектором в трехмерном пространстве [3].

Маскирование и демаскирования изображения методом QES описывается следующим образом:

$$\begin{aligned}&\mathbf{B}_{rot} = q\mathbf{B}q^{-1},\\&\mathbf{B} = q^{-1}\mathbf{B}_{rot}q;\end{aligned} \qquad (1)$$

где q – кватернион, $\mathbf{B}_{rot}$ – матрица поворота случайной матрицы $\mathbf{B}$.

Можно вычислить матрицу поворота, чтобы получить кватернионы высокого порядка, которые рассматриваются как последующие ключи шифрования и, следовательно, повышают безопасность данных. Количество вычисленных кватернионов-ключей высшего порядка равно $3n$, где $3n$ – порядок.

Схема работы метода поблочного маскирования полутонового изображения приведена на рис. 1, пример маскирования изображения методом QES– на рис. 2 [3].

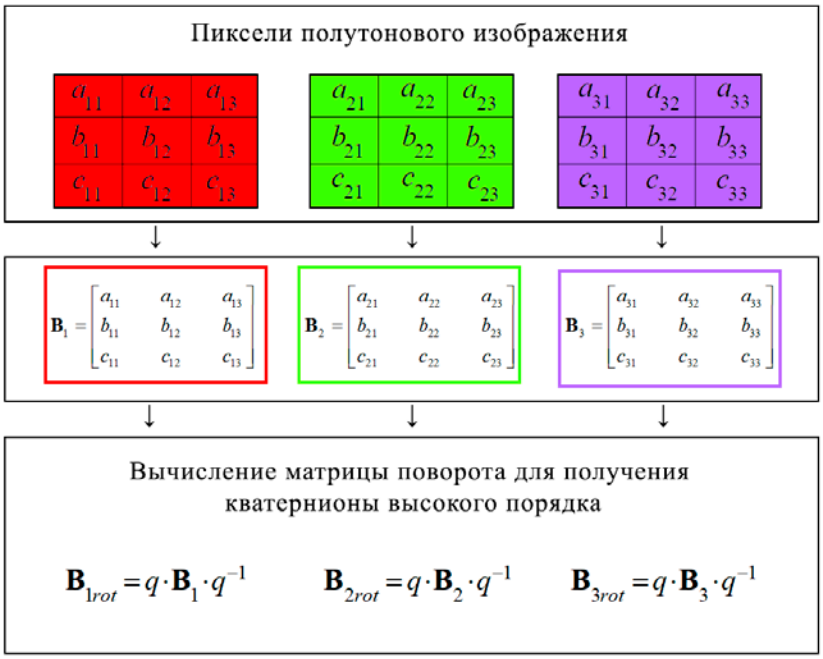
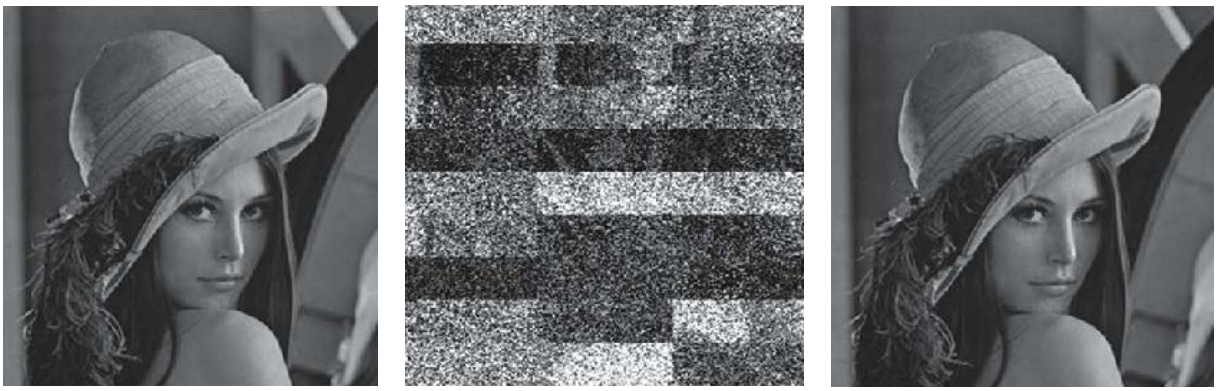


Рис. 1. Схема работы метода QES для полутонового изображения



а *б* *в*

Рис. 2. Пример маскирования методом QES: *а* – исходное изображение, *б* – маскированное изображение, *в* – восстановленное изображение)

Для получения более шумоподобного вида маскированного изображения процедуру QES необходимо выполнить итерационно несколько раз, что значительно увеличивает время преобразования.

Маскирование изображений на основе Стрип-метода

Стрип-метод изначально разрабатывался для помехоустойчивого кодирования [4]. Основу метода составляют матричные преобразования, обеспечивающие ослабление амплитуды импульсной помехи на передаваемом в канале изображении за счет равномерного ее распределения по всему изображению. Для максимального ослабления амплитуды помехи на выходе канала используются, как правило, ортогональные матрицы Адамара с двумя возможными значениями (уровнями) элементов {1, –1} такие, что:

$$\mathbf{H}^T\mathbf{H} = n\mathbf{I}, \tag{2}$$

где $\mathbf{H}$ – матрица Адамара, $\mathbf{I}$ – единичная матрица.

Из существующих двух модификаций стрип-метода для преобразования изображений – одностороннего и двухстороннего – основной интерес представляет вторая, обеспечивающая более полное "перемешивание" фрагментов изображения, результат которого может рассматриваться как его маскирование. Под двусторонним стип-преобразованием изображения в общем случае понимается преобразование вида

$$Z = \mathbf{A}_1\mathbf{P}\mathbf{A}_2, \tag{3}$$

где $\mathbf{A}_1$ и $\mathbf{A}_2$ – ортогональные матрицы размера $n \times n$; исходное изображение в виде матрицы $\mathbf{P}$ размера $n \times n$, Z – маскированное изображение размера $n \times n$, полученное в результате преобразования.

Под обратным двусторонним Стрип-преобразованием понимается преобразование вида

$$\mathbf{P} = \mathbf{A}_1^{-1}Z\mathbf{A}_2^{-1}, \tag{4}$$

На практике в двустороннем Стрип-преобразовании изображений используются матрицы $\mathbf{A}_1 = \mathbf{A}_2$ [9], поскольку это упрощает вычисления и экономит память. Таким образом, уравнение (3) имеет вид

$$Z=\mathbf{APA}, \tag{5}$$

где $\mathbf{A}$ – ортогональная матрица.

Поскольку матрица $\mathbf{A}$ является ортогональной, то $\mathbf{A}^{-1} = \mathbf{A}^T$. Следовательно, максимальные элементы у матриц $\mathbf{A}$ и $\mathbf{A}^{-1}$ одинаковы. Оптимальная матрица преобразования $\mathbf{A}$должна быть ортогональной с минимально возможным по модулю элементом. В отличие от представленного в работе [4] способа, результирующее изображение будет более шумоподобным при преобразованиях вида

$$Z=\mathbf{APA}^T,$$
$$\mathbf{P}=\mathbf{A}^T Z\mathbf{A}. \tag{6}$$

Пример работы двухстороннегоСтрип-преобразованияполутонового изображенияприведен на рис. 3 [4].

а *б*

Рис. 3. Двухстороннее стрип-преобразование: *а* – исходное изображение, *б* – преобразованное изображение

Оценка эффективности алгоритмов маскирования

Для оценки эффективности описанных методов маскирования использовались их реализации на языке C++. Эксперимент проведен на ЭВМ со следующими техническими характеристиками: процессор – Intel® Core™ i7-2630QM, ОЗУ – 8Гб, тип системы – 64-разрядная операционная система, процессор x64; операционная система – Windows 10.Для анализа использовалисьизображения размером 512×512 пикселей: "Lena" и"Flowers" (рис. 4).

а *б*

Рис. 4. Тестовые полутоновые изображения: *а*– "Lena", *б*– "Flowers"

Время маскирования и шифрования изображений в эксперименте включает процедуру сжатия без потерь и, следовательно, чем проще структура сжимаемого файла, тем быстрее производится сжатие и распаковка. Немаловажную роль играет вид представления пикселей: при шифровании на один пиксель отводится один байт, а при маскировании при представлении пикселей числами с фиксированной точкой на один пиксель приходится 8 байт. При представлении пикселей числами с плавающей точкой – 4 байта.

В таблицеприведенывремя маскированияи демаскирования изображений, соответственно, где столбец fix обозначает маскирование с представлением пикселей числами с фиксированной точкой, а float – представление пикселей маскируемого изображения числами с плавающей точкой.

Время обработки тестовых изображений методом QES и Стрип-методом

Исходное изображение	Метод QES		Маскирование Стрип-метод
	fix	float	
Время маскирования, мс			
"Lena"	133	71	41
"Flowers"	111	58	35
Время демаскирования, мс			
"Lena"	124	39	38
"Flowers"	70	39	37

Из табл. видно, что при маскировании Стрип-метод выигрывает в быстродействии в среднем в 1,7 раз по сравнению с методом QES, показывая примерно такое же время обработки изображений при демаскировании.

Заключение

Рассмотрено матричное маскирование изображения, с использованием уникальных квазиортогональных матриц Мерсенна, и двумерное стрип-преобразование изображений, а так же проведен их анализ. Показано, что Стрип-метод имеет большее быстродействие (в 1,7 раз) по сравнению с методом QES за счет деления изображения на фрагменты, что значительно сократило вычислительные затраты и необходимостью выполнения нескольких итераций маскирования в QES методе для достижения приемлемого результата. Следовательно, в режиме реального времени предпочтительнее использовать Стрип-метод.

MASKINGIMAGES

D.A. NAREIKO,A.G.SHAUCHUK

Abstract. Matrix masking of images using unique quasi-orthogonal Mersenne matrices (QES), as well as two-dimensional Strip image conversion are considered. It is shown that the Strip image conversion algorithm works much faster than the block masking method(QES).

Keywords: masking, strip method, block masking method, Mersenne matrix, quaterion.

Списоклитературы

1. Востриков А.А., Сергеев М.Б., Литвинов М.Ю. // Информационно-управляющие системы. 2015.№ 5 (78). С. 116–123.
2. Литвинов М.Ю. // Автореф. дис. канд. техн. Наук. ГУАП. СПб. 2009.23 с.
3. Czaplewski B., Dzwonkowski M., Rykaczewski R.// Journal of Telecommunications and Information Technology (JTIT) 2/2014. P. 3–11.
4. Мироновский Л.А.,Слаев В.А. Стрип-метод преобразования изображений и сигналов.// Монография. СПб: Политехника, 2006.