Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный индустриальный университет»

Посвящается 100-летию со дня рождения ректора СМИ, доктора технических наук, профессора Н.В.Толстогузова

НАУКА И МОЛОДЕЖЬ: ПРОБЛЕМЫ, ПОИСКИ, РЕШЕНИЯ

ГУМАНИТАРНЫЕ НАУКИ

ВЫПУСК 25

Труды Всероссийской научной конференции студентов, аспирантов и молодых ученых 12 – 14 мая 2021 г.

ЧАСТЬ III

Под общей редакцией профессора Н.А. Козырева

Новокузнецк
2021

ББК 74.48.278
Н 340

Н 340 Наука и молодежь: проблемы, поиски, решения: труды Всероссийской научной конференции студентов, аспирантов и молодых ученых, 12–14 мая 2021 г. Выпуск 25. Часть III. Гуманитарные науки / Министерство науки и высшего образования Российской Федерации, Сибирский государственный индустриальный университет ; под общ. ред. Н.А. Козырева – Новокузнецк; Издательский центр СибГИУ, 2021. – 452 с. : ил.

ISSN 2500-3364

Представлены труды Всероссийской научной конференции студентов, аспирантов и молодых ученых по результатам научно-исследовательских работ. Третья часть сборника посвящена актуальным вопросам иностранного языка, образования, культуры, социально-гуманитарных дисциплин, спорта, здоровья.

Материалы сборника представляют интерес для научных и научно-технических работников, преподавателей, аспирантов и студентов вузов.

ISSN 2500-3364

УДК 811.111 + 004.9

НОВЫЙ АЛГОРИТМ ШИФРОВАНИЯ ЦВЕТНОГО ИЗОБРАЖЕНИЯ С ПОМОЩЬЮ МОДИФИЦИРОВАННОЙ СХЕМЫ ЧУА

Четвертков Е.В.
Научный руководитель: канд. пед. наук, доцент Моисеенко Т. Г.

Сибирский государственный индустриальный университет,
г. Новокузнецк, email: *egorchetvertkov@list.ru*

Статья посвящена описанию нового алгоритма шифрования цветных изображений, использующий модифицированную схему Чуа для генерации случайных хаотических чисел. В алгоритме применяется функция побитового скремблирования. Представленный алгоритм при достаточно быстрой работе обеспечивает надежную защиту информации.

Ключевые слова: модифицированная схема Чуа, хаотические последовательности, шифрование и дешифрование изображений, битовое скремблирование, цветное изображение.

Безопасная передача изображений является одной из важных задач современной защиты информации и криптографии.

Традиционные криптографические методы являются более неэффективными, так как существует множество инструментов для декодирования файлов, защищенных общепринятыми методами, а методы, разработанные для защиты текста или черно-белых изображений, плохо работают с цветными изображениями.

Таким образом очень важной задачей является разработка все новых алгоритмов шифрования пригодных для кодирования цветных изображений.

В системах шифрования, использующих случайные числа, предпочтение отдается числам, полученным из какой-либо хаотической системы, поскольку выходные данные никогда не повторяются, и никто, кроме владельца, не может располагать информацией для расшифровки данных. В предложенном алгоритме шифрования в качестве хаотической системы используется модифицированная цепь Чуа.

Ключи криптосистемы генерируются с использованием открытого изображения и случайных шумов. Прежде всего получается 48-битное представление открытого изображения для ввода в функцию SHA-256.

Случайный шум генерируется в начале каждого процесса шифрования. Затем 256-битное значение хэша открытого изображения генерируется путем выполнения SHA-256 с входным сигналом в виде 48-битного представления открытого изображения и шума. Результатом этой операции является секретный ключ, уникальный для каждого процесса шифрования.

Крошечная разница в открытом изображении приведет к генерации совершенно другого секретного ключа.

Для работы алгоритма цветное изображение переводится в черно-белое следующим образом: компоненты RGB каждого пикселя исходного изображения размещаются друг под другом. Общее количество пикселей черно-белого изображения таким образом равно три умножить на количество пикселей исходного изображения.

Выделяют восемь шагов для шифрования цветного изображения. Схема алгоритма шифрования представлена на рисунке 1.

Шаг 1. С помощью известного алгоритма SHA-256 строится хэш данного изображения.

Шаг 2. На основе полученного хэша генерируются начальные значения модифицированной схемы Чуа.

Шаг 3. Используя эти начальные значения, генерируется последовательность хаотических чисел.

Шаг 4. Из полученных хаотических значений получается оптимальная матрица ключей. Для этого берется модуль произведения разности каждого хаотического числа и самого числа, округленного до ближайшего шестизначного, и десяти в шестой. Из полученной последовательности сначала исключаются повторяющиеся элементы, затем данная последовательность усекается до количества пикселей в черно-белом изображении и наконец сортируется в порядке возрастания.

Шаг 5. На основе матрицы пикселей черно-белого изображения строится специальная матрица. Для этого матрица пикселей приводится к матрице-столбцу. После каждый пиксель переводится в двоичный формат, тем самым получается матрица из восьми столбцов и прежним количеством строк. Затем полученную матрицу разделяют на две, первая содержит первые четыре столбца, а вторая - последние четыре.

Шаг 6. Вторая из полученных матриц переводится в матрицу-столбец, затем каждый элемент матрицы-столбца заменяется на элемент с индексом равным значению матрицы ключей с текущим индексом. После матрицу-столбец приводят к форме с четырьмя столбцами.

Шаг 7. К первой матрице, полученной на шаге 5 полученной на шаге 6, применяется диффузионный метод с использованием матрицы ключей.

Шаг 8. Обе матрицы, полученные на шаге 7 приводятся к двоичной форме и сливаются в одну. Элементы полученной матрицы приводятся к десятичному виду. В конце полученную десятичную матрицу приводят к форме изображения т.е. количество столбцов матрицы совпадает с количеством пикселей по ширине исходного цветного изображения, а количество строк - с количеством пикселей по высоте.

Для получения исходного цветного изображения необходимо зашифрованное изображение и хэш данного изображения. Для расшифровки выполняются пять шагов. Схема дешифрования изображения приведена на рисунке 2.

Шаг 1. Для получения матрицы ключей производятся шаги 2-4 алгоритма шифрования.

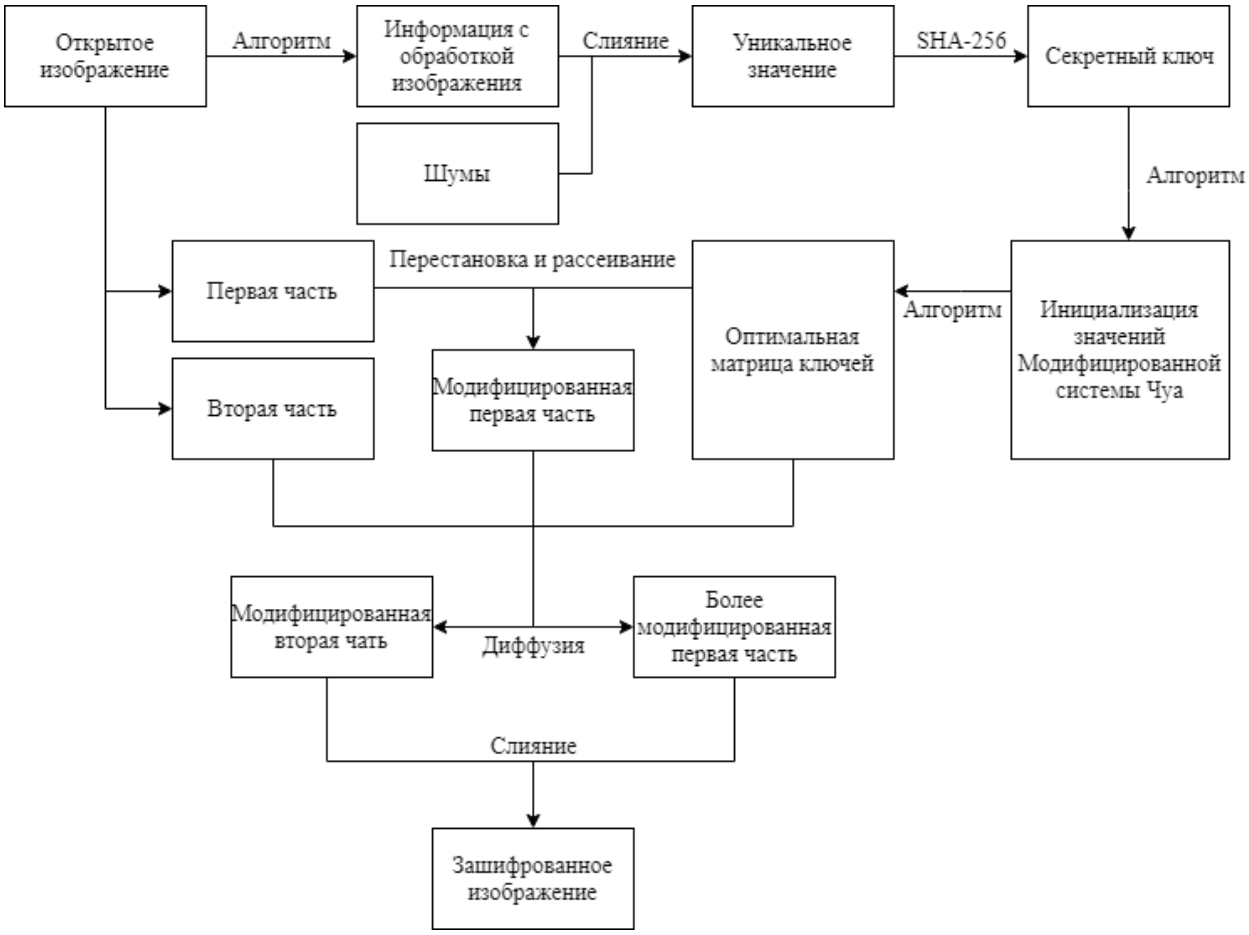

Рисунок 1 - Схема шифрования цветного изображения

Шаг 2. Подобно шагу 5 алгоритма шифрования получаются две двоичные матрицы.

Шаг 3. Для полученных на предыдущем шаге матриц применяется диффузионный метод, аналогичный тому, что использовался на шаге 7 алгоритма шифрования.

Шаг 4. Ко второй матрице, полученной на шаге 2, применяется метод обратного скремблирования.

Шаг 5. Находится декодированная матрица, аналогично шагу 8 в алгоритме шифрования.

Представленный алгоритм является надежным, что подтверждается тестами на ключевое пространство, чувствительность ключа к открытому изображению и т.д., кроме того, предложенное решение показывает неплохую скорость шифрования.

Пример работы алгоритма приведен на рисунке 3.

Пространство ключей, сгенерированных данным алгоритмом, на много превышает два в сотой степени, что серьезно затрудняет атаку грубой силой.

Поскольку при небольшая модификация начальных значениях любая хаотическая система дает совершенно разные результаты, ключ, сгенерированный модифицированной схемой Чуа, является одноразовым. Помимо это-

го, на ключ также влияют хэш-значении, генерируемом с использованием открытого изображения и шума.

Рисунок 2 - Схема дешифрования цветного изображения

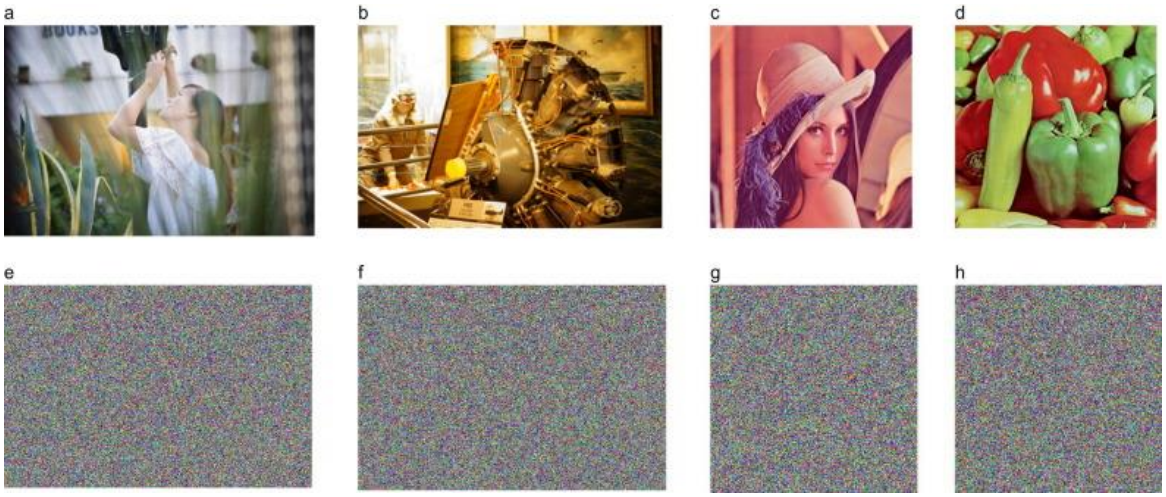

Рисунок 3 - Открытое изображение и соответствующее ему зашифрованное изображение

Таким образом, если условия запуска системы немного изменить, будет получен отличный от изначального зашифрованный образ.

Основными характеристиками, дающими количественную оценку чувствительности алгоритма шифрования к открытому тексту, являются процент пикселей, изменивших значение (NPCR) и среднее изменение интен-

сивности (UACI). Результаты проверки критерия NPCR приведены в таблице 1. Результаты проверки критерия UACI приведены в таблице 2.

Еще одним показателем надежности криптографической системы является энтропия информации. Чем выше энтропия информации в зашифрованном изображении, тем сложнее раскрыть закодированную информацию. Значения энтропии информации зашифрованных изображений приведены в таблице 3.

Представленный алгоритм справляется со своей работой в среднем за шестьдесят две сотых секунды. Очевидно, что данный алгоритм достаточно быстр для выполнения задач.

Таблица 1 - Средние значения NPCR (%) полученные с использованием предложенного алгоритма для каждого компонента RGB.

Изображение	R	G	B	Идеальное значение
B	99,6012	99,6002	99,6174	99,6094
C	99,6492	99,6145	99,6393	
D	99,6258	99,6146	99,6149	

Таблица 2 - Средние значения UACI (%) полученные с использованием предложенного алгоритма для каждого компонента RGB.

Изображение	R	G	B	Идеальное значение
B	33,4459	33,4129	33,4681	33,4635
C	33,3937	33,4921	33,4456	
D	33,4529	33,5141	33,3476	

Таблица 3 - Энтропия информации по компонентам RGB зашифрованных изображений.

Изображение	R	G	B	Идеальное значение
B	7,9905	7,9901	7,9899	8,0000
C	7,9949	7,9945	7,9941	
D	7,9888	7,9878	7,9978	

Алгоритм показывает хорошие результаты, обеспечивает эффективную технику шифрования и дешифрования цветных изображений, кроме того, алгоритм работает достаточно быстро.

Библиографический список

1. A new algorithm for the colored image encryption via the modified Chua’s circuit // ScienceDirect URL: https://doi.org/10.1016/j.jestch.2019.09.001 (дата обращения: 20.10.2019).