(19) Евразийское патентное ведомство

(21) 201900228 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2020.09.30

(22) Дата подачи заявки
2019.03.20

(51) Int. Cl. ***H04N 19/00*** (2006.01)
H04N 19/126 (2006.01)

(54) СПОСОБ ШИФРОВАНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ДИСКРЕТНЫХ ОТОБРАЖЕНИЙ И КЛЕТОЧНЫХ АВТОМАТОВ

(96) **2019/EA/0030 (BY) 2019.03.20**

(71) Заявитель:
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (БГУ) (BY)

(72) Изобретатель:
Сидоренко Алевтина Васильевна, Шишко Максим Сергеевич (BY)

(57) Изобретение относится к криптографической технике - зашифрованию и расшифрованию данных и используется для защиты информации, представленной в электронном виде, при ее хранении или передаче в системах связи и сетях передачи информации. Задачей изобретения является создание способа, позволяющего улучшить эффективность шифрования: увеличить скорость шифрования; уменьшить объем памяти, требуемый для хранения и передачи одного изображения; увеличить стойкость к различным видам криптографических атак. Сущность изобретения заключается в том, что посредством электронно-вычислительного программируемого устройства обрабатываемые данные считывают в оперативную память в виде матрицы целочисленных значений пикселей, к матрице пикселей изображения последовательно многократно применяют операцию базового преобразования, причем в качестве операции базового преобразования используют вейвлет-преобразование; затем матрицу вейвлет-коэффициентов делят на низкочастотную и высокочастотные компоненты; низкочастотную компоненту шифруют с помощью хаотического перестановочно-рассеивающего алгоритма с использованием отображения тент, начальное условие хаотического отображения модифицируют хеш-функцией; высокочастотные компоненты кодируют вложенным кодом и шифруют методом, основанным на обратимых клеточных автоматах второго порядка, в котором раундовый ключ модифицируют кусочно-линейным хаотическим отображением.

201900228 A1

201900228 A1

МПК ***H04L 9/28***

Способ шифрования изображений на основе дискретных отображений и клеточных автоматов

Изобретение относится к криптографической технике – зашифрованию и расшифрованию данных, и используется для защиты информации, представленной в электронном виде, при ее хранении или передаче в системах связи и сетях передачи информации.

Известен способ зашифрования и расшифрования изображений при использовании хаотического отображения [1], основанный на обработке значения пикселей изображения методом диффузии и рассеяния с использованием расширенного параметрического семейства обобщенного трехмерного хаотического отображения кота Арнольда.

Однако, данный алгоритм применяется к растровым изображениям. Растровые изображения занимают больший объем памяти, чем аналогичные по разрешению изображения, сжатые каким-либо алгоритмом сжатия. Это приводит к тому, что алгоритму необходимо обработать гораздо больший объем данных для зашифрования изображения, что проявляется в недостаточной производительности метода для шифрования изображений больших разрешений в реальном времени. Также для обеспечения стойкости шифрования алгоритм разработан так, что зашифрованное изображение обладает намного большей информационной энтропией, что приводит к неэффективности и нецелесообразности сжатия зашифрованного изображения, вследствие чего зашифрованные изображения требуют больший объем памяти при их хранении и передаче.

Известен способ зашифрования и расшифрования информации с 32N+D битным ключом при использовании хаоса [2], в основу которого положено добавление к входному блоку данных случайной последовательности, сгенерированной специфическим хаотическим уравнением, и последующее комбинирование входных блоков.

Однако, по причине использования операции округления при работе с действительными числами этот способ обладает существенным недостатком, который связан с наличием погрешностей в моделировании динамики хаотических систем, что приводит к потере хаотических свойств и слабой криптостойкости способа.

Задачей изобретения является создание способа шифрования изображений на основе дискретных отображений и клеточных автоматов, позволяющего улучшить эффективность шифрования, заключающуюся в увеличении скорости шифрования, а также уменьшении объема памяти, требуемого для хранения и передачи одного изображения; увеличить стойкость способа к различным видам криптографических атак.

Поставленная задача достигается тем, что в способе шифрования изображений на основе дискретных хаотических отображений и клеточных автоматов посредством электронно-вычислительного программируемого устройства обрабатываемые данные считывают в оперативную память в виде матрицы целочисленных значений пикселей, с помощью заданной последовательности действий, приводящей к созданию электрических сигналов в электронно-вычислительном программируемом устройстве, к матрице пикселей изображения последовательно многократно в течение r раундов применяют операцию базового преобразования, причем в качестве операции базового преобразования используют вейвлет-преобразование; полученную в результате вейвлет-преобразования матрицу вейвлет-коэффициентов делят на низкочастотную LL-компоненту и высокочастотные LH, HL, HH компоненты; LL-компоненту матрицы вейвлет-коэффициентов шифруют с помощью хаотического перестановочно-рассеивающего алгоритма, где в качестве хаотической функции используют хаотическое отображение-тент, а начальное условие для хаотического отображения модифицируют с помощью хеш-функции; высокочастотные LH, HL и HH компоненты кодируют вложенным кодом HBCT (Hardware Block Cluster Tree), а затем шифруют с помощью метода, основанного на обратимых клеточных автоматах второго порядка, в котором раундовый ключ модифицируют с помощью кусочно-линейного хаотического отображения.

Изложенная сущность поясняется фиг. 1-16, где на фиг. 1 – изображена общая блок-схема алгоритма шифрования заявленного способа: 1 – начало алгоритма, 2 – ввод входных параметров алгоритма шифрования, таких как шифруемое изображение, ключ шифрования и начальные условия хаотических отображений, 3 – вейвлет-преобразование изображения, 4 – отделение коэффициентов LL-поддиапазона, 5 – шифрование коэффициентов LL-поддиапазона, 6 – кодирование уточняющих вейвлет-коэффициентов, 7 – шифрование уточняющих вейвлет-коэффициентов, 8 – запись зашифрованных данных в ПЗУ; на фиг. 2 – приведена схема матрицы вейвлет-коэффициентов при трехуровневой вейвлет-декомпозиции; на фиг. 3 – показана схема метода шифрования коэффициентов LL-поддиапазона; на фиг. 4 – представлена блок-схема метода шифрования уточняющих вейвлет-коэффициентов: 1 – шифруемый блок данных длиной 256 бит, 2 – младшие 128 бит шифруемого блока (BL_i), 3 – старшие 128 бит шифруемого блока (BH_i), 4 – 128-битный ключ шифрования (K), 5 – 32-битный элемент хаотической последовательности (n_i^j), 6 – начальное условие хаотического отображения (x_i^0), 7 – 128-битный раундовый ключ (Sk_i), 8 – состояние клеточного автомата предшествующее начальному (C^{-1}), 9 – начальное состояние клеточного автомата (C^0), 10 – 15 раундов эволюции клеточного автомата функцией F_1,

11 – состояние клеточного автомата, предшествующее конечному (C^{15}), 12 – конечное состояние клеточного автомата (C^{16}), 13 – 16 раундов эволюции клеточного автомата функцией F_2, 14 – 16 раундов эволюции клеточного автомата функцией F_5, 16 – зашифрованный блок данных длиной 256 бит; на фиг. 5-10 – приведены гистограммы исходного (фиг. 5, 7, 9) и зашифрованного (фиг. 6, 8, 10) изображения, красной (фиг. 5, 6), зеленой (фиг. 7, 8) и синей (фиг. 9, 10) цветовых компонент; на фиг. 11-16 – изображены гистограммы рассеяния, показывающие корреляцию между соседними пикселями в горизонтальном направлении для исходного (фиг. 5, 7, 9) и зашифрованного (фиг. 6, 8, 10) изображения, красной (фиг. 5, 6), зеленой (фиг. 7, 8) и синей (фиг. 9, 10) цветовых компонент.

Входными данными способа шифрования изображений на основе дискретных отображений и клеточных автоматов являются шифруемое растровое изображение, полученное с помощью цифровой фото-видео камеры либо сохраненное в ОЗУ/ПЗУ, ключ шифрования и начальные условия хаотических отображений. В начале алгоритма все входные параметры считываются в ОЗУ на этапе 2 (фиг. 1).

Затем шифруемое изображение обрабатывается путем применения нескольких уровней дискретного вейвлет-преобразования (фиг. 1, п. 3) описываемого следующей формулой:

$$y_{2n+1} = x_{2n+1}^{ext} - \left\lfloor \frac{x_{2n}^{ext} + x_{2n+2}^{ext}}{2} \right\rfloor$$

$$y_{2n} = x_{2n}^{ext} - \left\lfloor \frac{x_{2n-1}^{ext} + x_{2n+1}^{ext} + 2}{4} \right\rfloor,$$

где x_i^{ext} – отсчеты симметрично расширенного сигнала;
$\lfloor a \rfloor$ – наибольшее целое, не превышающее a.

Вышеописанные вейвлет-преобразования применяются поочередно сначала ко всем строкам, а после ко всем столбцам растрового изображения. При этом изображение разбивается на четыре поддиапазона: LL, HL, LH, HH. LL-поддиапазон содержит уменьшенную копию исходного изображения; LH, HL и HH поддиапазоны содержат уточняющие коэффициенты, позволяющие восстановить изображение. Для LL-поддиапазона вейвлет преобразование может применяться снова при этом получится следующий уровень декомпозиции и т.д. На фиг. 2 показана схема трехуровневой декомпозиции изображения.

Так как LL-поддиапазон является уменьшенной копией исходного изображения и содержит наибольшее количество информации о исходном изображении, он шифруется отдельно с помощью перестановочно-рассеивающего алгоритма (фиг. 3). В этом типе криптографических систем есть два взаимно независимых этапа: перестановка и рассеяние. На этапе

перестановки все пиксели изображения меняются местами согласно некоторым преобразованиям, не меняя своих значений. Чтобы декоррелировать смежные пиксели, перестановка выполняется n раз, где $n \geq 1$. После этого этапа каждый пиксель становится замененным другим пикселем из этого же изображения. На этапе рассеяния значения пикселей меняются таким образом, чтобы гистограмма зашифрованного изображения отличалась от гистограммы шифруемого и походила на гистограмму равномерного шума. Цикл перестановки-рассеяния повторяется несколько раз для достижения удовлетворительного уровня беспорядка. Эти преобразования позволяют увеличить стойкость алгоритма к статистическому и дифференциальному криптоанализу.

Для сжатия изображения производится вложенное кодирование уточняющих вейвлет-коэффициентов с помощью алгоритма HBCT (Hardware Block Cluster Tree). Данный метод использует построение кластерных деревьев в пределах квадратных блоков битовых плоскостей матрицы вейвлет-коэффициентов и прогрессивное вложенное кодирование. Это позволяет убрать избыточность в матрице вейвлет-коэффициентов и уменьшить объем требуемой для ее хранения памяти, а также уменьшить время, необходимое на их шифрование по сравнению с аналогами.

После сжатия уточняющие коэффициенты разделяются на блоки размером 256 бит и шифруются блочным алгоритмом шифрования на основе обратимых клеточных автоматов (фиг. 4), базовое преобразование которого представляет собой 80 раундов обратимого клеточного автомата второго порядка, применяемого последовательно ко всем блокам данных с различными ключами, генерируемыми хаотической последовательностью.

В итоге все зашифрованные данные сохраняются в ПЗУ для последующей передачи по незащищенным каналам связи.

Для промежуточного анализа выходных зашифрованных последовательностей предлагается использование специализированных методов: вычисление корреляции, информационной энтропии, построение гистограммы распределения пикселей по яркости и диаграммы рассеяния, проведение статистических тестов по стандарту SP 800-22. Эти параметры позволяют оценить надежность шифрования при использовании заданных характеристик метода.

Поскольку в алгоритме для шифрования LL-поддиапазона и остальных коэффициентов применяются принципиально разные методы, было принято решение протестировать их на стойкость отдельно, а также провести тестирование производительности алгоритма целиком. Алгоритм шифрования LL-поддиапазона, так как он является классическим алгоритмом шифрования изображений типа перестановки-рассеяния, был протестирован на

устойчивость к статистическому и дифференциальному криптоанализу. Блочный алгоритм шифрования вейвлет-коэффициентов был протестирован с помощью набора тестов SP 800-22.

Оценка стойкости к статистическому криптоанализу осуществлялась с помощью построения гистограмм яркости пикселей, вычисление корреляций (в вертикальном, горизонтальном и диагональном направлениях) двух соседних пикселей в зашифрованном изображении, анализ информационной энтропии.

На фиг. 5-10 изображены гистограммы незашифрованных и зашифрованных с помощью предлагаемого алгоритма изображения «Лена». Как видно из гистограмм, исходное изображение имеет хорошо различимые пики для определенной яркости цвета, причем для каждой компоненты цвета пики находятся на разных интенсивностях.

Для зашифрованных же изображений характерно равномерное распределение яркости цвета, поэтому нельзя точно сказать, какой цвет является преобладающим в зашифрованном изображении, а следовательно, анализ гистограммы не может дать злоумышленникам информации об исходном распределении пикселей по цветам.

Корреляция является мерой, которая показывает зависимость между двумя соседними пикселями в изображении. Различают коэффициент корреляции по горизонтали, вертикали и диагонали. Коэффициенты корреляции для незашифрованного изображения, как правило, имеют значение, стремящееся к единице. Это означает, что значения соседних пикселей связаны между собой некоторой зависимостью. Для зашифрованного же изображения коэффициент корреляции должен стремиться к нулю. Чем ближе коэффициент к нулю, тем меньше связаны соседние пиксели и тем выше стойкость алгоритма к статистическому криптоанализу.

Для графического представления корреляции строятся диаграммы рассеяния для соседних пикселей. Диаграмма рассеяния строится как зависимость Y(X), где X – яркость компоненты цвета исходного пикселя; Y - яркость компоненты цвета пикселя, соседнего с исходным. В зависимости от типа корреляции соседний пиксель берется по горизонтали, вертикали или диагонали. На фиг. 11-16 изображены диаграммы рассеяния для незашифрованного и зашифрованного изображения «Лена».

Как следует из диаграмм, у незашифрованного изображения прослеживается четкая корреляция между значениями соседних пикселей во всех направлениях. Однако, на диаграммах зашифрованного изображения точки распределены равномерно по всей площади диаграммы, что позволяет говорить об отсутствии корреляции между пикселями в зашифрованном

изображении. Это подтверждают и рассчитанные коэффициенты корреляции, приведенные в таблице 1. Как видно из таблицы, коэффициент корреляции для незашифрованного изображения близок к единице, это означает, что значения соседних пикселей в незашифрованном изображении коррелируют. Для зашифрованного изображения коэффициент корреляции близок к нулю, это означает, что корреляция между соседними пикселями практически отсутствует. Этот факт затрудняет злоумышленникам статистический криптоанализ зашифрованного текста.

Таблица 1 – Коэффициенты корреляции

Изображение	Незашифрованное			Зашифрованное		
	Гориз.	Верт.	Диаг.	Гориз.	Верт.	Диаг.
Мандрил	0.9223	0.8742	0.8656	-0.0176	-0.0086	-0.0729
Лена	0.9813	0.9887	0.9699	0.0180	0.0019	-0.0090
Перцы	0.9673	0.9658	0.9670	0.0006	-0.0132	-0.0377

По Шеннону энтропия или информационная энтропия является мерой неопределенности, связанной со случайной величиной. Она дает количественную оценку информации, содержащейся в данных, как правило, в битах или битах на символ. Растровые изображения представляют собой набор пикселей, меняющих значение от 0 до 255. Если значение пикселя является случайной величиной, то энтропия данной случайной величины должна быть равна 8. Чтобы осложнить статистический криптоанализ алгоритма шифрования изображений, необходимо чтобы зашифрованное изображение походило на случайный набор пикселей, следовательно, энтропия шифра должна быть близка к максимальному значению, то есть к 8.

Таблица 2 – Информационная энтропия

Изображение	Незашифрованное, бит			Зашифрованное, бит		
	R	G	B	R	G	B
Мандрил	7.76	7.61	7.72	7.97	7.96	7.96
Лена	7.75	7.21	7.41	7.96	7.97	7.97
Перцы	7.49	7.50	7.38	7.95	7.95	7.97
Мармелад	6.58	6.36	6.21	7.97	7.96	7.97

В таблице 2 представлена энтропия различных цветовых компонент (красной (R), зеленой (G) и синей (B)) для незашифрованных и зашифрованных изображений. Как видно из таблицы, энтропия зашифрованных изображений больше, чем энтропия незашифрованных и близка к 8. Даже для изображения с наименьшей энтропией «Мармелад» энтропия зашифрованного изображения остается на уровне остальных и близка к своему максимальному значению. Это означает, что алгоритм шифрования вносит достаточную долю неопределенности в зашифрованное изображение и делает его похожим на случайный набор пикселей. Это, вкупе

с низко корреляцией, позволяет говорить о высокой стойкости алгоритма к статистическому криптоанализу.

Для оценки стойкости метода к дифференциальному криптоанализу были вычислены коэффициенты NPCR (Number of Pixel Changing Rate – процент измененных пикселей) и UACI (Unified Averaged Changed Intensity – среднее изменение интенсивности). NPCR и UACI показывают число изменяющихся пикселей и усредненное изменение интенсивности изображения при небольшом изменении в изображении открытого текста (обычно изменение в одном пикселе). В ходе проведения данной работы были вычислены коэффициенты UACI и NPCR данного алгоритма для разных цветовых компонент: красной (R), зеленой (G) и синей (B). Результаты тестов приведены в таблице 3. По результатам теста видно, что NPCR близок к 100%, а UACI к 33,(3)% что означает хорошую стойкость алгоритма к дифференциальному криптоанализу.

Таблица 3 – Элементы дифференциального анализа

Изображение	NPCR, %			UACI, %		
	R	G	B	R	G	B
Мандрил	99.62	99.61	99.58	33.44	33.28	33.42
Лена	99.55	99.51	99.57	33.41	33.39	33.45
Перцы	99.60	99.59	99.53	33.37	33.29	33.47
Мармелад	99.60	99.61	99.66	33.46	33.42	33.37

Вторая составляющая алгоритма шифрования, отвечающая за шифрование уточняющих вейвлет-коэффициентов, была протестирована с помощью набора статистических тестов SP 800-22. Данный инструмент обнародован в 2003 году Американским Национальным институтом стандартов и технологий (American National Institute of Standards and Technology – NIST). Это стандарт для тестирования статистики случайных и псевдослучайных последовательностей. Он включает в себя 15 тестов, позволяющих оценить различные статистические параметры последовательности.

Результаты тестирования приведены в таблице 4. Как следует из таблицы, алгоритм не прошел универсальный тест Маурера для трех из четырех изображений, это означает, что в двоичной последовательности существуют значительно сжимаемые участки. Также алгоритм не прошел тест на последовательности и тест энтропии. Это означает то, что алгоритм генерирует битовую последовательность, которая по данным критериям не является случайной. Однако, учитывая остальные результаты, двоичная последовательность достаточно близка к случайной, чтобы препятствовать несанкционированному получению информации злоумышленниками.

Таблица 4 – Тестирование алгоритмами SP 800-22

№	Тест	Изображение							
		Мандрил		Лена		Перцы		Мармелад	
		P-value		P-value		P-value		P-value	
1	Frequency	0.739918	Пройден	0.534146	Пройден	0.350485	Пройден	0.911413	Пройден
2	Block Frequency	0.534146	Пройден	0.066882	Пройден	0.350485	Пройден	0.991468	Пройден
3	Runs	0.122325	Пройден	0.911413	Пройден	0.534146	Пройден	0.739918	Пройден
4	Longest Run	0.534146	Пройден	0.213309	Пройден	0.534146	Пройден	0.534146	Пройден
5	Rank	0.739918	Пройден	0.350485	Пройден	0.122325	Пройден	0.350485	Пройден
6	DFT	0.122325	Пройден	0.035174	Пройден	0.350485	Пройден	0.534146	Пройден
7	Non-Owerlaping Template	0.739918	Пройден	0.534146	Пройден	0.350485	Пройден	0.350485	Пройден
8	Owerlaping Template	0.534146	Пройден	0.739918	Пройден	0.739918	Пройден	0.911413	Пройден
9	Universal	0.000000	Не пройден	0.000000	Не пройден	0.350485	Пройден	0.000000	Пройден
10	Linear Complexity	0.739918	Пройден	0.534146	Пройден	0.350485	Пройден	0.213309	Пройден
11	Serial	0.000000	Не пройден	0.000000	Не пройден	0.000000	Не пройден	0.008879	Не пройден
12	Entropy	0.000000	Не пройден	0.000000	Не пройден	0.000000	Не пройден	0.035174	Не пройден
13	Cumulative Sums	0.739918	Пройден	0.534146	Пройден	0.122325	Пройден	0.066882	Пройден

Заявляемый способ представлен исполняемым модулем на базе платформы разработки программного обеспечения Qt и библиотеки OpenCL. Данный программный модуль предназначен для запуска на электронно-вычислительном программируемом устройстве и содержит набор классов и операций в них, которые приводят к созданию электрических сигналов в электронно-вычислительном программируемом устройстве и осуществлению в его оперативной памяти преобразования данных описанным способом.

Для увеличения скорости шифрования данный способ был разработан с учетом возможности использования параллельных вычислений. Обрабатываемое изображение представляется в виде матрицы пикселей по каждому из цветов в теле главной функции модуля. Матрица пикселей преобразуется путем последовательного применения нескольких раундов горизонтального и вертикального вейвлет-преобразования, реализованных в виде методов ядра OpenCL. Вейвлет преобразования для каждой строки и столбца вычисляются параллельно на отдельном вычислительном ядре графического процессора. К матрице LL-коэффициентов применяют последовательно r раундов перестановки и рассеяния с помощью хаотической последовательности. Данные преобразования также реализованы в виде функций OpenCL ядра для каждой строки и столбца матрицы пикселей выполняются раздельно и независимо. Уточняющие вейвлет-коэффициенты преобразуются в битовую последовательность и разбиваются на блоки равной длины. Каждый блок шифруется отдельно и независимо от других при помощи специальной функции OpenCL ядра. К каждому блоку многократно, r раундов, последовательно применяют базовое преобразование обратимого клеточного автомата второго порядка.

Для оценки производительности способа данным алгоритмом было зашифровано с использованием сжатия без потерь тестовое изображение «Мандрил» в различных разрешениях. Тестирование проводилось с помощью интегрированного графического процессора Intel(R) HD Graphics 4000, центрального процессора Intel Core i5-3230M. В таблице 5 представлены результаты тестирования. Скорость шифрования при сжатии без потерь находится на уровне 8 Мбит/с. Скорость шифрования может быть увеличена при использовании сжатия с потерями, однако качество восстановленного изображения будет ниже.

Таблица 5. Оценки времени шифрования изображения «Мандрил»

Разрешение	Количество пикселей	Размер, кбайт	Время шифрования, с
128x128	16384	48	0,209
192x192	36864	108	0,243
256x256	65536	192	0,278
384x344	147456	432	0,378
512x512	262144	768	0,692
640x640	409600	1200	0,907
768x768	589824	1728	1,343
896x896	802816	2352	2,102
1024x1024	1048576	3072	3,398
1152x1152	1327104	3888	3,664
1280x1280	1638400	4800	4,038
1536x1536	2359296	6912	6,351

Таким образом, заявляемый способ позволяет повысить эффективность шифрования из-за использования предварительного сжатия данных, что уменьшает объем данных, который необходимо зашифровать, а также, благодаря применению параллельных вычислений, позволяет проводить зашифрование в несколько потоков. Способ также имеет высокую стойкость к различным криптографическим атакам. Оценка гистограммы, коэффициентов корреляции и информационной энтропии в открытом и зашифрованном текстах. Результаты тестирования алгоритмами SP-800-22 позволяют сделать вывод о том, что данный способ является устойчивым к статистическим атакам. Оценка коэффициентов UACI и NPCR говорит о высокой стойкости способа к атакам дифференциального криптоанализа.

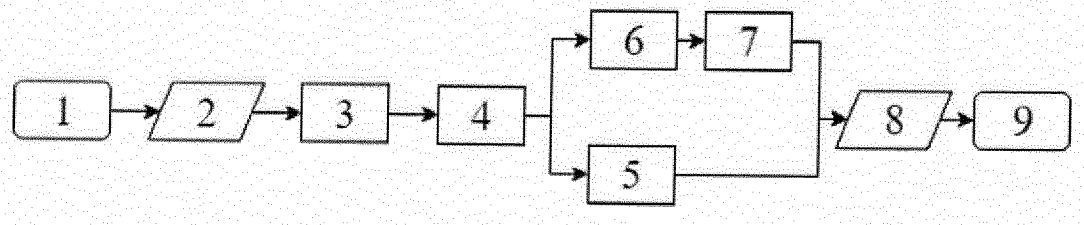
Источники информации:

1. Патент США №0202326, МПК H04L 9/00, 10.4.2003
2. Патент США №5751811, МКИ H04L 9/14; H04L 9/00, 12.05.1998

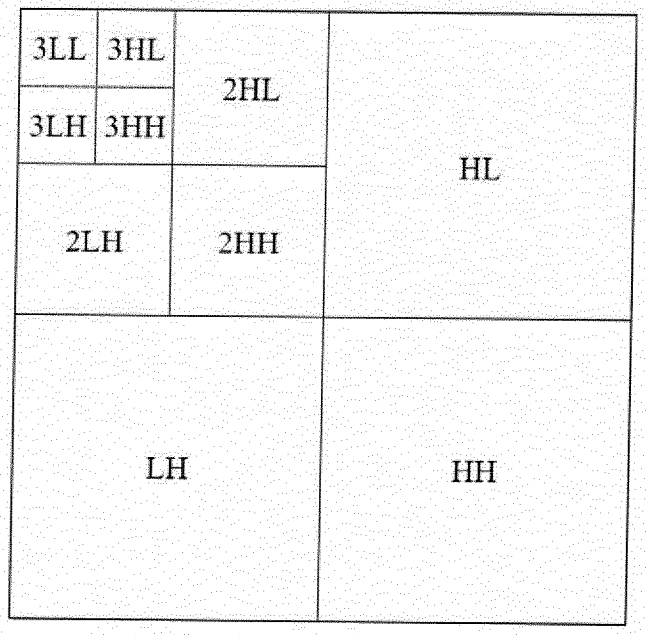
Формула изобретения

Способа шифрования изображений на основе дискретных хаотических отображений и клеточных автоматов, заключающийся в том, что посредством электронно-вычислительного программируемого устройства обрабатываемые данные считывают в оперативную память в виде матрицы целочисленных значений пикселей, с помощью заданной последовательности действий, приводящей к созданию электрических сигналов в электронно-вычислительном программируемом устройстве, к матрице пикселей изображения последовательно многократно в течение r раундов применяют операцию базового преобразования, причем в качестве операции базового преобразования используют вейвлет-преобразование; полученную в результате вейвлет-преобразования матрицу вейвлет-коэффициентов делят на низкочастотную LL-компоненту и высокочастотные LH, HL, HH компоненты; LL-компоненту матрицы вейвлет-коэффициентов шифруют с помощью хаотического перестановочно-рассеивающего алгоритма, где в качестве хаотической функции используют хаотическое отображение-тент, а начальное условие для хаотического отображения модифицируют с помощью хеш-функции; высокочастотные LH, HL и HH компоненты кодируют вложенным кодом HBCT (Hardware Block Cluster Tree), а затем шифруют с помощью метода, основанного на обратимых клеточных автоматах второго порядка в котором раундовый ключ модифицируют с помощью кусочно-линейного хаотического отображения.

Способ шифрования изображений на основе дискретных отображений и клеточных автоматов.

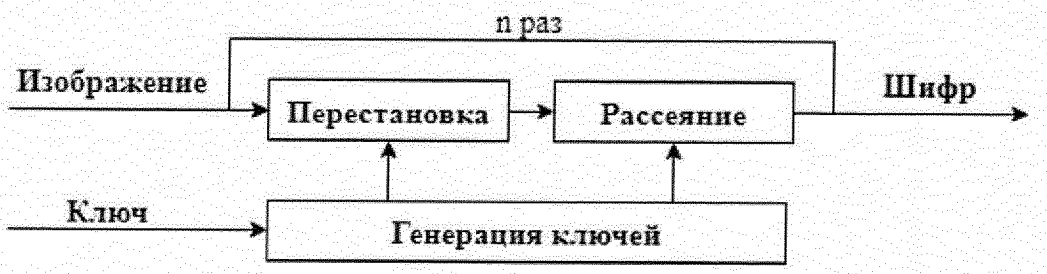


Фиг. 1

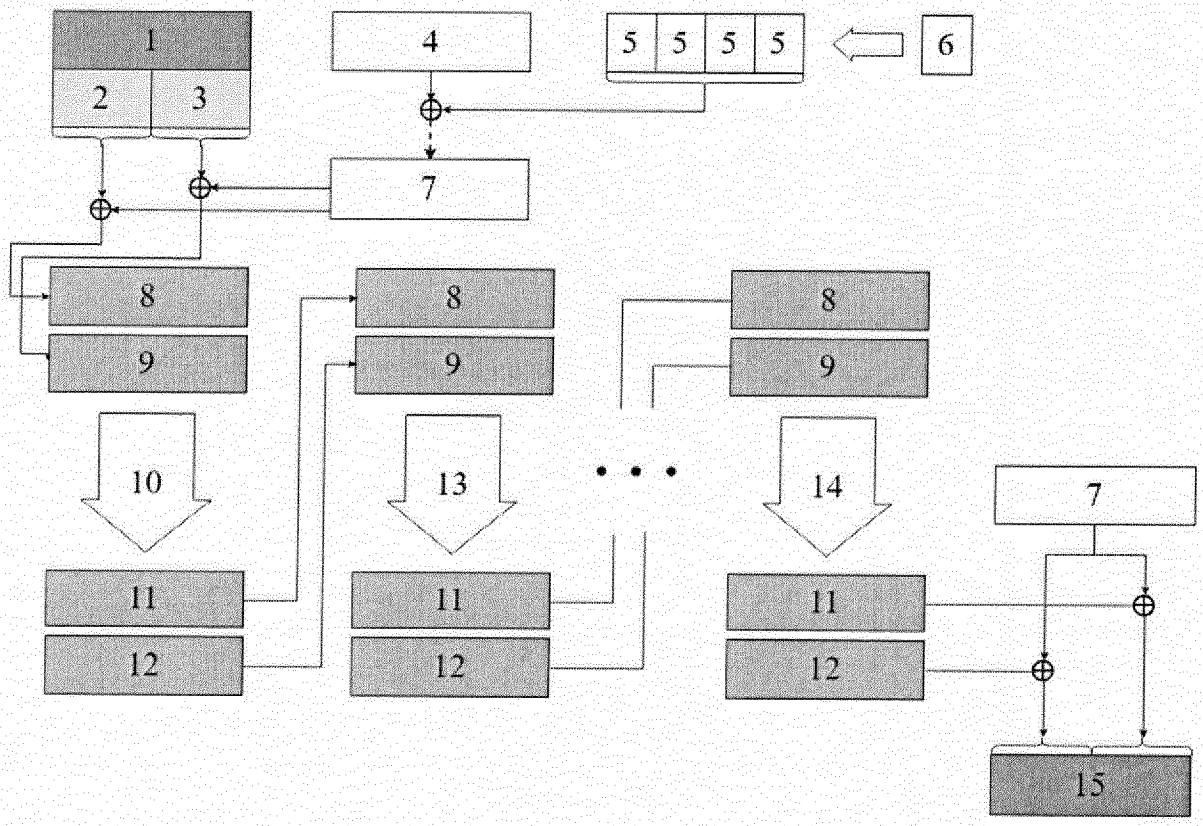


Фиг. 2

Способ шифрования изображений на основе дискретных отображений и клеточных автоматов.

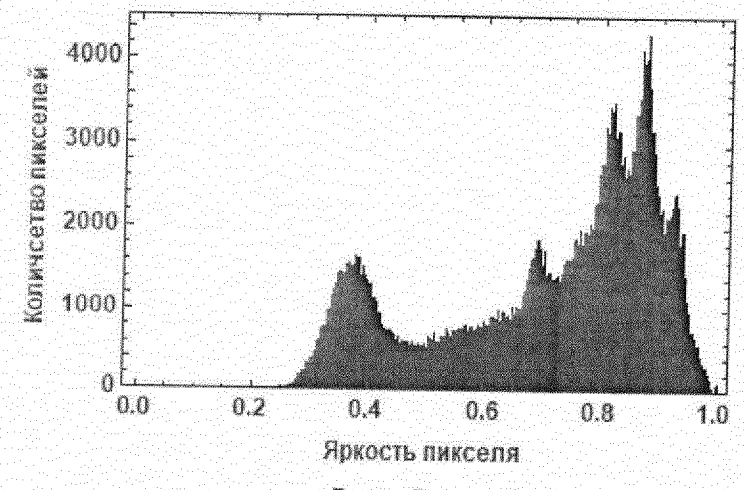


Фиг. 3

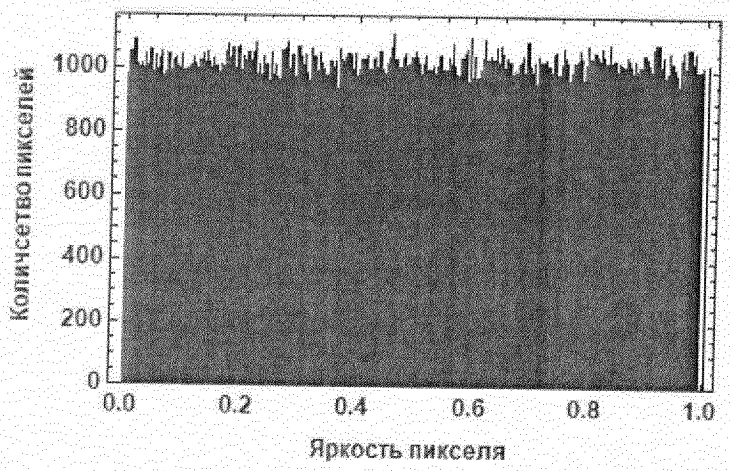


Фиг. 4

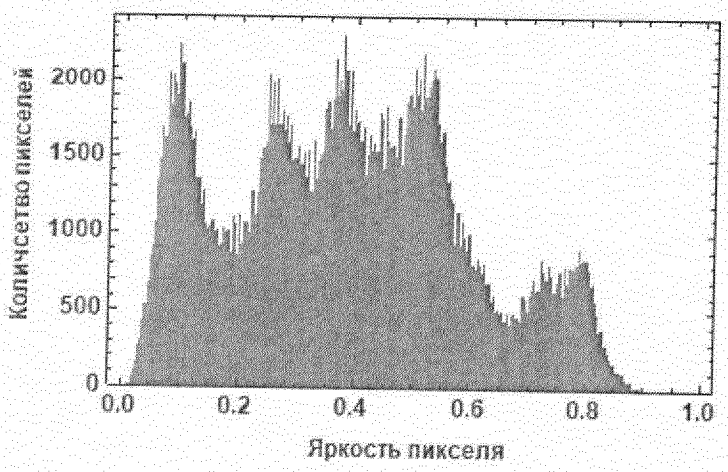
Способ шифрования изображений на основе дискретных отображений и клеточных автоматов.



Фиг. 5

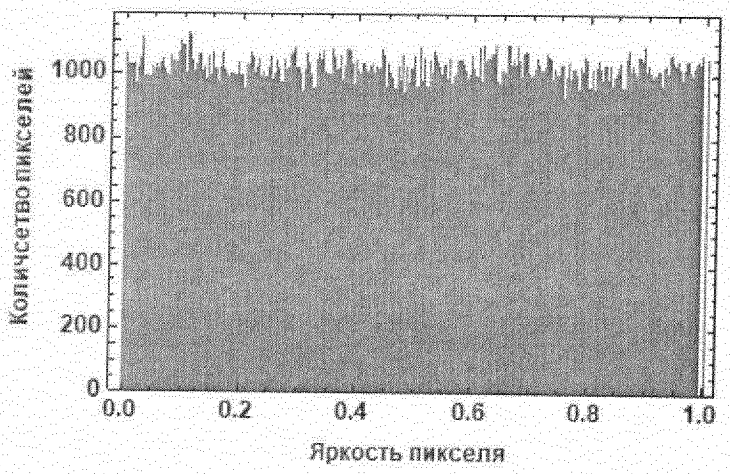


Фиг. 6

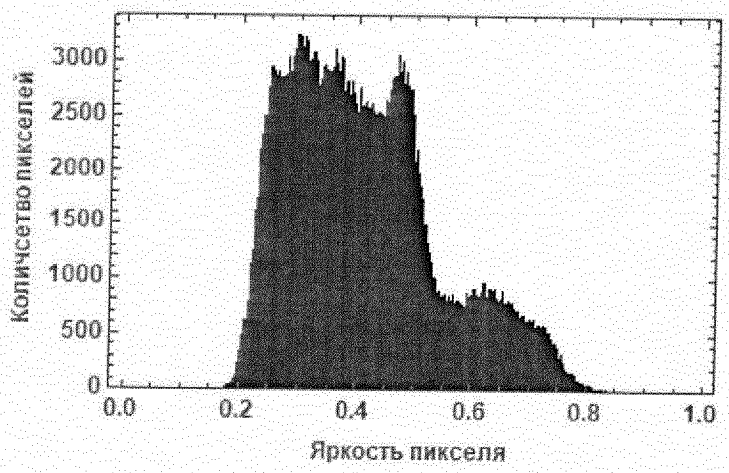


Фиг. 7

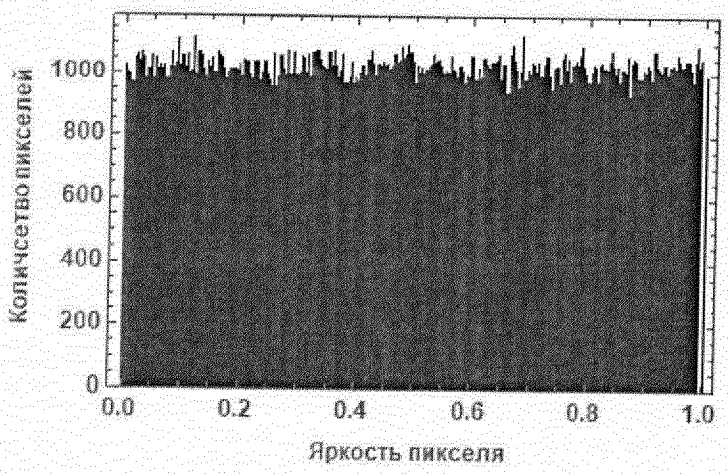
Способ шифрования изображений на основе дискретных отображений и клеточных автоматов.



Фиг. 8

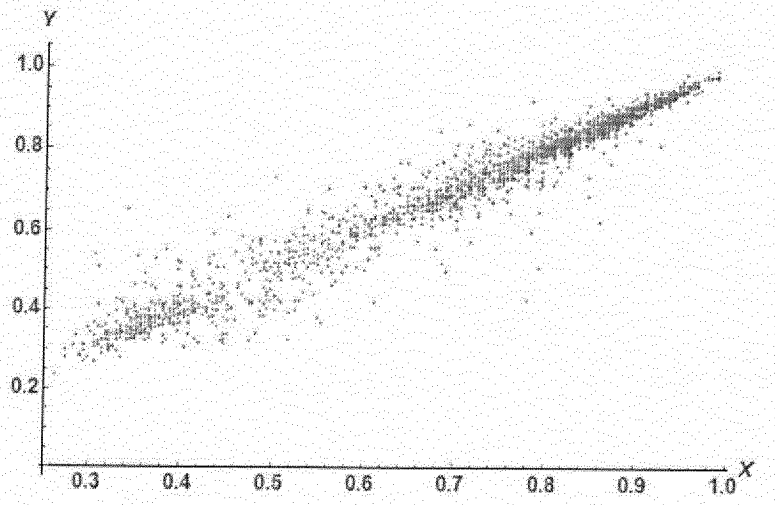


Фиг. 9

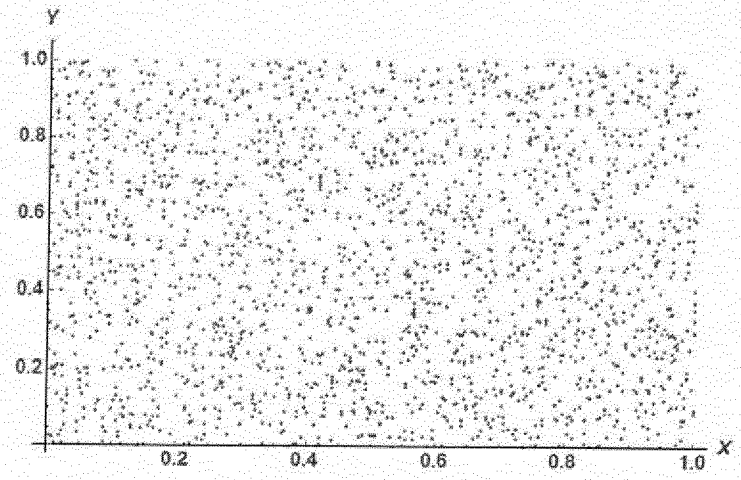


Фиг. 10

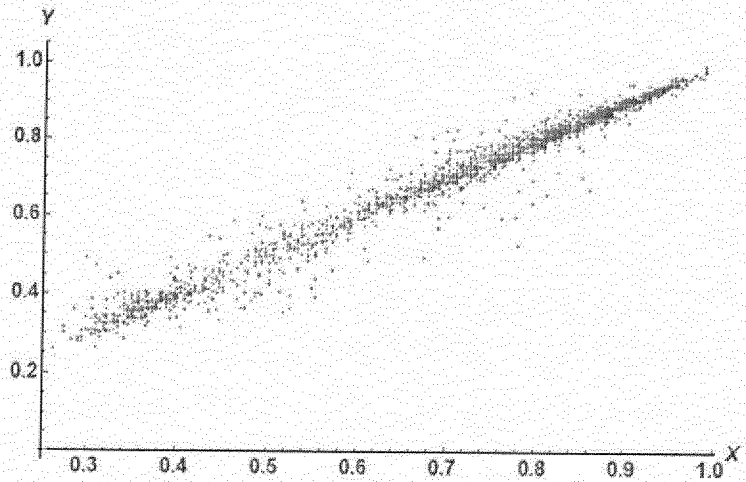
Способ шифрования изображений на основе дискретных отображений и клеточных автоматов.



Фиг. 11

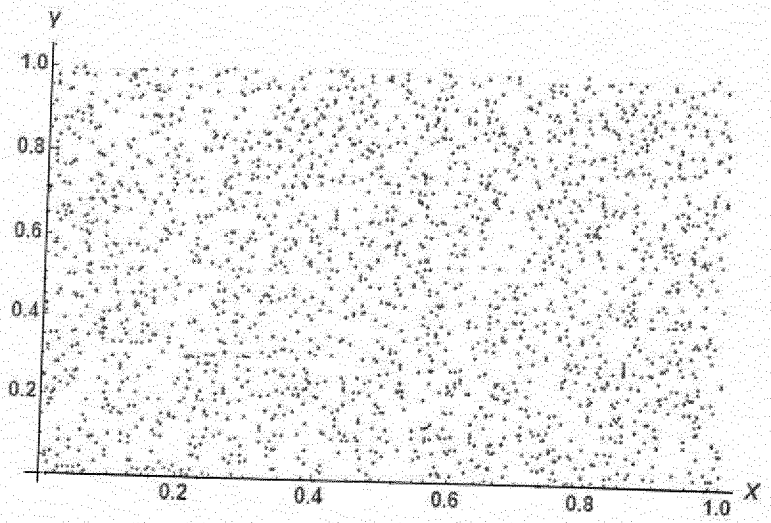


Фиг. 12

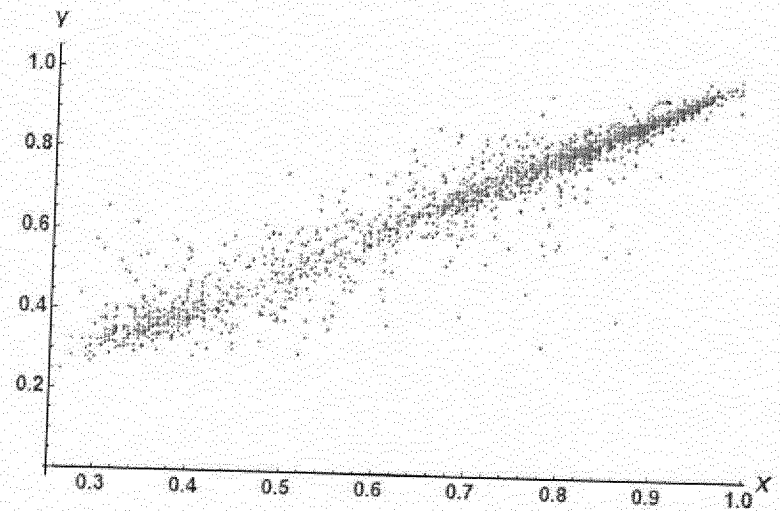


Фиг. 13

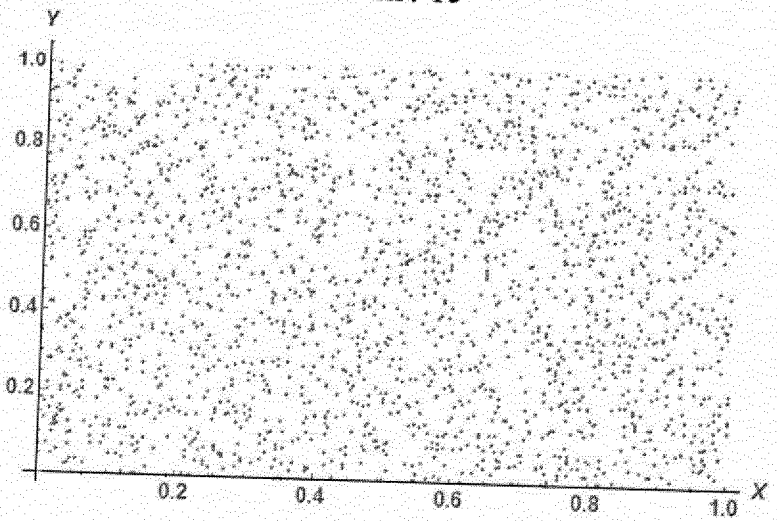
Способ шифрования изображений на основе дискретных отображений и клеточных автоматов.



Фиг. 14



Фиг. 15



Фиг. 16

ЕВРАЗИИСКОЕ ПАТЕНТНОЕ ВЕДОМСТВО

ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ

(статья 15(3) ЕАПК и правило 42 Патентной инструкции к ЕАПК)

Номер евразийской заявки: 201900228

Дата подачи: 20 марта 2019 (20.03.2019) | Дата испрашиваемого приоритета:

Название изобретения: СПОСОБ ШИФРОВАНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ДИСКРЕТНЫХ ОТОБРАЖЕНИЙ И КЛЕТОЧНЫХ АВТОМАТОВ

Заявитель: БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (БГУ)

☐ **Некоторые пункты формулы не подлежат поиску (см. раздел I дополнительного листа)**

☐ **Единство изобретения не соблюдено (см. раздел II дополнительного листа)**

А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:

МПК: ***H04N 19/00*** *(2014.01)* СПК: ***H04N 19/00*** *(2014-11)*
H04N 19/126 *(2014.01)* ***H04N 19/126*** *(2014-11)*

Согласно Международной патентной классификации (МПК) или национальной классификации и МПК

Б. ОБЛАСТЬ ПОИСКА:

Минимум просмотренной документации (система классификации и индексы МПК)
H04N 19/00-19/91

Другая проверенная документация в той мере, в какой она включена в область поиска:

В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
X	СИДОРЕНКО А.В. и др., Шифрование изображений на основе хаотических отображений с использованием параллельных вычислений, Информатика, издание, №4, 2017, с. 78-88, с. 78 Введение, с. 79-83 раздел 1. Алгоритм шифрования изображений на основе хаоса	1
A	US 2016/0255347 A1 (JEAN-CLAUDE COLIN) 01.09.2016	1
A	XING-YUAN Wang и др., Discrete wavelet transform-based simple range classification strategies for fractal image coding, Springer Science+Business Media Dordrecht, 02 October 2013, <doi: 10.1007/s11071-013-1076-4>	1
A	AMANY M. SARHAN и др., Chaos-based model for encryption and decryption of digital images, Multimedia Tools and Applications, September 2015, <doi: 10.1007/s11042-015-2883-z>	1

☐ последующие документы указаны в продолжении графы В ☐ данные о патентах-аналогах указаны в приложении

* Особые категории ссылочных документов:
"A" документ, определяющий общий уровень техники
"E" более ранний документ, но опубликованный на дату подачи евразийской заявки или после нее
"O" документ, относящийся к устному раскрытию, экспонированию и т.д.
"P" документ, опубликованный до даты подачи евразийской заявки, но после даты испрашиваемого приоритета
"D" документ, приведенный в евразийской заявке
"T" более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения
"X" документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну или изобретательский уровень, взятый в отдельности
"Y" документ, имеющий наиболее близкое отношение к предмету поиска, порочащий изобретательский уровень в сочетании с другими документами той же категории
"&" документ, являющийся патентом-аналогом
"L" документ, приведенный в других целях

Дата действительного завершения патентного поиска: 31 октября 2019 (31.10.2019)

Наименование и адрес Международного поискового органа:
Федеральный институт промышленной собственности
РФ, 125993,Москва, Г-59, ГСП-3, Бережковская наб., д. 30-1.Факс: (499) 243-3337, телетайп: 114818 ПОДАЧА

Уполномоченное лицо :
Т.М. Иванова
Телефон № (499) 240-25-91