УДК 004.415.2, 004.588

КВАНТОВОЕ РАСПОЗНАВАНИЕ ЛИЦ И КВАНТОВАЯ ВИЗУАЛЬНАЯ КРИПТОГРАФИЯ: МОДЕЛИ И АЛГОРИТМЫ

Ульянов Сергей Викторович[1], Петров Сергей Павлович[2]

[1]Доктор физико-математических наук, профессор;
ГОУ ВПО «Международный Университет природы, общества и человека «Дубна»,
Институт системного анализа и управления;
PronetLabs;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: ulyanovsv@mail.ru.

[2]Студент;
ГОУ ВПО Международный Университет природы, общества и человека «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: msgtome@bk.ru.

В работе проводится краткая классификация алгоритмов распознавания лиц. Вводится новая технология распознавания лиц, использующая разработанные квантовые алгоритмы и позволяющая повысить эффективность процесса распознавания. Работа полученных алгоритмов демонстрируется в задачах обработки изображений, предшествующих собственно распознаванию. В качестве дополнительного результата представлен квантовый алгоритм, разработанный на основе классического алгоритма визуальной криптографии и способный повысить эффективность кодирования и декодирования изображений. Задача сокрытия информации в изображении и задача распознавания и понимания изображения являются обратными и должны решаться совместно.

Ключевые слова: распознавание лиц, квантовый алгоритм, извлечение особенностей, детектор особенностей, дескриптор особенностей, квантовый бит, квантовая суперпозиция, квантовая корреляция, алгоритм шифрования, визуальная криптография.

QUANTUM FACE RECOGNITION AND QUNTUM VISUAL CRYPTOGRAPHY: MODELS AND ALGORITHMS

Ulyanov Sergey[1], Petrov Sergey[2]

[1]Doctor of Science in Physics and Mathematics, professor;
Dubna International University of Nature, Society and Man,
Institute of system analysis and management;
PronetLabs;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: ulyanovsv@mail.ru.

[2]Student;
Dubna International University of Nature, Society and Man,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: msgtome@bk.ru.

In this paper short classification of the face recognition algorithms is represented. A new face recognition technology that uses developed quantum algorithms is introduced. This approach can improve efficiency of face recognition process. The performance of the algorithms is demonstrated on image processing tasks which precede to actually recognition process. As additional result, quantum algorithm based on classical visual cryptography is represented. This algorithm is able to improve efficiency of image encryption and decryption. The task of information concealing and task of image recognition and understanding are inverse tasks and they should be solved jointly.

Keywords: face recognition, quantum algorithm, features extraction, features detector, features descriptor, quantum bit, quantum superposition, quantum correlation, encryption algorithm, visual cryptography.

Введение

В настоящее время возрастает интерес к решению задач распознавания лиц. В основном это связано с многочисленными практическими потребностями и огромным потенциалом области распознавания лиц. Вот далеко неполный список приложений алгоритмов распознавания лиц:

- Охранные системы;
- Криминалистика;
- Взаимодействие компьютер-человек;
- Виртуальная реальность, компьютерные игры;
- Контроль иммиграции;
- Персонификация бытовых устройств;
- Шифрование данных;
- Электронная коммерция и др.

Алгоритм распознавания лиц можно, так или иначе, разложить на несколько обобщенных этапов. На рис. 1 изображена общая последовательность шагов в процессе распознания лиц.

Рис. 1. Общая схема распознавания лиц

Более детализировано, процесс распознавания лиц на изображении может быть представлен следующими этапами:

1. предварительная обработка изображения, необходимая для приведения его в стандартный формат, удобный для распознавания;
2. выделение (обнаружение) лиц на изображении;
3. извлечение и кодирование наиболее представительных характеристик лиц (особенностей) из изображения;
4. сравнение лиц из изображения с лицами, хранящимися в базе данных, принятие решения о достоверности распознавания.

Каждый этап схемы может быть реализован множеством способов. Часть алгоритмов может использоваться одновременно на нескольких этапах процесса распознавания лица.

Эффективность работы алгоритма распознавания лица оценивается качеством распознавания (определяемым долей правильно идентифицированных изображений и долей ложно-позитивной классификации) т.е., в конечном счете, определяется доступными методами и алгоритмами анализа изображений, а также скоростью работы этих алгоритмов. Скорость зависит от качества программной реализации и используемых аппаратных средств.

Проблемы, возникающие в процессе распознавания лиц: наличие в наборе изображений лиц вариаций, таких как раса, пол, эмоции, освещения, положение головы, а также присутствие маскирующих признаков (очков, усов, зажмуренных глаз и др.).

Тематика данной работы посвящена новому подходу к распознаванию лиц на изображении, который применяет разработанные ранее (в [1, 2]) технологии квантовых вычислений. Используя эти технологии самостоятельно или совместно с классическими алгоритмами распознавания лиц, можно повысить эффективность отдельных этапов распознавания, а также процесса распознавания в целом. Данная работа является кратким анализом существующих технологий распознавания лиц. Кроме того здесь приводятся разработанные нами к настоящему моменту квантовые алгоритмы, используемые на начальных этапах процесса распознавания лиц на изображении и видео.

На сегодняшний день известно огромное количество классических алгоритмов и технологий распознавания лиц и их классификаций [3, 4 ,5]. В следующем разделе мы кратко рассмотрим одну из возможных классификаций методик, используемых в процессе распознавания лиц.

Классификации и краткий анализ характеристик классических алгоритмов, используемых в распознавании

Ниже рассмотрена одна из возможных классификаций техник распознавания лиц:

1. На основе геометрии (используется информация об относительной позиции и размерах особенностей). Требует настройки пороговых значений. Примеры: детектор Харриса, детектор Харриса-Лапласа, *SUSAN* (*Smallest Univalue Segment Assimilating Nucleus*) и др.
2. На основе шаблонов. Основной недостаток – необходимо проектировать шаблоны предварительно, сложность проектирования робастных шаблонов.
3. Сегментация на основе цвета. Основной недостаток – извлечение особенностей только из фронтальных или близких к ним изображений лиц.
4. Appearance-based approaches (*ASM*, *AAM*, *PCA*, *ICA*, вейвлеты Габора). Очень ресурсоемкий подход (с точки зрения использования памяти и процессорного времени). Кроме того, необходимо обучение и ручная расстановка контуров или ориентиров на изображениях. Такие подходы как *PCA*, *ICA* и вейвлеты Габора естественнее использовать для обнаружения лиц, нежели для извлечения особенностей.
5. Гибридные техники.

Отметим, что если задачу извлечения и кодирования особенностей удалось решить должным образом, то задача распознавания тривиальна и сводится к поиску экземпляра базы лиц с минимальным расстоянием до классифицируемого объекта.

В этом случае имеем следующую **постановку задачи**:

*Даны **N** точек особенностей входного изображения лица, сопоставив их с каждым набором точек особенностей изображений лиц из базы M_j, найти наиболее «близкое» изображение базы с точки зрения выбранной меры.*

Для этой поставленной задачи необходимо решить две основные подзадачи:

I. Каждая точка особенности характеризуется своим *дескриптором*. Дескриптором особенности в простейшем случае может выступать сама окрестность точки особенности. Необходимо выбрать/разработать алгоритм создания такого дескриптора, который был бы инвариантен к аффинным и проективным преобразованиям изображения, а также к изменению освещения.

   На сегодняшний день распространенны следующие подходы к созданию и сопоставлению дескрипторов особенностей [4, 6, 7]:
   - GLOH (Gradient Location and Orientation Histogram);
   - Affine shape adaptation;
   - Scale-space theory;
   - LESH (Local Energy based Shape Histogram);
   - Harris affine region detector;
   - Hessian affine region detector;
   - SURF (Speeded Up Robust Feature).

II. Другая не менее важная подзадача – выбор подходящей меры сходства двух множеств дескрипторов, соответствующих особенностям изображений лиц. В настоящее время широко используются меры сходства на основе кросс-корреляции двух изображений (см. Табл. 1).

Таблица 1. *Основные меры сходства двух изображений на основе кросс-корреляции*

Мера сходства	**Формула**
Сумма модулей разностей (Sum of Absolute Differences, SAD)	$\sum_{(i,j)\in W} \left\| I_1(i,j) - I_2(x+i,y+j) \right\|$
Сумма модулей разностей с нулевым средним значением (Zero-mean Sum of Absolute Differences, ZSAD)	$\sum_{(i,j)\in W} \left\| I_1(i,j) - \overline{I}_1(i,j) - I_2(x+i,y+j) + \overline{I}_2(x+i,y+j) \right\|$
Локально взвешенная сумма модулей разностей (Locally scaled Sum of Absolute Differences, LSAD)	$\sum_{(i,j)\in W} \left\| I_1(i,j) - \frac{\overline{I}_1(i,j)}{\overline{I}_2(x+i,y+j)} I_2(x+i,y+j) \right\|$
Сумма квадратов разностей (Sum of Squared Differences, SSD)	$\sum_{(i,j)\in W} \left(I_1(i,j) - I_2(x+i,y+j) \right)^2$
Сумма квадратов разностей с нулевым средним значением (Zero-mean Sum of Squared Differences, ZSSD)	$\sum_{(i,j)\in W} \left(I_1(i,j) - \overline{I}_1(i,j) - I_2(x+i,y+j) + \overline{I}_2(x+i,y+j) \right)^2$
Локально взвешенная сумма квадратов разностей (Locally scaled Sum of Squared Differences, LSSD)	$\sum_{(i,j)\in W} \left(I_1(i,j) - \frac{\overline{I}_1(i,j)}{\overline{I}_2(x+i,y+j)} I_2(x+i,y+j) \right)^2$
Нормализованная кросс-корреляция (Normalized Cross Correlation, NCC)	$\frac{\sum_{(i,j)\in W} I_1(i,j) I_2(x+i,y+j)}{\sqrt{\sum_{(i,j)\in W} I_1^{\,2}(i,j) \sum_{(i,j)\in W} I_2^{\,2}(x+i,y+j)}}$
Нормализованная кросс-корреляция с нулевым средним значением (Zero-mean Normalized Cross Correlation, ZNCC)	$\frac{\sum_{(i,j)\in W} (I_1(i,j) - \overline{I}_1(i,j))(I_2(x+i,y+j) - \overline{I}_2(x+i,y+j))}{\sqrt{\sum_{(i,j)\in W} (I_1(i,j) - \overline{I}_1(i,j))^2 \sum_{(i,j)\in W} (I_2(x+i,y+j) - \overline{I}_2(x+i,y+j))^2}}$
Сумма Хеммингових расстояний (Sum of Hamming Distances, SHD)	$\sum_{(i,j)\in W} \left(I_1(i,j) \; XOR \; I_2(x+i,y+j) \right)$

Очевидно, что такое решение задачи распознавания носит комбинаторный характер и требует поисков методов дальнейшей оптимизации. Эффективное решение этих подзадач является целью исследований множества авторов [3, 8, 9, 10].

В отдельный класс можно выделить *квантовые алгоритмы распознавания и обработки изображений*. Они призваны повысить эффективность классических алгоритмов распознавания за счет использования свойства квантового массивного параллелизма и, кроме того, представляют собой совершенно новый подход к распознаванию лиц и визуальной криптографии.

В следующем разделе описаны разработанные на данном этапе квантовые аналоги некоторых классических алгоритмов, описанных в этом разделе. Большая часть разработанных алгоритмов используется на начальных этапах распознавания лиц.

Разработанные модели квантовых алгоритмов, основанные на классических алгоритмах

Рассмотрим кратко некоторые модели квантовых алгоритмов распознавания.

Алгоритм преобразования классического изображения в квантовое состояние

Основное назначение данного алгоритма – конвертация изображения исходного изображения в квантовый вид с целью последующего применения квантовых алгоритмов (например, алгоритма Гровера [1] или квантовых геометрических преобразований [2]).

Разработанный квантовый подход к представлению и обработке изображения предполагает, что каждый пиксель изображения $x(i, j)$ должен быть преобразован в квантовое состояние $\left|q\left(i,j\right)\right\rangle$:

$$\left|q\left(i,j\right)\right\rangle = c_0\left|0\right\rangle + c_1\left|1\right\rangle,$$

где $\left|c_0\right|^2$ и $\left|c_1\right|^2$ – вероятности того, что после измерения состояние будет $\left|0\right\rangle$ и $\left|1\right\rangle$ соответственно, причем выполняется следующее условие: $\left|c_0\right|^2 + \left|c_1\right|^2 = 1$.

Необходимо отметить, что выбор начальных значений амплитуд вероятности $\left|c_0\right|^2$ и $\left|c_1\right|^2$, которые кодируют цвета пикселей изображения, может быть различным и зависит от используемого алгоритма преобразования изображения в квантовый вид.

Также, в зависимости от дальнейших преобразований, может возникнуть необходимость создания суперпозиции пикселей входного изображения. Суперпозиция создается в несколько шагов:

– Кодирование цветов пикселей (представленных в виде вещественных чисел) в комплексные амплитуды квантовых состояний:

$$\delta : \mathcal{R}^3 \to \mathbb{C}_1^2, \quad \left(x_1, x_2, x_3\right) \mapsto \left(r_1 e^{i\phi_1}, r_2 e^{i\phi_2}\right),$$

где x_1, x_2, x_3 – компоненты цветовой модели *RGB (red, green, blue)*, $r_1 := \sqrt{1 - x_3^2}$, $r_2 := x_3$, $\phi_1 := \arcsin\left(2x_1 - 1\right)$, $\phi_2 := \arcsin\left(2x_2 - 1\right)$.

Пусть $z_1 = r_1 e^{i\phi_1}, z_2 = r_2 e^{i\phi_2}$, тогда имеем цвет пикселя в виде:

$$\left|q_i\right\rangle = z_1\left|0\right\rangle + z_2\left|1\right\rangle.$$

Обратное преобразование выполняется по следующей схеме:

$$\gamma : \mathbb{C}_1^2 \to \mathcal{R}^3, \quad \left(z_1, z_2\right) \mapsto \left(\frac{1+\sin\phi_1}{2}, \frac{1+\sin\phi_2}{2}, \left|z_2\right|\right),$$

где $\phi_1 := \arg\left(z_1\right)$, $\phi_2 := \arg\left(z_2\right)$.

– Кодирование координат пикселей осуществляется следующим образом:

$$\left|k\right\rangle = \left|x\right\rangle\left|y\right\rangle = \left|x_{n-1}x_{n-2}...x_0\right\rangle\left|y_{n-1}y_{n-2}...y_0\right\rangle, x_i, x_i \in \{0,1\},$$

где состояния $\left|x\right\rangle$ и $\left|y\right\rangle$ кодируют координаты пикселей (номера столбца и строки пикселя соответственно).

В итоге получаем суперпозицию квантовых состояний пикселей входного изображения в виде:

$$\left|I\right\rangle = \frac{1}{2^n}\sum_{k=0}^{2^{2n}-1}\left|q_k\right\rangle \otimes \left|k\right\rangle.$$

Таким образом, алгоритм преобразования представляет изображение, состоящее из множества пикселей, в виде единой суперпозиции, содержащей характеристики всех пикселей изображения. Но так как в данном случае идет речь о модели квантового алгоритма и хранении пикселей на классическом компьютере, то амплитуды вероятности и вектора состояния, являющиеся слагаемыми суперпозиции, хранятся как отдельные значения.

Восстановление исходного изображения из квантовой суперпозиции носит более сложный характер. Результаты декодирования классического изображения из квантового состояния суперпозиции представлены на рис. 2 и 3.

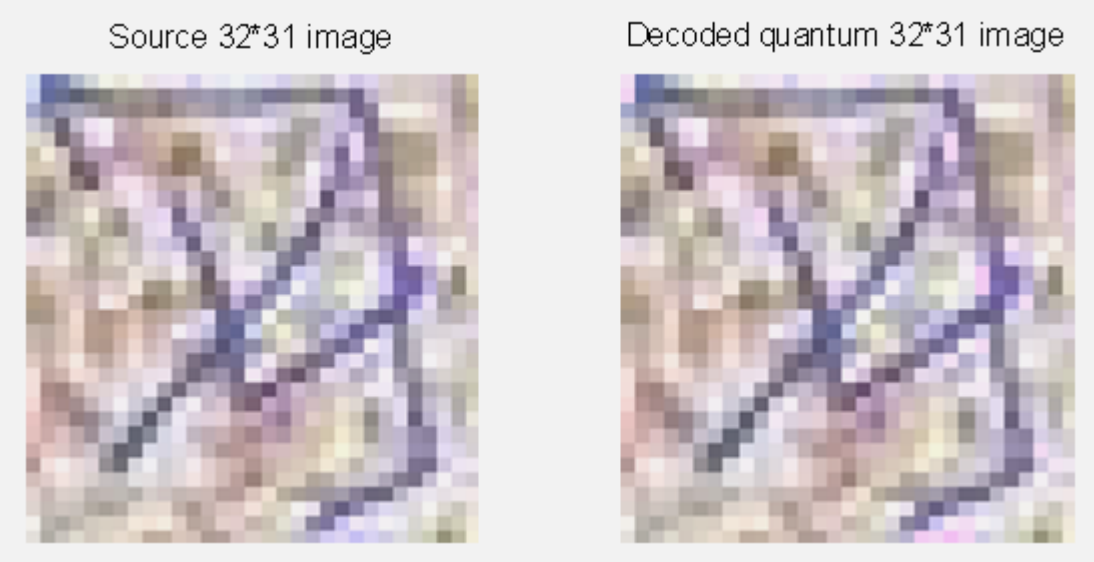

Рис. 2. Декодирование исходного изображения из квантовой суперпозиции

Количество неправильно декодированных пикселей: 36 из 992 (~3.6%)

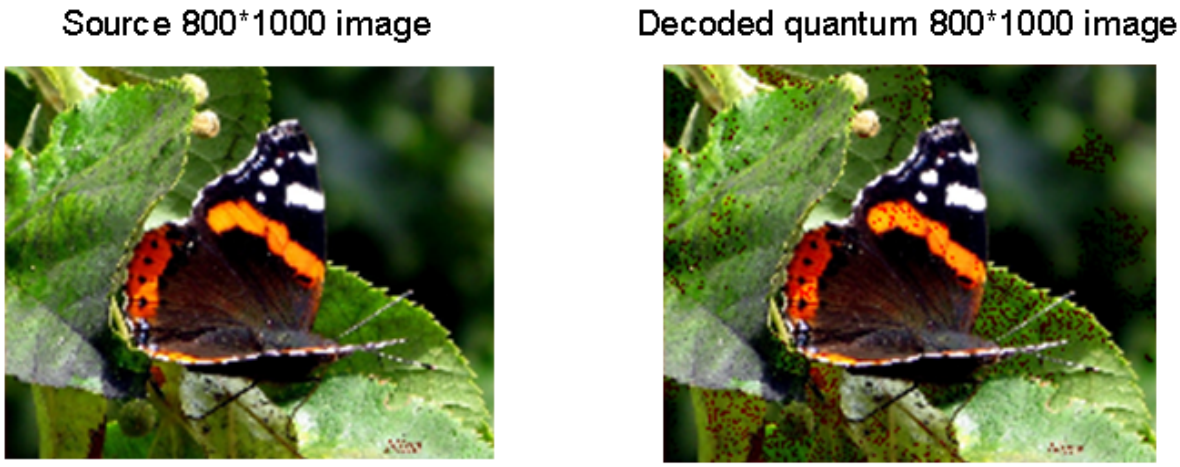

Рис. 3. Декодирование исходного изображения из квантовой суперпозиции.

Количество неправильно декодированных пикселей: 64973 из 800000 (~8.1%)

Наличие неправильно декодированных пикселей связано с необходимостью вычисления обратных тригонометрических функций в процессе декодирования пикселей входного изображения, что и ведет к потере информации. Процесс декодирования требуют дополнительных исследований.

Модель квантового алгоритма преобразования полутонового изображения в бинарное изображение.

Преобразование изображения из шкалы серого в бинарное является неотъемлемой частью предварительной обработки изображения многих классических алгоритмов распознавания лиц. Оно может неоднократно использоваться на различных этапах работы алгоритма. Разработанный алгоритм может быть применен в задачах, позволяющих сжатие входного изображение за счет удаления избыточной в данной задаче информации, например, задаче сегментации изображения для обнаружения на нем лиц. Бинарное изображения занимает меньше памяти и требует меньшего процессорного времени на обработку.

Разработанный квантовый алгоритм можно разделить на несколько шагов:

Шаг 1. Дано полутоновое изображение (в шкале яркости серого цвета) размером $M \times N$. Преобразуем каждый пиксель входного изображения $x(i, j)$ в квантовое состояние $\left|q(i, j)\right\rangle$ (кубит), которое является суперпозицией базовых квантовых состояний $\left|0\right\rangle, \left|1\right\rangle$, т.е. $\left|q(i, j)\right\rangle = c_0\left|0\right\rangle + c_1\left|1\right\rangle$, где $|c_0|^2$ – вероятность измерения $\left|0\right\rangle$, $|c_1|^2$ – вероятность измерения $\left|1\right\rangle$. Сумма этих вероятностей равна единице.

Если интенсивность каждого пикселя представлена вещественным числом из отрезка [0,1], то вероятности $|c_0|^2$ и $|c_1|^2$ могут быть вычислены стандартным образом.

Определим две суммы s_1 и s_2 так:

$$s_1 = \sum_{k=-1}^{1}\sum_{l=0}^{1} x(i-k, j-l) + x(i, j+l) + x(i, j+2);$$

$$s_2 = x(i-1, j-1) + x(i-1, j) + x(i, j-l).$$

Пусть $P = (s_1 + s_2)/5$.

Тогда $|c_0|^2 = f(P)$, а $|c_1|^2 = 1 - f(P)$, где $f(P) = \dfrac{1}{1 + e^{-\frac{P-a}{b}}}$, a и b – известные параметры.

Когда базисные состояния $\left|0\right\rangle, \left|1\right\rangle$ соответствуют векторам $\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}$, тогда квантовому биту $\left|q(i, j)\right\rangle$ соответствует вектор $\begin{pmatrix}1-f(P)\\f(P)\end{pmatrix}$, т.е. интенсивность каждого пикселя изображения отображается в 2D пространство.

Шаг 2. Измерение кубита $\left|q(i, j)\right\rangle$ каждого пикселя входного изображения позволяет сформировать матрицу изображения, каждый элемент которой есть некоторое базисное состояние, зависящее от результата измерения соответствующего кубита. Измерение проводится следующим способом: разыгрывается случайное число из отрезка [0, 1]. Если случайное число попало в отрезок $[0, |c_1|^2]$, то результат измерения – базисное состояние $\left|0\right\rangle$, если же случайное число попало в отрезок $[c_1|^2, 1]$, то результат измерения – базисное состояние $\left|1\right\rangle$. Пусть базисные состояния $\left|0\right\rangle, \left|1\right\rangle$ соответствуют значениям 0, 1 пикселя выходного бинарного изображения. Таким образом, мы получили выходное бинарное изображение.

В качестве примера на рис. 4 представлены результаты работы алгоритма при значении параметра $a = 0.5$ и различных значениях параметра b, влияющего на степень размытия бинарного изображения.

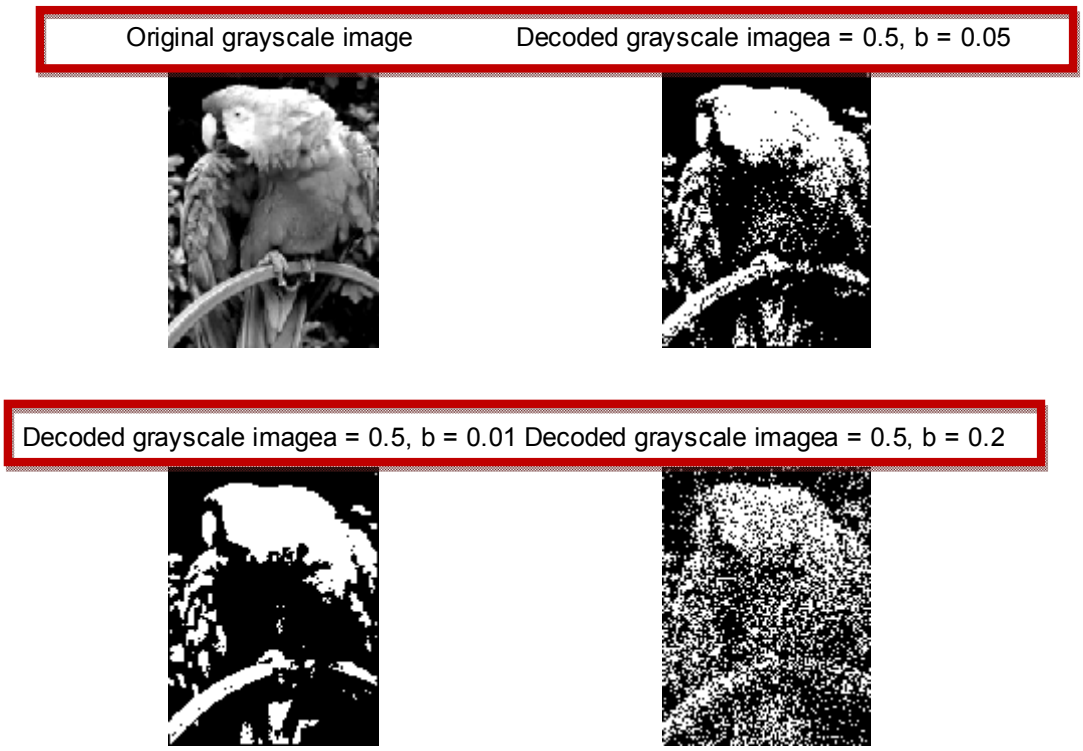

Рис. 4. Результаты работы алгоритма преобразования полутонового изображения в бинарное

Примечание. На рис. 4 и ниже на рис. 5 обозначено: original grayscale image – исходное изображение на шкале серого цвета; decoded grayscale image - декодированное изображение на шкале серого цвета; containing edges – параметры градации шкал цвета)

Модель квантового алгоритма выделения границ

Данный алгоритм позволяет преобразовывать входное изображение в бинарную карту краев, тем самым также осуществляет сжатие информации. Карта краев может быть использована, например, для поиска и выделения предметов на изображении (в том числе и лиц).

Алгоритм разработан в рамках первого этапа распознавания, связанного с подготовкой входного изображения к последующему обнаружению лица и извлечения его характеристик. В процессе работы этого алгоритма создается карта краев изображения, анализируя которую можно вычленить из изображения такие элементы как: лицо, глаза, рот и т.д. Работу алгоритма можно логически разделить на два шага.

Шаг 1. Дано полутоновое изображение (в шкале яркости серого цвета) размером $M \times N$. Преобразуем каждый пиксель входного изображения $x(i, j)$ в квантовое состояние $\left|q(i, j)\right\rangle$ (кубит), которое является суперпозицией базовых квантовых состояний $\left|0\right\rangle, \left|1\right\rangle$, т.е. $\left|q(i, j)\right\rangle = c_0\left|0\right\rangle + c_1\left|1\right\rangle$, где $|c_0|^2$ – вероятность измерения $\left|0\right\rangle$, $|c_1|^2$ – вероятность измерения $\left|1\right\rangle$. Сумма этих вероятностей равна единице.

Если интенсивность каждого пикселя представлена вещественным числом из отрезка [0,1], то вероятности $|c_0|^2$ и $|c_1|^2$ могут быть вычислены по аналогии с вышеприведенным.

Вычислим производные для каждого пикселя изображения по методу Собеля [13]:

$$g_r(i, j) = [x(i+1, j-1) + 2x(i+1, j) + x(i+1, j+1)] - [x(i+1, j-1) - 2x(i-1, j) - x(i-1, j+1)];$$

$$g_c(i, j) = [x(i-1, j+1) + 2x(i, j+1) + x(i+1, j+1)] - [x(i-1, j-1) - 2x(i, j-1) - x(i+1, j-1)].$$

Далее вычислим величину градиента в каждом пикселе: $g(i,j)=\sqrt{g_r{}^2(i,j)+g_c{}^2(i,j)}$. Тогда $|c_0|^2=1-f(g(i,j))$ и $|c_1|^2=f(g(i,j))$, где $f(P)=\dfrac{1}{1+e^{-\frac{P-a}{b}}}$, a и b – известные параметры.

Шаг 2. Измерение кубита $|q(i,j)\rangle$ каждого пикселя входного изображения позволяет сформировать матрицу изображения, каждый элемент которой есть некоторое базисное состояние, зависящее от результата измерения соответствующего кубита. Измерение проводится следующим способом: разыгрывается случайное число из отрезка [0, 1]. Если случайное число попало в отрезок $[0,|c_1|^2]$, то результат измерения – базисное состояние $|0\rangle$, если же случайное число попало в отрезок $[c_1|^2,1]$, то результат измерения – базисное состояние $|1\rangle$.

Состояние пикселя выходной карты изображений определяется следующим образом:

- Если в результате измерений получено базисное состояние $|0\rangle$, то пиксель выходного изображения будет нулевым.
- Если в результате измерений получено базисное состояние $|1\rangle$ и выполняются следующие условия: $|g_r(i,j)|>|g_c(i,j)|$, $g(i,j)>g(i+1,j)$, $g(i,j)>g(i-1,j)$, то значение пикселя выходного изображения будет равным единице.
- Если в результате измерений получено базисное состояние $|1\rangle$ и выполняются следующие условия: $|g_c(i,j)|>|g_r(i,j)|$, $g(i,j)>g(i,j+1)$, $g(i,j)>g(i,j-1)$, то значение пикселя выходного изображения будет равным единице.
- В остальных случаях значение пикселя выходного изображения будет равным нулю.

Результаты работы алгоритма при различных параметрах *a* и *b* представлены на рис. 5.

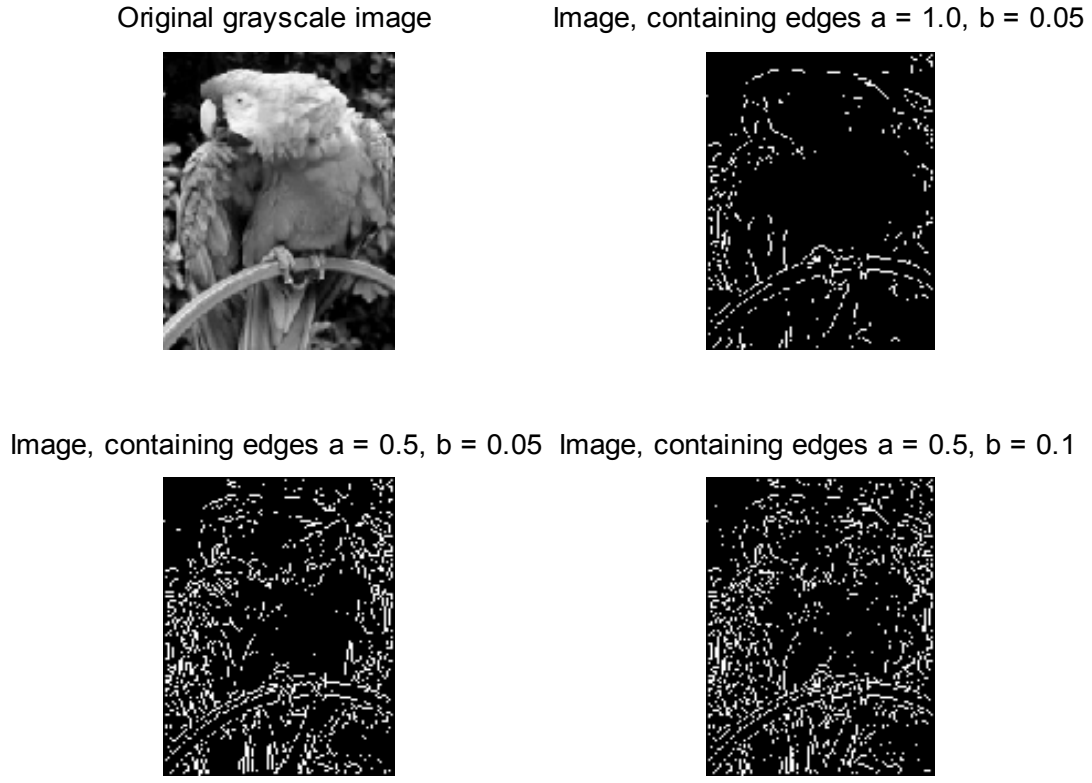

Рис. 5. Результаты работы алгоритма выделения границ

Результат работы алгоритма – карта краев – используется в процессе распознавания.

Обратной задачей для распознавания является задача сокрытия информации в изображении или их последовательности. Эту задачу можно решать с помощью квантового криптографического алгоритма.

Модель квантового алгоритма визуальной криптографии

В качестве дополнительного результата был разработан алгоритм квантовой визуальной криптографии. Алгоритм является расширением классического алгоритма визуальной криптографии (М. Наор, А. Шамир, 1994, см. Приложение) и предназначен для кодирования изображений при обмене секретной информацией.

Рассмотрим (2, 2)-квантовую визуальную схему секретного обмена. Пусть имеем изображение размером $M \times N$, из которого необходимо получить два «теневых» изображения размером $2M \times 2N$ каждое. Преобразуем каждый пиксель входного изображения $x(i, j)$ в квантовое состояние $\left|q(i, j)\right\rangle$, которое является суперпозицией четырех базовых квантовых состояний $\left|00\right\rangle, \left|01\right\rangle, \left|10\right\rangle$ и $\left|11\right\rangle$, т.е. $\left|q(i, j)\right\rangle = c_1\left|00\right\rangle + c_2\left|01\right\rangle + c_3\left|10\right\rangle + c_4\left|11\right\rangle$. Вероятности измерения каждого базового состояния равны, т.е. $|c_1|^2 = |c_2|^2 = |c_3|^2 = |c_4|^2 = 1/4$.

Для каждого базового состояния из $\left|00\right\rangle, \left|01\right\rangle, \left|10\right\rangle$ и $\left|11\right\rangle$ выбирается взаимно-однозначное соответствие из множества возможных состояний группы пикселей, характеризующих каждый пиксель исходного изображения в «теневом» изображении. Например, состоянию $\left|00\right\rangle$ может соответствовать группа пикселей $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$, состоянию $\left|01\right\rangle$ может соответствовать группа пикселей $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$, состоянию $\left|10\right\rangle$ может соответствовать группа пикселей $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, состоянию $\left|11\right\rangle$ может соответствовать группа пикселей $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Таким образом, в зависимости от того какое базовое квантовое состояние мы получили при измерении квантового состояния пикселя исходного квантового изображения будут выбраны соответствующие цвета пикселей одного из классических «теневых» изображений, характеризующих пиксель исходного изображения.

На рис. 6 проиллюстрирован пример выбора цветов, описанный выше.

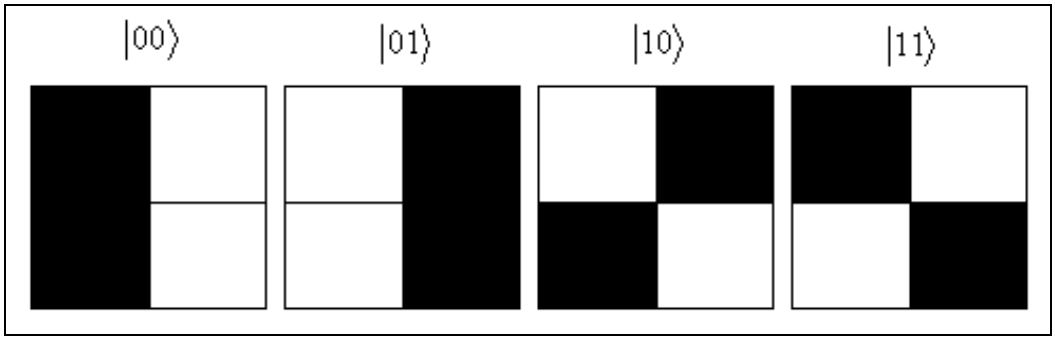

Рис. 6. Соответствие квантовых состояний цветам пикселей «теневого» изображения

Цвета пикселей остальных «теневых» изображений (в нашем случае еще одного) будут выбраны таким образом, чтобы при наложении «теней» получался «серый» пиксель для белого пикселя исходного изображения и черный (несущий информацию) пиксель для черного пикселя исходного изображения (см. предыдущий раздел).

На рис. 7 приведен результат моделирования описанной (2, 2)-квантовой визуальной схемы секретного обмена. Исходное черно-белое изображения используется описанным в этом разделе алгоритмом для получения двух «теневых» изображений, каждое из которых может передаваться без опасений за сохранность информации исходного изображения.

Информация, содержащаяся в исходном изображении, проявляется при совмещении обоих «теней» посредством логической операции *OR*[1].

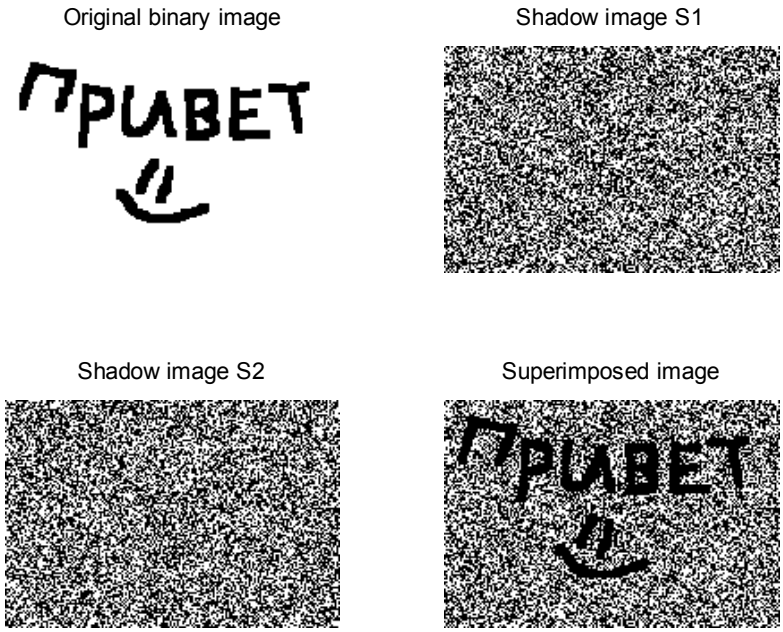

Рис. 7. Результат работы квантового криптографического алгоритма: надпись исходного изображения проявляется только при наложении двух «теневых» изображений

Гибридный алгоритм обнаружения лиц на изображении

Данный алгоритм используется для локализации лиц на изображении. Работа алгоритма делится на две ветви: обнаружение лица по карте краев, и обнаружение лица по цвету кожи.

Для получения карты краев может использоваться квантовый алгоритм обнаружения краев или один из существующих классических алгоритмов обнаружение краев. Алгоритм обнаружения лица по цвету кожи является чисто классическим, суть его состоит в следующем: на подготовительном этапе выполняется построение распределения цветов кожи на основе выборки изображений участков кожи людей различной расы, на последнем этапе участки изображения, найденные с помощью карты краев, с учетом их формы анализируются посредством построенного распределения и для каждого участка выставляется степень его соответствия лицу. Задание порогового значения позволяет отбраковать часть неподходящих участков изображения.

В связи с тем, что алгоритм не учитывает условия освещения, эффективность его невелика. Неправильное задание порогового значения также может привести к отбраковке реальных лиц.

На рис. 8 представлены работа алгоритма в случае, когда на вход ему подается изображение карты краев, полученной квантовым алгоритмом.

Из рис. 8 видно, что по карте краев изначально обнаружено два округлых замкнутых объекта, каждый из которых, вообще говоря, мог бы быть лицом. Но после фильтрации объектов по размеру, осталось только реальное изображение лица. Таким образом, для определенного класса изображений требуется собственная настройка параметров алгоритма.

[1] Различные логические операции, используемые при совмещении двух и более изображений, позволяют регулировать представление исходного изображения, полученное при наложении «теневых». Например, чтобы получить *белый* фон конечного изображения (а не *серый*), необходимо просто использовать операцию *XOR*.

Рис. 8. Слева – карта краев, полученная квантовым алгоритмом, справа – результат работы алгоритма по обнаружения лиц

Рассмотрим рис. 9 и 10, на которых изображены карты краев с различными параметрами, полученные квантовым алгоритмом выделения границ и результат работы алгоритма по обнаружению лиц соответственно.

Рис. 9. Карты краев полученные квантовым алгоритмом выделения границ

Рис. 10. Результат работы алгоритма по обнаружения лиц

Из рис. 10 видно, что возникают случаи, когда за лицо принимается часть изображения, не являющаяся лицом.

Другие квантовые алгоритмы, требуемые в процессе распознавания

Алгоритм Гровера представляет собой квантовый алгоритм поиска заданного лица (или нескольких лиц) в неупорядоченной базе лиц. Этот алгоритм обладает скоростью $\sqrt{N}$, что гораздо выше классических алгоритмов неупорядоченного поиска. Для ускорения поиска перебора лиц на классическом компьютере можно использовать модель алгоритма Гровера [1]. Одна из возможных схем реализации может быть следующая.

Входное изображение обрабатывается с целью обнаружения на нем лиц, представительные особенности лиц извлекаются и кодируются в форму, удобную для сравнения с лицами, находящимися в базе (можно использовать стандартные меры, приведенные в Табл. 1). Лица, находящиеся в базе также подвергаются процедуре кодирования.

Таким образом, имеем базу лиц, хранимых в удобной для нас форме. Далее применяются операторы квантового алгоритма Гровера, причем алгоритм сравнения лиц закодирован в виде квантового оракула (см. рис. 11).

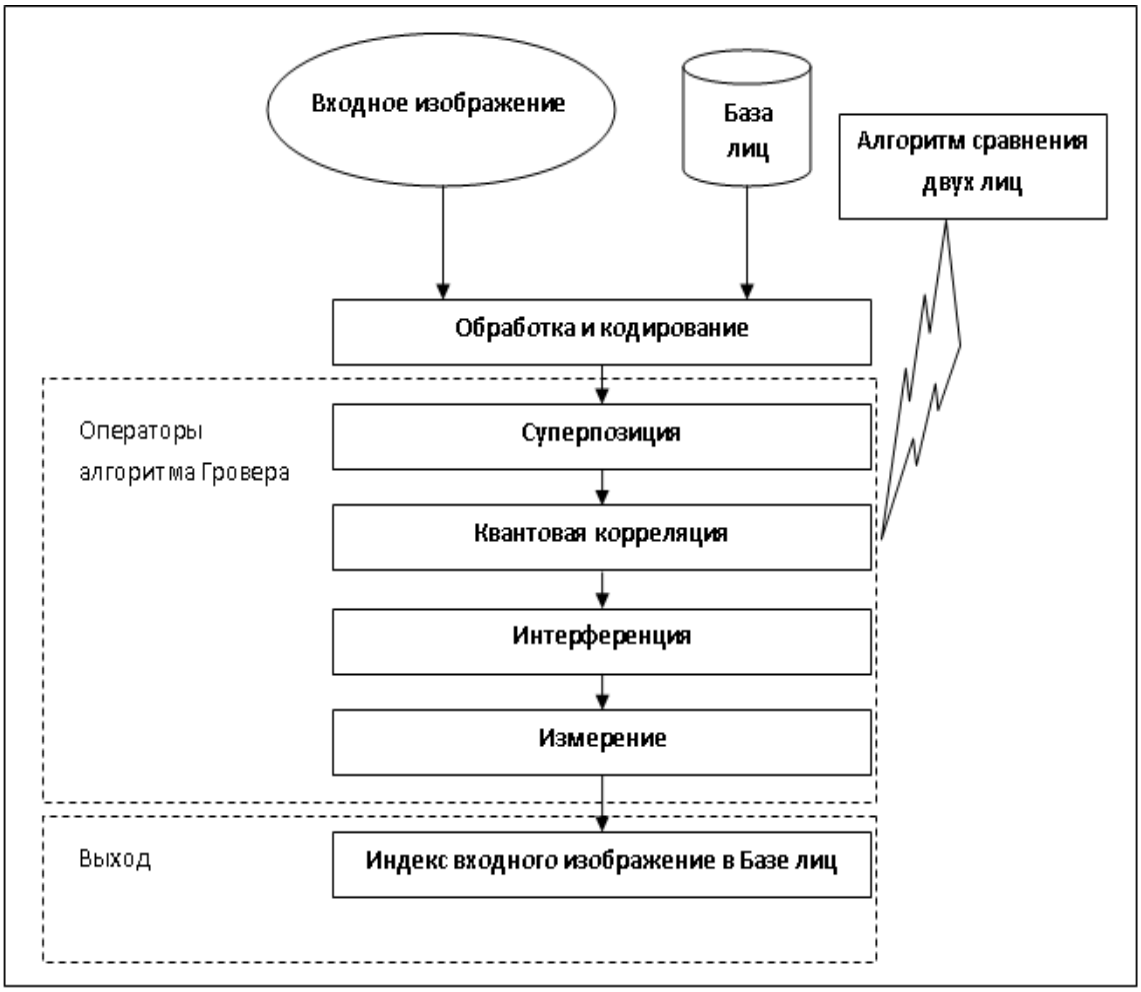

Рис. 11. Схема квантового распознавания лица

Важно, что весь процесс распознавания лиц можно разделить на два независимых этапа:

- Обработка и кодирование начальных данных и параметров;
- Поиск в базе с помощью квантового алгоритма Гровера.

Меняя качество начальной обработки изображений и алгоритм сравнения лиц можно добиться более эффективного распознавания лиц. Необходимо отметить, что первый этап распознавания может быть выполнен как с помощью классических методов, так и с помощью квантовых.

Кроме того, любая задача распознавания образов, подразумевающая перебор вариантов, может быть решена, используя модификации алгоритма.

Квантовые алгоритмы геометрических преобразований. Данные алгоритмы позволяют совершать преобразования поворота изображения или его частей, изменения положения частей внутри изображения, выполнять масштабирование изображения посредством применения квантовых операторов. Наличие такого универсального базиса квантовых алгоритмов позволит реализовать практически любые операции по обработке изображения (аффинные трансформации, реструктуризация элементов изображения, применение фильтров и др.).

Другие алгоритмы распознавания лиц. Наличие квантовых аналогов классических алгоритмов (таких как ASM, AAM, PCA, ICA, квантовые вейвлеты Габора) позволит повысить эффективность существующих методик распознавания, а также сделает возможным разработку и использование новых техник.

Заключение

К недостаткам современных методик распознавания изображений относятся:

- погрешность при поиске по большим базам данным;
- погрешность распознавания при изменении ракурса объекта;
- влияние освещения на качество распознавания;
- возрастные изменения;
- маскирующие признаки;
- чувствительность ПО к лицевой мимике.

Разрабатываемая технология для систем распознавания лиц на изображениях и видео базируется на применении интеллектуальных квантовых вычислений. Она позволит осуществлять параллельную обработку больших массивов данных изображений лиц и с использованием квантовой корреляции между информативными признаками изображений реализует эффективный метод распознавания.

Используя базис квантовых алгоритмов в сочетании с имеющимися классическими алгоритмами можно реализовать эффективное распознавание лиц, которое позволит преодолеть (полностью или частично) многих перечисленных недостатков.

Преимущества использование квантовых вычислений в распознавании лиц:

- потенциальные возможности ускорения вычислений за счет применения квантовых эволюционных операторов;
- введение квантовых операторов суперпозиции и корреляции в классический алгоритм, а также вероятностная сущность квантового алгоритма, влекут за собой появления уникальных свойств процесса обработки данных, что отражается на результате работы алгоритма;
- принципиально новый подход к описанию алгоритмов распознавания лиц и алгоритмов визуальной криптографии/стеганографии;
- слабая зависимость от помех окружающей среды;
- независимость от статичности или движения объекта или камеры;
- передача полноценного видеоизображение по низкоскоростным каналам связи;
- обеспечение высокого уровня безопасности при попытках внесения помех в каналы контроля изображений.

Задача сокрытия визуальной информации является обратной к задаче распознавания. Классическая схема визуальной криптографии обладает такими достоинствами как: простота реализации, высокая криптостойкость, возможность распараллеливания процессов кодирования и декодирования изображения, отсутствие необходимости вообще использовать сложную вычислительную технику (в широком смысле) для использования этой схемы.

Полученная в качестве дополнительного результата схема квантовой визуальной криптографии наследует большинство преимуществ классической схемы, а также расширяет ее возможности. Кван-

товый алгоритм визуальной криптографии можно использовать самостоятельно или в составе других квантовых криптографических алгоритмов, квантовых алгоритмах обработки изображений и видео.

Применение в будущем квантового компьютера может повысить эффективность представленного алгоритма путем интеграции с квантовым оракулом [1]. Высокая скорость кодирования/декодирования изображений позволит использовать схему визуальной криптографии для потокового видео, и тем самым повысит безопасность онлайн видео-коммуникаций.

Список литературы

1. Litvintseva L.V., Ulyanov S.V. et al. Quantum information and quantum computational intelligence: Backgrounds and applied toolkit of information design technologies. – Milan. Note del Polo (Ricerca), Universita degli Studi di Milano, 2005. – Vol. 78-86.
2. Le P.Q., Iliyasu A.M., Dong F., Hirota K. Fast geometric transformations on quantum images // IAENG Intern. J. of Applied Mathematics. – 2010. – Vol. 40. – № 3; A framework for representing and producing movies on quantum computers // International Journal of Quantum Information. – 2011. – Vol. 9. – №. 6. – Pp. 1459-1497.
3. Ekta W., Anu S. A conceptual study on image matching techniques. // Global Journal of Computer Science and Technology. – 2010. – Vol. 10. – № 12. – Pp. 83-88.
4. Stan Z.L., Anil K.J. Handbook of face recognition. – Springer Science + Business Media, 2005.
5. Лифшиц Ю. Методы распознавания лиц. – М: Лаборатория Знаний, 2005.
6. Lowe D.J. Object recognition from local scale-invariant features. – Computer Science Department University of British Columbia, Vancouver, 1999.
7. Lowe D.J. Distinctive image features from scale-invariant key points. – Computer Science Department University of British Columbia, Vancouver, 2004.
8. Aichert A. Feature extraction techniques. – Camp medical seminar ws0708, 2008.
9. Mikolajczyk K., Tuytelaars T., Schmid C. et al. A comparison of affine region detectors. // International Journal of Computer Vision. – 2006. – № 4.
10. Nixon M.S, Aguado A. S. Feature extraction and image processing, Second edition. – Elsevier, 2008.
11. Naor M., Shamir A. Visual cryptography. // In EUROCRYPT'94. – Springer-Verlag Berlin, 1995. – Vol. LNCS 950. – Pp. 1-12.
12. Jin D., Yan W.Q., Kankanhalli M.S. Progressive color visual cryptography. // Journal of Electronic Imaging, 2005. – Vol. 14. – № 3.
13. Hou Y.C. Visual cryptography for color images. // Pattern Recognition. – 2003. – Vol. 173. – Pp. 1-11.
14. Zhou Z., Arce G.R., Di Crescenzo G. Halftone visual cryptography. // Proceedings of 2003 International Conference on Image Processing, 2003. – Vol. 1. – Pp. 521-524.
15. Liu F. and Wu C. Embedded extended visual cryptography schemes. – China, 2006.
16. Smith S.M., Brady J.M. SUSAN – a new approach to low level image processing. // International Journal of Computer Vision (IJCV), 1997. – Vol. 23. – № 1. – Pp. 45-78.
17. Lai S. Robust image matching under partial occlusion and spatially varying illumination change. // Computer Vision and Image Understanding. – 2000. – Vol. 78. – Pp. 84-98.
18. Tseng C.C. and Hwang T.M. Quantum digital image processing algorithms // 16th IPPR Conference on Computer Vision, Graphics and Image Processing (CVGIP 2003). – 2003. – Kinmen, ROC. – Pp. 827-834.
19. Mutze U. Quantum image dynamics – an entertainment application of separated quantum dynamics. – 2008. – [Электронный ресурс]. URL: available in http://www.ma.utexas.edu/mp_arc/c/08/08-199.pdf.

Приложение

Визуальная криптография Визуальная криптография (ВК) впервые была введена Мони Наором и Ади Шамиром в 1994 году [11]. Она используется для шифрования напечатанного текста или изображения. Основная идея модели визуальной криптографии состоит в разбиении исходного изображения на несколько шифрованных («теневых»), каждое из которых не дает никакой информации об исходном изображении кроме его размера (изображение-«белый шум»). При наложении шифрованных изображений друг на друга, можно получить исходное изображение. Таким образом, для декодирования не требуется специальных знаний или высокопроизводительных вычислений. В случае использования этого алгоритма в компьютерных системах, наложить все части изображения друг на друга можно используя логические операции *AND*, *OR*, *XOR* или установив нужную степень прозрачности в графическом редакторе. Кроме того, данная технология обладает высокой криптоустойчивостью за счет разделения случайным образом исходного изображения на множество шифроизображений.

Приложением таких технологий могут быть защита от копирования и проверка подлинности (*watermarking*), сокрытие информации для передачи по незащищенному каналу связи или для сохранения в БД, отслеживание электронных бланков при удаленном голосовании, шифрование финансовых документов, идентификация банковских клиентов, управление ключами (доступа, шифроключами) и совместное использование паролей.

Если визуальная криптография используется для безопасного общения, то отправитель передаст одно или более «теневые» изображения для каждого возможного (из небольшого набора) сообщения заблаговременно получателю. Если у отправителя есть сообщение, он остальные необходимые для дешифровки «теневые» изображения для конкретного отправленного сообщения и передает их получателю. Получатель соединяет все «теневые» изображения и получает секретную информацию. При этом всем, ему не требуется использовать устройства расшифровки, производить сложные математические расчеты, и даже не обязательно применять компьютер (если изображения находятся в печатном виде).

Классический алгоритм визуальной криптографии

Наор и Шамир продемонстрировали (k, n)-визуальную схему секретного обмена, где изображение было разбито на n частей, таким образом, что кто-либо, обладавший любыми k частями мог расшифровать его, в то время как любые k-1 частей не давали никакой информации о содержании исходного изображения. Когда все k частей будут наложены друг на друга, мы увидим исходное изображение.

Для того, чтобы разбить исходное черно-белое изображение на n частей, каждый пиксель изображения представляется в виде некоторого количества меньших частей (*subpixels*). Количество белых и черных частей всегда одинаковое. Если пиксель делится на две части, то получается один белый и один черный блок. Если пиксель делится на четыре равные части, то получаем два белых и два черных блока.

Рассмотрим (2, 2)-визуальную схему секретного обмена, т.е. исходная изображение разбивается на две части («тени»), каждая из которых представляет собой изображение белого шума, но при наложении дают исходное изображении. Каждый пиксель исходного изображения будем разбивать на четыре части, таким образом, если размер исходного изображения был $M \times N$, то размеры обеих «теней» будут $2M \times 2N$.

На рисунке ниже (рис. П1) показано, что пиксель, разделенный на четыре части, может иметь шесть разных состояний.

Если пиксель на первом слое имеет одно положение, пиксель на втором слое в свою очередь может иметь два положения: идентичное либо инвертированное пикселю первого слоя. Если пиксель части 2 идентичен пикселю части 1, то пиксель, полученный в результате наложения обеих «теней», будет наполовину белый и наполовину черный. Такой пиксель называют серым или пустым. Если

пиксели части 1 и части 2 противоположны, то пиксель, полученный в результате наложения, будет полностью черным. Он будет являться информационным.

Процесс получения «теневых» изображений для исходного изображения можно описать следующим образом: для каждого пикселя исходного изображения для первой «тени» *случайным образом* выбирается одно из шести возможных состояний пикселя, приведенных на рис. П1. Состояние пикселя второй «тени» выбирается идентичным или симметричным состоянию пикселя первой «тени» в зависимости от того, белый или черный это был пиксель в исходном изображении соответственно.

Аналогичным образом можно построить любую (*k*, *n*) визуальную схему секретного обмена.

Легко увидеть, что для некоторой заданной схемы визуальной криптографии (k, n), алгоритм шифрования изображения обладает следующими свойствами:

- регулярность (производятся одинаковые действия для каждого исходного пикселя);
- независимость (каждый исходный пиксель шифруется независимо от других);
- простота (производится случайный выбор матриц из совокупностей, заданных самой схемой разделения секрета).

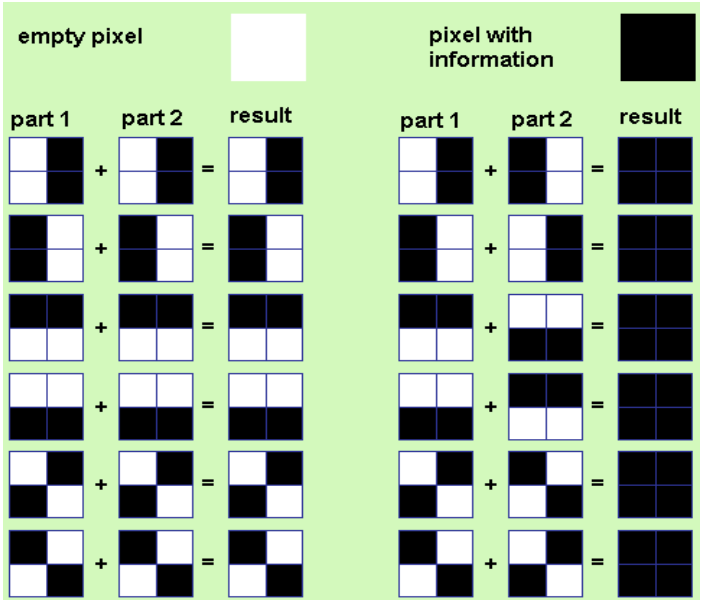

Рис. П1. Возможные состояния пикселя

Система является стойкой до тех пор, пока обе части изображения не попадут в чужие руки. Если же перехвачен только один слой, то расшифровка исходного изображения – невозможна.

Нельзя узнать используется ли пиксель второго слоя для создания серого или черного пикселя, пока не узнаем состояние этого пикселя на первом слое, чтобы узнать результат перекрытия. Если в процессе использования данной системы полностью соблюдается случайный подход к разбитию пикселей на блоки, то визуальная криптография предлагает абсолютную надежность и секретность.

С тех пор как классическая схема визуальной криптографии была изобретена, множество авторов предложили расширенные модели схемы, используемых, например, для кодирования полутоновых и цветных изображений [12-14], или схемы, где вместо «теневых» изображений в виде белого шума используются семантически значимые изображения [15], а также схемы визуальной стеганографии, базирующиеся на расширениях классической схемы визуальной криптографии. Множество расширений базовой модели схемы делает все более и более привлекательной с точки зрения ее приложения. В данной работе мы предлагаем расширение классической схемы визуальной криптографии в виде схемы квантовой визуальной криптографии [16, 17].