# АЛГОРИТМЫ ВСТРАИВАНИЯ ИНФОРМАЦИИ НА ОСНОВЕ QIM, СТОЙКИЕ К СТАТИСТИЧЕСКОЙ АТАКЕ

*В.А. Митекин [1,2], В.А. Федосеев [1,2]*

*[1] Самарский национальный исследовательский университет имени академика С.П. Королёва, Самара, Россия,*

*[2] Институт систем обработки изображений РАН – филиал ФНИЦ «Кристаллография и фотоника» РАН, Самара, Россия*

***Аннотация***

В работе предлагаются два новых алгоритма встраивания информации в мультимедиа, относящиеся к семейству алгоритмов на основе управляемого переквантования (Quantization Index Modulation, QIM). Предлагаемые алгоритмы спроектированы таким образом, чтобы обеспечить стойкость к статистической атаке, эффективной для других алгоритмов данного семейства и позволяющей восстановить секретный ключ встраивания, используя корреляционные связи между битами ключа и отсчётами носителя встроенной информации. В предлагаемых алгоритмах стойкость к данной атаке обеспечивается за счёт использования корреляционно-стойких функций встраивания информации, которые гарантируют статистическую независимость модифицируемых компонент контейнера и битов ключа. Будучи описанными на примере полутоновых изображений, новые алгоритмы могут использоваться для модификации любых мультимедийных данных в пространственно-временной и спектральной области. Результаты экспериментальных исследований подтвердили требуемую стойкость к статистической атаке и показали, что предложенные алгоритмы не вносят дополнительных искажений по сравнению с базовыми алгоритмами. Однако также эксперименты показали, что новые алгоритмы характеризуются несколько сниженной робастностью к аддитивному зашумлению и JPEG-сжатию.

*Ключевые слова:* цифровой водяной знак; переквантование; корреляционно-стойкая функция, статистическая атака; QIM.

*Цитирование:* **Митекин, В.А.** Алгоритмы встраивания информации на основе QIM, стойкие к статистической атаке / В.А. Митекин, В.А. Федосеев // Компьютерная оптика. – 2018. – Т. 42, № 1. – С. 118-127. – DOI: 10.18287/2412-6179-2018-42-1-118-127.

## *Введение*

В сетях распространения мультимедийной информации одной из актуальных задач является защита авторских прав на мультимедийную продукцию. Один из наиболее распространённых подходов решения данной задачи предполагает встраивание в защищаемый объект *цифровых водяных знаков* (ЦВЗ) – малозаметного шумоподобного сигнала, содержащего закодированную информацию об авторе или владельце [1]. При оценке практической применимости подобных алгоритмов ключевой характеристикой является количественное соотношение между объёмом шумовых искажений, вносимых при встраивании ЦВЗ, и стойкостью встроенного ЦВЗ к преднамеренным атакам и непреднамеренным искажениям мультимедиа. Таким образом, алгоритмы кодирования и методы встраивания водяного знака являются основными факторами, определяющими данное количественное соотношение в заданных условиях использования ЦВЗ (наличие и способы преднамеренных атак, возможность искажения и сжатия с потерями защищённого изображения и т.д.).

Одним из наиболее распространённых методов скрытого встраивания информации (в том числе ЦВЗ) в изображения является *метод управляемого переквантования*, нашедший своё отражение в семействе алгоритмов *Quantization Index Modulation* (QIM) [2]. Суть его заключается в том, что для встраивания различных битов информации используются различные шкалы переквантования исходных данных. При этом в качестве исходных данных могут выступать не только пиксели изображений или отсчёты звуковых и видеосигналов, но также и коэффициенты какого-либо спектрального преобразования исходного сигнала [3–10]. Важным практическим преимуществом данного метода является обеспечиваемое им высокое соотношение «степень искажения – стойкость ЦВЗ» в условиях, когда основным типом искажений защищённого изображения является аддитивный белый гауссовский шум [2]. На основе общего метода был разработан ряд конкретных алгоритмов [2–5], отличающихся выбором функций переквантования, объёмом встраивания, способом компенсации искажений и образующих единое семейство.

Наиболее распространённой реализацией метода QIM является алгоритм DM-QIM [2], основанный на использовании дополнительного параметра – *массива подмешиваемых значений* (*dither vector*), который используется в качестве секретного ключа, необходимого и для встраивания, и для извлечения ЦВЗ. Помимо этого, массив подмешиваемых значений также позволяет скрыть специфичные искажения гистограммы сигнала, являющиеся следствием переквантования, и тем самым позволяет защитить ЦВЗ от преднамеренного обнаружения атакующим, не знающим ключа встраивания.

Несмотря на широкое использование алгоритмов семейства QIM, известны примеры атак, позволяющих обнаружить и/или извлечь встроенную информацию без знания секретного ключа. Так, в работах [11–13] были предложены методы, позволяющие по одному изображению с ЦВЗ с вероятностью не ниже

0,9 обнаружить и извлечь встроенный ЦВЗ без знания ключа. Кроме того, в работе [14] предложен другой подход, который по множеству изображений, содержащих информацию, встроенную при помощи одного и того же ключа, позволяет не только обнаружить встроенную информацию, но и восстановить секретный ключ системы. В настоящей работе предлагаются два новых алгоритма семейства QIM, названные IM-QIM (*statistically IMmune QIM*) и SIM-QIM (*Sliding statistically IMmune QIM*), позволяющие защититься от данной атаки.

Работа организована следующим образом. Параграф 1 содержит описание двух реализаций QIM – упрощённой Simple QIM и вышеупомянутой DM-QIM, а также статистической атаки на эти алгоритмы, предложенной в работе [14]. Параграф 2 посвящён анализу причин применимости данной атаки и поиску решения, направленного на снижение её эффективности. В 3-м параграфе приводится описание двух новых алгоритмов, реализующих найденное решение, а 4-й параграф посвящён экспериментальным исследованиям предложенных алгоритмов. Работу завершают заключение и благодарности.

## *1. Базовые алгоритмы семейства QIM и статистическая атака на них*

### *1.1. Базовый метод QIM и простейшая его реализация*

Как отмечалось выше, метод QIM применим для защиты не только изображений, но и видео, а также звуковых сигналов. Однако для определённости будем рассматривать все алгоритмы в данной статье на примере модификации отдельных пикселей полутонового изображения.

Итак, пусть $I(n,m)$ – исходное полутоновое изображение-контейнер, принимающее значения в диапазоне $[0, 255]$, $n\in[1,N]$, $m\in[1,M]$. Пусть $W(k)$ – двоичная последовательность, выступающая в качестве встраиваемого ЦВЗ, где $k\in[1,N\cdot M]$. Основными параметрами алгоритма являются:

– шаг переквантования $\Delta\in\mathbb{N}$, который определяет одновременно устойчивость встроенного ЦВЗ к аддитивному белому шуму и среднюю амплитуду так называемого «шума квантования» (искажений, вносимых при встраивании ЦВЗ);

– шкала переквантования, используемая для встраивания информации и задаваемая в виде функции $Q(x,\Delta)$, где $x$ – квантуемое значение яркости. Простейшая шкала переквантования, которая повсеместно будет использоваться в данной работе, имеет вид:

$$Q(x,\Delta)=\Delta\cdot\mathrm{round}\left(\frac{x}{\Delta}\right), \tag{1}$$

где $\mathrm{round}(\cdot)$ – операция округления до ближайшего целого.

Для начала рассмотрим алгоритм, который для определённости назовём Simple QIM, являющийся упрощённой реализацией метода QIM. Он почти не используется на практике, но полезен для пояснения самого базового метода. В данном алгоритме формирование *носителя встроенной информации* – изображения $I^W(n,m)$ – осуществляется по формуле

$$\begin{aligned} I^W(n,m) &= \mathrm{E}_{QIM}\left(I,W,\Delta\right)= \\ &= Q\left(I(n,m),\Delta\right)+\frac{\Delta}{2}W\left(k\right), \end{aligned} \tag{2}$$

где $k$ и $(n,m)$ связаны между собой каким-либо биективным отображением, например: $k=nM+m$.

Таким образом, в результате встраивания информации $I^W(n,m)$ содержит значения, кратные $\Delta/2$, как показано на рис. 1.

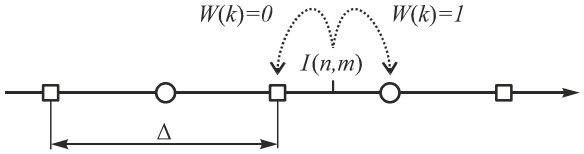


*Рис. 1. Иллюстрация встраивания информации алгоритмом Simple QIM*

Для извлечения информации воспользуемся не самым удобным, но наиболее универсальным способом, который применяется и для других алгоритмов семейства. Пусть $\widetilde{I^W}(n,m)$ – изображение, поступившее на принимающую сторону. В общем случае оно не совпадает с $I^W(n,m)$, поскольку в процессе передачи могло быть подвергнуто каким-либо искажениям или атакам. Тогда извлечение информации происходит по формулам:

$$\widetilde{I}_0(n,m)=\mathrm{E}_{QIM}\left(\widetilde{I^W},0,\Delta\right)=Q\left(\widetilde{I^W}(n,m),\Delta\right), \tag{3}$$

$$\widetilde{I}_1(n,m)=\mathrm{E}_{QIM}\left(\widetilde{I^W},1,\Delta\right)=Q\left(\widetilde{I^W}(n,m),\Delta\right)+\frac{\Delta}{2}, \tag{4}$$

$$\widetilde{W}\left(k\right)=\arg\min_{p\in\{0,1\}}\left|\widetilde{I^W}(n,m)-\widetilde{I}_p(n,m)\right|. \tag{5}$$

Иными словам, при извлечении ЦВЗ осуществляется подстановка битов 0 и 1 в формулу (2), причём в качестве контейнера используется $\widetilde{I^W}(n,m)$, а далее оцениваются отклонения полученных результатов.

Ввиду существенного сужения множества возможных значений пикселей, результат применения алгоритма Simple QIM легко обнаруживается по гистограмме изображения [15], поэтому на практике чаще применяются другие алгоритмы, среди которых наиболее популярным является DM-QIM.

### *1.2. Алгоритм DM-QIM*

Алгоритм DM-QIM (*Dither Modulation – QIM*) предполагает использование двух дополнительных параметров – массивов подмешиваемых значений (*dither vectors*), согласованных друг с другом и используемых при встраивании битов «0» и «1»:

$$d_0(k),\ d_1(k)\in\left[-\Delta/2;\Delta/2-1\right],\ k\in\left[1,N\cdot M\right].$$

Пусть $d(k)$ – массив псевдослучайных целых чисел, равномерно распределённых на отрезке $[-\Delta/2;\Delta/2-1]$, который генерируется на основе секретного ключа. Определим $d_0(k)$ и $d_1(k)$ как

$$d_0(k) = d(k),$$
$$d_1(k) = d_0(k) - \operatorname{sign}(d_0(k)) \cdot \Delta/2 . \quad (6)$$

Формула встраивания информации будет иметь вид

$$I^W(n,m) = \mathrm{E}_{DM-QIM}\left(I, W, d, \Delta\right) = Q(I(n,m) + d_{W(k)}(k), \Delta) - d_{W(k)}(k), \quad (7)$$

то есть к значению яркости очередного пикселя перед переквантованием подмешивается соответствующее значение одного из массивов $d_0(k)$ или $d_1(k)$, соответствующее встраиваемому биту и его позиции в векторе. Вычитание шумоподобной добавки из переквантованных значений позволяет затруднить обнаружение встраивания DM-QIM по гистограмме результирующего изображения.

Извлечение информации происходит по формуле (5), где $\widetilde{I}_p(n,m)$, $p = \{0,1\}$ формируются согласно изменённой формуле встраивания:

$$\widetilde{I}_0(n,m) = \mathrm{E}_{DM-QIM}\left(\widetilde{I^W}, 0, d, \Delta\right) = Q\left(\widetilde{I^W}(n,m) + d_0(k), \Delta\right) - d_0(k), \quad (8)$$

$$\widetilde{I}_1(n,m) = \mathrm{E}_{DM-QIM}\left(\widetilde{I^W}, 1, d, \Delta\right) = Q\left(\widetilde{I^W}(n,m) + d_1(k), \Delta\right) - d_1(k). \quad (9)$$

### *1.3. Статистическая атака на DM-QIM*

Принцип атаки на алгоритм DM-QIM, предложенной в работе [14] и применимой также для других реализаций QIM [2–7], основан на том, что смещение яркости пикселей результирующего изображения относительно переквантованных значений определяется только значением $d_0(k)$ или зависящим от него $d_1(k)$. Таким образом, если атака позволяет восстановить шаг квантования, а также смещения яркости пикселей $d_0(k)$ и $d_1(k)$, то это позволит не только обнаружить факт встраивания, но и с точностью до одного бита (согласно формуле (6)) восстановить ключевую последовательность $d_0(k)$.

Предложенный в работе [14] метод атаки на алгоритм DM-QIM использует набор из $T$ изображений $I_t^W(n,m)$, $t \in [1,T]$, в которые произведено встраивание информации при помощи одного ключа (встраиваемые последовательности при этом могут различаться). Далее, если взять какой-либо пиксель $(n,m)$ и построить гистограмму его значений на всём наборе из $T$ изображений, то подобная гистограмма будет иметь хорошо различимые пики, повторяющиеся с периодом $\Delta/2$. Для иллюстрации на рис. 2 показан пример такой гистограммы и для сравнения пример аналогичной гистограммы, полученной по исходным контейнерам.

На основе анализа гистограммы восстанавливается как значение $\Delta$, так и смещение в данном пикселе, по которому при наличии хотя бы одного изображения $I_t^W(n,m)$ с известной встроенной последовательностью $W_t(k)$ однозначно восстанавливаются $d_0(k)$ и $d_1(k)$, что позволяет полностью взломать систему встраивания скрытой информации и извлечь информацию из всех изображений-носителей, использующих тот же секретный ключ.

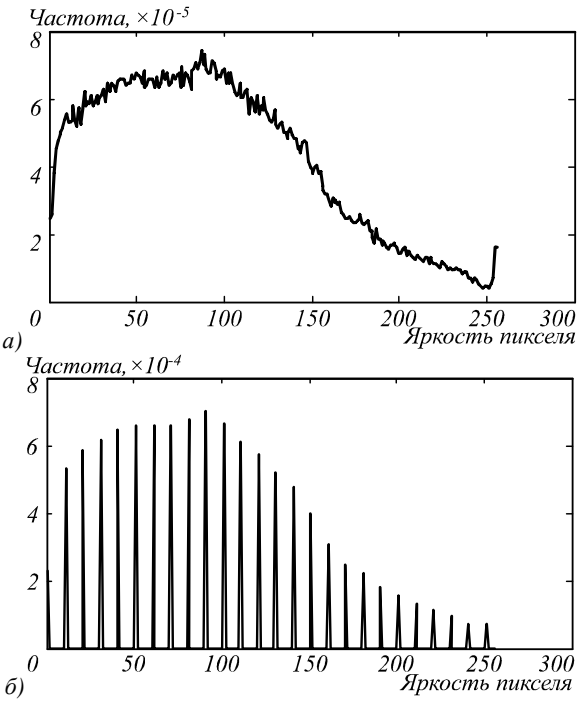


*Рис. 2. Гистограмма значений одного пикселя на множестве изображений: исходные контейнеры (а); результаты встраивания алгоритмом DM-QIM (б)*

## *2. Поиск решений для противодействия статистической атаке*

### *2.1. Причины уязвимости DM-QIM и подходы к их устранению*

Источником уязвимости DM-QIM является тот факт, что в результате встраивания информации по формуле (7) неизбежно возникает корреляционная зависимость между яркостью отдельного пикселя изображения $I^W(n,m)$ (точнее, остатком от деления $I^W(n,m)$ на $\Delta$) и отдельным битом ключа $d_{W(k)}(k)$. Атакующий в подобной ситуации может без какой-либо информации о значении ключа сформировать выборку пикселей таким образом, чтобы по их статистическим характеристикам оценить неизвестный ему фрагмент ключа.

Можно предположить существование как минимум двух способов защиты от подобного типа атаки.

Во-первых, атаки можно избежать, используя различные значения ключа для каждого нового изображения-контейнера. Данный подход рассмотрен в ряде работ, где предложены либо способы генерации ключа на основе статистических характеристик изображения-контейнера, либо способы встраивания информации об используемом ключе в само изображение-контейнер. Как показано в [16, 17], в случае использования данного подхода возникает опасность применения атакующим более узкоспециализирован-

ных атак, основанных на так называемой «десинхронизации» ключа, то есть невозможности восстановления исходного ключа из носителя встроенной информации.

Во-вторых, при встраивании ЦВЗ возможно использовать более сложные функции встраивания, для которых корреляционная зависимость между отдельным битом ключа и отдельным пикселем (отсчётом) изображения-контейнера не возникает в результате встраивания ЦВЗ даже с использованием одного и того же ключа. Такими функциями являются так называемые *корреляционно-стойкие функции* (*correlation-immune functions*) [18], широко используемые в системах поточного шифрования.

### *2.2. Корреляционно-стойкие функции для отсчётов полутонового изображения*

Функция $F(X_1, X_2, ..., X_q)$ называется *корреляционно-стойкой функцией* $j$-го порядка, если для любых $u_1, u_2 ... u_j$, выбранных из диапазона $[1, q]$, случайная переменная $Z = F(X_1, X_2, ..., X_q)$ и случайный вектор $(X_{u_1}, X_{u_2}, ..., X_{u_j})$ являются статистически независимыми.

Наиболее известным на практике примером подобной функции является функция сложения по модулю 2 (функция XOR)

$$F_{XOR}(X_1, X_2, ..., X_q) = X_1 \oplus X_2 \oplus ... \oplus X_q,$$

где $X_1, X_2, ..., X_q \in \{0, 1\}$. Действительно, несложно показать, что данная функция является корреляционно-стойкой функцией порядка $q-1$, т.к.

$$P\left(F_{XOR}(X_1, X_2, ..., X_q) = z \mid X_1 = g_1, ..., X_{q-1} = g_{q-1}\right) = \\ = P\left(F_{XOR}(X_1, X_2, ..., X_q) = z\right)$$

для любых $z, g_1, g_2, ..., g_{q-1}$.

Фактически, данная функция не позволяет атакующему использовать априорную информацию об известных ему $(X_1, X_2, ..., X_{q-1})$ для построения прогноза о значении $z = F_{XOR}(X_1, X_2, ..., X_q)$ с достоверностью выше $1/2$.

Рассмотрим теперь следующую функцию – функцию сложения по модулю Δ:

$$F_{IM}(I(n_1, m_1), I(n_2, m_2), ..., I(n_q, m_q)) = \\ = \mathrm{M}\left(I(n_1, m_1) + I(n_2, m_2) + ... + I(n_q, m_q), \Delta\right), \quad (10)$$

где $\{I(n_1, m_1), I(n_2, m_2) \ldots I(n_q, m_q)\}$ – некая секретным образом выбранная группа пикселей изображения $I$, а

$$\mathrm{M}(x, \Delta) = x \left(\mathrm{mod}\, \Delta\right). \quad (11)$$

Покажем, что данная функция является корреляционно-стойкой функцией порядка $q-1$ при условии, что значения $\mathrm{M}(I(n_q, m_q), \Delta)$ являются независимыми равномерно распределёнными в диапазоне $[-\Delta/2, \Delta/2)$ случайными величинами. Действительно, если атакующему известны все значения $I(n_1, m_1), I(n_2, m_2), ..., I(n_{q-1}, m_{q-1})$ и, как следствие, значение $F_{IM}(I(n_1, m_1), I(n_2, m_2), ..., I(n_{q-1}, m_{q-1}))$, то величина $F_{IM}(I(n_1, m_1), I(n_2, m_2), ..., I(n_q, m_q))$, с точки зрения атакующего, будет также являться равномерно распределённой случайной величиной.

Пусть Δ является делителем 256 (напомним, что $I(n, m)$ принимает значения в диапазоне $[0, 255]$). Тогда для любого $x \in [0, \Delta-1]$ и для любого $y = F_{IM}(I(n_1, m_1), I(n_2, m_2), ..., I(n_{q-1}, m_{q-1})) \in [0, \Delta-1]$ будут существовать $256/\Delta$ значений $I(n_q, m_q)$, при которых $F_{IM}(I(n_1, m_1), I(n_2, m_2), ..., I(n_q, m_q)) = x$. Следовательно, для атакующего величины $F_{IM}(I(n_1, m_1), I(n_2, m_2), ..., I(n_q, m_q))$ и $F_{IM}(I(n_1, m_1), I(n_2, m_2), ..., I(n_{q-1}, m_{q-1}))$ являются статистически независимыми. Аналогично можно показать, что статистически независимыми являются $F_{IM}(I(n_1, m_1), I(n_2, m_2), ..., I(n_q, m_q))$ и любой вектор $I(n_{u_1}, m_{u_1}), I(n_{u_2}, m_{u_2}), ..., I(n_{u_{q-1}}, m_{u_{q-1}})$, где $u_1, u_2, ..., u_{q-1} \in [1, q]$. Отметим также, что если 256 не делится на Δ, то число различных значений $I(n_q, m_q)$ для некоторых сочетаний $x$ и $y$ будет равно $\lfloor 256/\Delta \rfloor + 1$, однако при малых Δ разница в единицу не будет являться определяющей.

В следующем подпараграфе показано, как именно полученные функции (10)–(11) могут быть использованы для построения алгоритмов встраивания информации, защищённых от рассмотренной ранее статистической атаки.

### *2.3. Использование корреляционно-стойкой функции для встраивания информации*

Возвращаясь к соотношениям (8)–(9), (5), можно увидеть, что рассмотренное значение извлечённого бита $\widetilde{W}(k) = \arg\min_{p \in \{0,1\}} \left| \widetilde{I^W}(n, m) - \widetilde{I}_p(n, m) \right|$ коррелировано именно с величиной $\mathrm{M}(\widetilde{I^W}(n, m), \Delta)$, т.е. с остатком от деления $\widetilde{I^W}(n, m)$ на Δ, а не с самим значением яркости $\widetilde{I^W}(n, m)$. Действительно, если в выражениях (8)–(9) заменить конкретное значение $\widetilde{I^W}(n, m)$ на $\left(\widetilde{I^W}(n, m) + \Delta\right)$, то результат вычисления (5) извлечённого бита при этом не изменится при любых допустимых значениях $\widetilde{I^W}(n, m)$. Именно эта корреляционная связь и используется для проведения статистической атаки [14].

Идея предлагаемых алгоритмов заключается в том, чтобы заменить исходную функцию переквантования яркости отдельного пикселя $Q(I(n, m), \Delta)$ (1) в выражениях (8) и (9) на функцию переквантования суммы яркостей сразу нескольких пикселей $I(n_1, m_1) + I(n_2, m_2) + ... + I(n_q, m_q)$. Тогда, согласно (7)–(9), (5), значение встроенного бита ЦВЗ будет коррелированным уже не с яркостью отдельных пикселей изображения-контейнера, а с функцией $\mathrm{M}(I(n_1, m_1) + I(n_2, m_2) + ... + I(n_q, m_q), \Delta)$. В то же время корреляционной зависимости между битом ЦВЗ и яркостью отдельных пикселей $I(n_1, m_1), I(n_2, m_2), ..., I(n_q, m_q)$ наблюдаться не будет ввиду доказанной выше корреляционной стойкости функции $\mathrm{M}(x, \Delta)$. Таким образом, атака [14] становится реализуемой лишь в случае, когда атакующему известно точное разбиение

пикселей изображения на группы для суммирования с последующим переквантованием.

Также отдельно отметим рассмотренное ранее требование к значениям $\mathrm{M}(I(n_q, m_q), \Delta)$, необходимое для обеспечения корреляционной стойкости выбранной функции встраивания. Для выполнения этого требования в предлагаемых алгоритмах должно применяться аддитивное зашумление всех пикселей изображения равномерно распределённым белым шумом.

### *3. Описание разработанных алгоритмов*

В результате для противодействия статистической атаке [14] было разработано два алгоритма, получивших названия IM-QIM (*statistically IMmune QIM*) и SIM-QIM (*Sliding statistically IMmune QIM*), причём второй является развитием первого.

Для начала представим область определения изображения – носителя информации $\mathrm{D}=\{(n,m)\}_{n=1..N,\, m=1..M}$ как объединение двух подмножеств пикселей:

– множества $D_{emb}$, каждый пиксель которого будет содержать бит встроенной информации,

– множества оставшихся пикселей $D_{rest} = D \backslash D_{emb}$, не предназначенных для встраивания информации.

В алгоритмах Simple QIM и DM-QIM для встраивания информации используется всё множество пикселей, то есть $D_{rest} = \varnothing$. Оба предлагаемых алгоритма отличаются тем, что для них это множество не пусто.

#### *3.1. Алгоритм IM-QIM*

Принципиальным отличием алгоритма IM-QIM от исходного DM-QIM является способ использования секретного ключа – в предлагаемом алгоритме ключ используется для разбиения множества пикселей изображения на группы, к которым в дальнейшем применяется операция переквантования. Алгоритм IM-QIM использует также массивы $d_0^g(k)$, $d_1^g(k)$, $g = 2..G$ (об индексации речь пойдёт ниже) – аналоги массивов $d_0(k)$ и $d_1(k)$ в DM-QIM, но в алгоритме IM-QIM данные массивы не используются при извлечении ЦВЗ. Это означает, что массивы $d_0^g(k)$, $d_1^g(k)$ могут генерироваться уникальным образом для каждого нового изображения и проблемы синхронизации ключа, в отличие от алгоритма DM-QIM, в данном случае не возникает.

Разделим область определения $D$ на $G$ равных непересекающихся частей (групп пикселей) $D_1, D_2, ..., D_G$, объединение которых равно всему множеству $D$, причём $D_{emb} = D_1$, а $D_{rest} = D \backslash D_1$. Это разбиение определяется секретным ключом и неизвестно атакующему. Далее пронумеруем пиксели, входящие в каждое из множеств $D_1, D_2, ..., D_G$: $(n_1^g, m_1^g)$, $(n_2^g, m_2^g)$, ..., $(n_{NM/G}^g, m_{NM/G}^g)$, где $g = 1..G$ – индекс, определяющий подмножество.

Тогда изменение пикселей множества $D_1$ будет осуществляться по формуле:

$$\begin{aligned} I^W\left(n_k^1, m_k^1\right) &= \mathrm{E}_{IM-QIM}\left(I, W, d, \Delta\right) = \\ &= Q\left(I\left(n_k^1, m_k^1\right) + d_{W(k)}^1(k), \Delta\right) - d_{W(k)}^1(k), \end{aligned} \tag{12}$$

где

$$d_0^1(k) = \sum_{g=2}^{G}\left(I\left(n_k^g, m_k^g\right) + d_0^g(k)\right), \tag{13}$$

$$d_1^1(k) = d_0^1(k) - \mathrm{sign}\left(d_0^1(k)\right)\cdot\Delta/2\ , \tag{14}$$

а массивы $d_0^g(k)$, $g = 2..G$ генерируются на основе ключа для каждого подмножества $D_g$ аналогично алгоритму DM-QIM.

Пиксели изображения, не относящиеся к $D_1$, будут лишь аддитивно зашумляться в соответствии со значениями массива $d_0^g(k)$:

$$I^W\left(n_k^g, m_k^g\right) = I\left(n_k^g, m_k^g\right) + d_0^g(k),\ \ g = 2..G. \tag{15}$$

Данная операция не реализует встраивание ЦВЗ, но призвана обеспечить выполнение условий, при которых функция (11) является доказанно корреляционно стойкой.

Для извлечения информации по принятому носителю встроенной информации рассчитываются оценки массивов подмешиваемых значений

$$\widetilde{d}_0^1(k) = \sum_{g=2}^{G}\widetilde{I^W}\left(n_k^g, m_k^g\right), \tag{16}$$

$$\widetilde{d}_1^1(k) = \widetilde{d}_0^1(k) - \mathrm{sign}\left(\widetilde{d}_0^1(k)\right)\cdot\Delta/2\ , \tag{17}$$

после чего извлечение происходит по традиционной схеме, аналогичной (3) – (5) и (8) – (9):

$$\begin{aligned} \widetilde{I}_0\left(n_k^1, m_k^1\right) &= \mathrm{E}_{IM-QIM}\left(\widetilde{I^W}, 0, \tilde{d}, \Delta\right) = \\ &= Q\left(\widetilde{I^W}\left(n_k^1, m_k^1\right) + \widetilde{d}_0^1(k), \Delta\right) - \widetilde{d}_0^1(k), \end{aligned} \tag{18}$$

$$\begin{aligned} \widetilde{I}_1\left(n_k^1, m_k^1\right) &= \mathrm{E}_{IM-QIM}\left(\widetilde{I^W}, 1, \tilde{d}, \Delta\right) = \\ &= Q\left(\widetilde{I^W}\left(n_k^1, m_k^1\right) + \widetilde{d}_1^1(k), \Delta\right) - \widetilde{d}_1^1(k), \end{aligned} \tag{19}$$

$$\widetilde{W}(k) = \arg\min_{p\in\{0,1\}}\left|\widetilde{I^W}\left(n_k^1, m_k^1\right) - \widetilde{I}_p\left(n_k^1, m_k^1\right)\right|. \tag{20}$$

#### *3.2. Алгоритм SIM-QIM*

Если сравнить множества $D_{emb}$ и $D_{rest}$ для IM-QIM

$$D_{emb}^{IM-QIM} = D_1,\ D_{rest}^{IM-QIM} = \bigcup_{g=2}^{G} D_g$$

с аналогичными множествами для базовых алгоритмов:

$$D_{emb}^{QIM} = D_{emb}^{DM-QIM} = D,\ D_{rest}^{QIM} = D_{rest}^{DM-QIM} = \varnothing,$$

то становится очевидным, что IM-QIM обладает меньшей ёмкостью контейнера: вместо

$$C_{N,M}^{QIM} = C_{N,M}^{DM-QIM} = NM \tag{21}$$

бит информации он позволяет встроить лишь

$$C_{N,M}^{IM-QIM} = NM/G \tag{22}$$

бит в контейнер размерами $N \times M$.

Идея алгоритма SIM-QIM (*Sliding statistically IMmune QIM*) заключается в том, чтобы модифицировать алгоритм IM-QIM, используя результаты встраивания информации в пиксели одних групп в качестве

аргументов корреляционно-стойкой функции (10) при встраивании данных в другие группы (по принципу «скользящего окна» – *sliding window*), и за счёт этого увеличить ёмкость контейнера.

Пусть $S \geq 2$ – количество слагаемых, используемых в корреляционно-стойкой функции для данного алгоритма. Тогда $S-1$ – число групп пикселей, которые не несут скрытую информацию. В отличие от IM-QIM, для SIM-QIM пусть $D_{rest}^{SIM-QIM}$ содержит группы с меньшими индексами:

$$D_{emb}^{SIM-QIM} = \bigcup_{g=S}^{G} D_g \ , \ D_{rest}^{SIM-QIM} = \bigcup_{g=1}^{S-1} D_g \ . \qquad (23)$$

Модификация пикселей из $D_{rest}^{SIM-QIM}$ осуществляется аналогично формуле (15):

$$I^W\left(n_k^g, m_k^g\right) = I\left(n_k^g, m_k^g\right) + d_0^g(k), \ \ g = 1..S-1. \qquad (24)$$

Что касается оставшихся отсчётов, то при суммировании в формуле (13) используются $S$ ближайших групп с меньшими индексами. При этом формулы (12) – (14) принимают следующий вид:

$$\begin{aligned} I^W\left(n_k^g, m_k^g\right) &= \mathrm{E}_{SIM-QIM}\left(I, W, d, \Delta, g\right) = \\ &= Q\left(I\left(n_k^g, m_k^g\right) + d_{W(k)}^g(k), \Delta\right) - d_{W(k)}^g(k), \ \ g = S..G, \end{aligned} \qquad (25)$$

$$d_0^g(k) = \sum_{i=g-S+2}^{g-1} \left(I\left(n_k^i, m_k^i\right) + d_{W(k)}^i(k)\right), \qquad (26)$$

$$d_1^g(k) = d_0^g(k) - \mathrm{sign}\left(d_0^g(k)\right) \cdot \Delta/2 \ . \qquad (27)$$

В результате согласно (24) – (27) ёмкость контейнера в битах увеличивается до

$$C_{N,M}^{SIM-QIM} = NM\left(G-S+1\right)/G \ . \qquad (28)$$

Таким образом, при увеличении числа групп $G$ ёмкость контейнера стремится к $NM$.

### *4. Экспериментальные исследования*

В рамках работы были проведены исследования разработанных алгоритмов, имевшие целью проверку их работоспособности (стойкости к атаке [14]), а также оценку уровня вносимых искажений и изучение влияния искажений носителя информации на точность её извлечения.

#### *4.1. Исследование возможности проведения статистической атаки*

Для исследования применимости атаки [14] для разработанных алгоритмов были использованы изображения из набора BOWS-2 [19]. В каждое изображение встраивался ЦВЗ алгоритмами Simple QIM, DM-QIM, IM-QIM, SIM-QIM. Значение параметра встраивания $\Delta$ при этом было одинаково для всех изображений и равнялось 10. Далее для указанного набора была воспроизведена исходная атака [14], основанная на построении гистограммы для значений яркости всех пикселей с заданными координатами.

На рис. 3 показаны фрагменты подобной гистограммы для выборки из 200000 пикселей, построенной до и после встраивания (при этом для встраивания информации во все пиксели использовался один и тот же ключ). На первой-второй гистограммах, соответствующих алгоритмам встраивания Simple QIM и DM-QIM, чётко просматриваются пики, следующие с частотой $\Delta/2$ и $\Delta$ соответственно. Как уже было отмечено ранее, это связано с наличием корреляционной связи между битом ЦВЗ (0 или 1) и величиной $\mathrm{M}(\widetilde{I^W}(n,m),\Delta)$.

Иными словами, сам факт встраивания ЦВЗ алгоритмами DM-QIM или Simple QIM формирует множество «предпочитаемых» значений яркости таким образом, что для всех значений в нём величина $\mathrm{M}(\widetilde{I^W}(n,m),\Delta)$ будет равна заданной константе (причём эта величина однозначно определяется величинами $\Delta$, $d_0(k)$ и $d_1(k)$, как было показано в [14]). В то же время на третьей-четвёртой гистограммах такой картины не наблюдается, т.е. корреляционная связь между яркостью отдельного пикселя и битом ЦВЗ не прослеживается. Таким образом, можно констатировать стойкость новых алгоритмов к статистической атаке в данном эксперименте.

#### *4.2. Исследование искажений, вносимых при встраивании информации*

В ходе исследований также анализировалось, как влияют изменённые процедуры встраивания информации на качество результирующих изображений при различных значениях параметра $\Delta$ в сравнении с базовыми методами. В качестве показателя качества использовалось среднеквадратичное отклонение (MSE) носителя информации от контейнера. Теоретически значение MSE для новых алгоритмов не должно отличаться от значений для Simple QIM и DM-QIM и согласно закону нормального распределения должно быть близким к $\Delta^2/12$. Для проверки был проведён эксперимент на множестве из 50 изображений тестового набора [19]. Для новых алгоритмов использовались значения $G \in \{2,4,8\}$.

Результаты эксперимента отражены в табл. 1. Помимо усреднённых значений MSE для всех алгоритмов, в таблице также отражены наибольшее и наименьшее значения MSE для алгоритма Simple QIM. Результаты показывают, что искажения, индуцируемые новыми алгоритмами, не превышают искажения от базовых методов и близки к $\Delta^2/12 + 1/6$.

#### *4.3. Исследование стойкости ЦВЗ при искажениях носителя информации*

В рамках работы были также проведены эксперименты по исследованию точности извлечения встроенной информации при искажениях её носителя. В качестве искажений рассматривались наложение аддитивного белого гауссовского шума (АБГШ), традиционно рассматриваемое при анализе алгоритмов семейства QIM [2], и сжатие в формате JPEG. В экспериментах использовались значения $G \in \{2,4,8\}$, $\Delta = 10$ и то же множество 50 изображений из набора [19]. В качестве показателя стойкости бралась точность извлечения информации *Acc*, определяемая как доля правильно извлечённых бит ЦВЗ и равная $Acc = 1 - BER$, где BER (*Bit Error Rate*) – известная характеристика ЦВЗ-систем, определяемая как доля ошибок извлечения. Результаты исследований отражены на рис. 4-5.

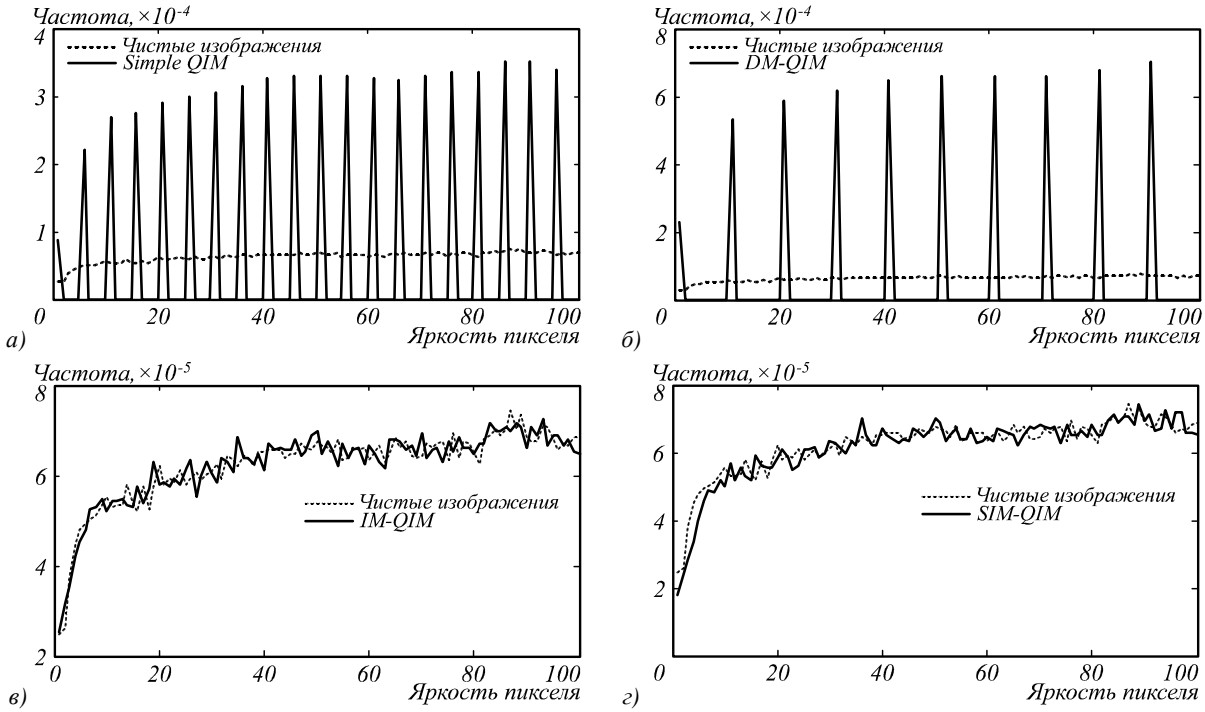


*Рис. 3. Результаты статистической атаки на алгоритмы Simple QIM (а), DM-QIM (б), IM-QIM (в), SIM-QIM (г) (фрагменты гистограмм)*

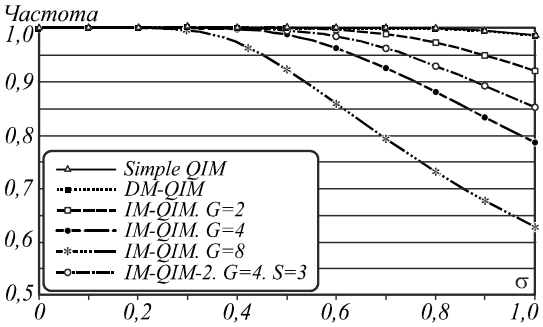


*Рис. 4. Влияние АБГШ на точность извлечения информации для разных алгоритмов*

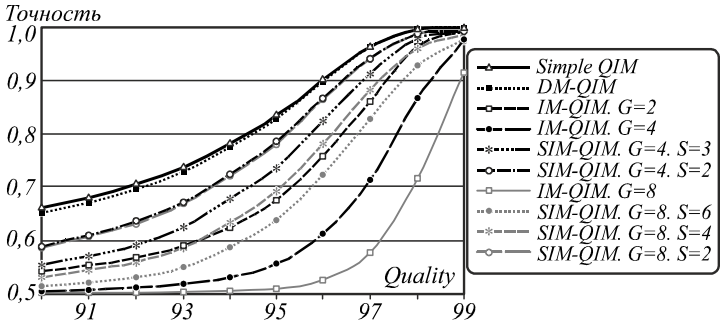


*Рис. 5. Влияние JPEG-сжатия с параметром Quality на точность извлечения информации для разных алгоритмов*

*Табл. 1. Средний уровень искажений носителя информации (MSE) для разных алгоритмов в зависимости от Δ*

| Δ | 4 | 8 | 12 |
|---|---|---|---|
| $\Delta^2/12$ | 1,333 | 5,333 | 12 |
| Simple QIM | 1,499 | 5,486 | 12,131 |
| DM-QIM | 1,499 | 5,5 | 12,17 |
| Simple QIM (мин.) | 1,463 | 5,417 | 11,808 |
| Simple QIM (макс.) | 1,524 | 5,542 | 12,238 |
| IM-QIM. $G=2$ | 1,499 | 5,5 | 12,162 |
| IM-QIM. $G=4$ | 1,5 | 5,498 | 12,167 |
| SIM-QIM. $G=4$. $S=3$ | 1,499 | 5,501 | 12,165 |
| SIM-QIM. $G=4$. $S=2$ | 1,5 | 5,501 | 12,165 |
| IM-QIM. $G=8$ | 1,5 | 5,497 | 12,165 |
| SIM-QIM. $G=8$. $S=6$ | 1,5 | 5,499 | 12,165 |
| SIM-QIM. $G=8$. $S=4$ | 1,5 | 5,499 | 12,173 |
| SIM-QIM. $G=8$. $S=2$ | 1,499 | 5,502 | 12,165 |

Как и ожидалось, предложенные алгоритмы уступают по стойкости к АБГШ и JPEG-сжатию известным алгоритмам, что является обратной стороной защищённости к статистической атаке [14]. Если сравнивать кривые при разных параметрах алгоритмов, можно сделать вывод о том, что стойкость повышается при снижении числа суммируемых отсчётов, равного $G$ для алгоритма IM-QIM (согласно (12)–(13)) и равного $S$ для алгоритма SIM-QIM (согласно (25)–(26)). Также можно отметить несколько большую стойкость к JPEG-сжатию алгоритма SIM-QIM в сравнении с IM-QIM при равном числе суммируемых отсчётов.

### *Заключение*

В работе предложены новые алгоритмы встраивания ЦВЗ, относящиеся к семейству QIM. Основным их преимуществом является их доказуемая стойкость к классу атак, основанных на выявлении статистической зависимости между яркостью пикселя и отдельным битом ЦВЗ. Данное свойство достигнуто за счёт использования корреляционно-стойкой функции сложения целых чисел по модулю. В итоге обнару-

жение корреляционной связи между битом ЦВЗ и отдельными пикселями изображения возможно только в случае точного «угадывания» атакующим всей группы пикселей, используемой при встраивании (то есть координат этих пикселей на изображении). Исходя из этого, при использовании значения $G=4$ в алгоритме IM-QIM или соответствующего ему $S=4$ в алгоритме SIM-QIM число попыток, необходимых для нахождения каких-либо 4 пикселей, входящих в одну группу, может быть оценено как

$$\frac{C_{N\times M}^{4}}{(N\times M)/4}=\frac{4(N\times M-1)!}{4!(N\times M-4)!}.$$

Данное соотношение означает, что, например, для изображения размером 1000×1000 пикселей атакующий вынужден будет проанализировать гистограммы примерно $1\cdot10^{17}$ возможных групп пикселей, прежде чем найдёт группу, необходимую для вычисления бита ЦВЗ. При увеличении числа пикселей в группе $G$, очевидно, будет наблюдаться близкий к экспоненциальному рост сложности подобной атаки.

Проведённые экспериментальные исследования показали, что предлагаемые алгоритмы обладают следующими свойствами:

– обеспечивают такой же уровень искажения контейнера (MSE), как и базовые алгоритмы;

– обеспечивают меньшую в сравнении с QIM информационную емкость контейнера: в $G$ раз для IM-QIM и в $G/(G-S+1)$ раз для SIM-QIM;

– проигрывает базовым методам по стойкости к АГБШ и JPEG-сжатию.

Таким образом, можно утверждать, что за счёт незначительного снижения ключевых показателей эффективности алгоритма встраивания (объёма встраиваемой информации, стойкости к искажениям) была достигнута доказуемая стойкость алгоритма к целому классу атак, основанных на выявлении корреляционных связей между отдельными битами ЦВЗ и пикселями изображения-контейнера.

### *Благодарности*

Работа выполнена при поддержке Федерального агентства научных организаций (соглашение № 007-ГЗ/Ч3363/26), а также при поддержке РФФИ (гранты 15-07-05576, 16-41-630676) и Минобрнауки РФ в рамках гранта президента РФ МК-1907.2017.9.

### *Литература*

1. **Cox, I.J.** Digital watermarking and steganography / I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, T. Kalker. – 2nd ed. – San Francisco: Morgan Kaufmann Publishers Inc., 2009. – 593 p. – ISBN: 978-0-12-372585-1.
2. **Chen, B.** Quantization index modulation: A class of provably good methods for digital watermarking and information embedding / B. Chen, G.W. Wornell // IEEE Transactions on Information Theory. – 2001. – Vol. 47, Issue 4. – P. 1423-1443. – DOI: 10.1109/18.923725.
3. **Noda, H.** High-performance JPEG steganography using quantization index modulation in DCT domain / H. Noda, M. Niimi, E. Kawaguchi // Pattern Recognition Letters. – 2006. – Vol. 27, Issue 5. – P. 455-461. – DOI: 10.1016/j.patrec.2005.09.008.
4. **Jiang, Y.** Adaptive spread transform QIM watermarking algorithm based on improved perceptual models / Y. Jiang, Y. Zhang, W. Pei, K. Wang // AEU – International Journal of Electronics and Communications. – 2013. – Vol. 67, Issue 8. – P. 690-696. – DOI: 10.1016/j.aeue.2013.02.005.
5. **Phadikar, A.** Multibit quantization index modulation: A high-rate robust data-hiding method / A. Phadikar // Journal of King Saud University – Computer and Information Sciences. – 2013. – Vol. 25, Issue 2. – P. 163-171. – DOI: 10.1016/j.jksuci.2012.11.005.
6. **Hakka, M.** DCT-OFDM based watermarking scheme robust against clipping attack / M. Hakka, M. Kuribayashi, M. Morii // Proceedings of the 1st international workshop on Information hiding and its criteria for evaluation (IWIHC '14). – 2014. – P. 18-24. – DOI: 10.1145/2598908.2598914.
7. **Fang, Y.** CDMA-based watermarking resisting to cropping / Y. Fang, J. Huang, S. Wu // Proceedings of 2004 International Symposium on Circuits and Systems (ISCAS '04). – 2004. – Vol. 2. – P. 25-28. – DOI: 10.1109/ISCAS.2004.1329199.
8. **Huang, Y.-B.** A dither modulation audio watermarking algorithm based on HAS / Y.-B. Huang, Q.-Y. Zhang, Z. Liu, Y.-J. Di, Z.-T. Yuan // Research Journal of Applied Sciences, Engineering and Technology. – 2012. – Vol. 4, Issue 21. – P. 4206-4211.
9. **Khademi, N.** Audio watermarking based on quantization index modulation in the frequency domain / N. Khademi, M.A. Akhaee, S.M. Ahadi, M. Moradi, A. Kashi // IEEE International Conference on Signal Processing and Communications (ICSPC 2007). – 2007. – P. 1127-1130. – DOI: 10.1109/ICSPC.2007.4728522.
10. **Zolotavkin, Y.** A new two-dimensional quantization method for digital image watermarking / Y. Zolotavkin, M. Juhola // 2015 17th International Conference on Advanced Communication Technology (ICACT). – 2015. – P. 155-160. – DOI: 10.1109/ICACT.2015.7224776.
11. **Matam, B.R.** Watermarking: How secure is the DM-QIM embedding technique? / B.R. Matam, D. Lowe // 16th International Conference on Digital Signal Processing. – 2009. – P. 1-8. – DOI: 10.1109/ICDSP.2009.5201248.
12. **Matam, B.R.** Watermark-only security attack on DM-QIM watermarking: Vulnerability to guided key guessing / B.R. Matam, D. Lowe. – In book: Crime prevention technologies and applications for advancing criminal investigation / ed. by Ch.-T. Li, A.T.S. Ho. – 2012. – P. 85-106. – DOI: 10.4018/978-1-4666-1758-2.ch007.
13. **Wang, Y.** Steganalysis of block-structured stegotext / Y. Wang, P. Moulin // Proceedings of SPIE. – 2004. – Vol. 5306. – P. 477-488. – DOI: 10.1117/12.527745.
14. **Mitekin, V.** A new key recovery attack against DM-QIM image watermarking algorithm / V. Mitekin // Proceedings of SPIE. – 2017. – Vol. 10341. – 103411A. – DOI: 10.1117/12.2268550.
15. **Глумов, Н.И.** Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н.И. Глумов, В.А. Митекин // Компьютерная оптика. – 2011. – Т. 35, № 2. – С. 262-267.
16. **Митекин, В.А.** Метод встраивания информации повышенной ёмкости в видео, стойкий к ошибкам потери синхронизации / В.А. Митекин, В.А. Федосеев // Компьютерная оптика. – 2014. – Т. 38, № 3. – С. 564-573.
17. **Mitekin, V.** A new method for high-capacity information hiding in video robust against temporal desynchronization / V. Mitekin, V.A. Fedoseev // Proceedings of SPIE. – 2015. – Vol. 9445. – 94451A. – DOI: 10.1117/12.2180550.

18. **Siegenthaler, T.** Correlation-immunity of nonlinear combining functions for cryptographic applications (Corresp.) / T. Siegenthaler // IEEE Transactions on Information theory. – 1984. – Vol. 30, Issue 5. – P. 776-780. – DOI: 10.1109/TIT.1984.1056949.
19. BOWS-2: Break our watermarking system. 2nd ed. [Electronical Resource]. – URL: http://bows2.ec-lille.fr (request date 01.02.2017).
20. **Barni, M.** Watermarking systems engineering: Enabling digital assets security and other applications / M. Barni, F. Bartolini. – New York, Basel: Marcel Dekker, Inc., 2004. – 500 p. – ISBN: 0-8247-4806-9.

### *Сведения об авторах*

**Митекин Виталий Анатольевич**, 1983 года рождения. В 2006 году окончил Самарский государственный аэрокосмический университет (ныне – Самарский национальный исследовательский университет имени академика С.П. Королева) по специальности «Прикладная математика и информатика», кандидат технических наук (2009). В настоящее время работает доцентом кафедры геоинформатики и информационной безопасности того же университета и научным сотрудником в ИСОИ РАН – филиале ФНИЦ «Кристаллография и фотоника» РАН. Круг научных интересов включает обработку изображений и распознавание образов, стеганографию и стегоанализ, криптографию. E-mail: vmitekin@gmail.com .

**Федосеев Виктор Андреевич**, 1986 года рождения, в 2009 году окончил Самарский государственный аэрокосмический университет имени академика С.П. Королёва (ныне – Самарский национальный исследовательский университет имени академика С.П. Королева) по специальности «Прикладная математика и информатика», кандидат физико-математических наук (2012). В настоящее время работает доцентом кафедры геоинформатики и информационной безопасности того же университета и научным сотрудником в ИСОИ РАН – филиале ФНИЦ «Кристаллография и фотоника» РАН. Области научных интересов: обработка и анализ изображений, цифровые водяные знаки, стеганография. E-mail: vicanfed@gmail.com .

*ГРНТИ: 28.21.19.*
*Поступила в редакцию 14 ноября 2017 г. Окончательный вариант – 20 декабря 2017 г.*

## NEW SECURE QIM-BASED INFORMATION HIDING ALGORITHMS

*V.A. Mitekin [1,2], V.A. Fedoseev [1,2]*
*[1] Samara National Research University, Samara, Russia,*
*[2] Image Processing Systems Institute of RAS – Branch of the FSRC "Crystallography and Photonics" RAS, Samara, Russia*

### *Abstract*

The paper proposes two information hiding algorithms for multimedia based on Quantization Index Modulation (QIM): IM-QIM and SIM-QIM. They are designed to prevent a statistical attack which is able to restore a secret key using the correlation between key bits and multimedia data samples. To obtain the required security, we use a correlation immune embedding function, which guarantees statistical independence between the watermarked data and the key. The proposed algorithms are described for the case of spatial embedding in images but the algorithms can also be used to hide information in any multimedia data source in spatio-temporal and spectral domains. The results of the experimental investigation have confirmed that the algorithms developed provide the required security against a statistical attack and also have shown that the algorithms do not introduce additional distortions compared with the conventional QIM method. However, the experiments have also shown that the new algorithms are less robust against additive noise and JPEG compression.

*Keywords:* QIM, DM-QIM, IM-QIM, quantization index modulation, dither modulation, digital watermark.

*Citation*: Mitekin VA, Fedoseev VA. New secure QIM-based information hiding algorithms. Computer Optics 2018; 42(1): 118-127. DOI: 10.18287/2412-6179-2018-42-1-118-127.

*Acknowledgements:* The work was supported by the Russian Foundation for Basic Research (RFBR grants ## 15-07-05576, and 16-41-630676) and by the RF Ministry of Education and Science (grant MK-1907.2017.9).

### *References*

[1] Cox IJ, Miller ML, Bloom JA, Fridrich J, Kalker T. Digital watermarking and steganography. 2nd ed. San Francisco: Morgan Kaufmann Publishers Inc.; 2009. ISBN: 978-0-12-372585-1.
[2] Chen B, Wornell GW. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. IEEE Transactions on Information Theory 2001; 47(4): 1423-1443. DOI: 10.1109/18.923725.
[3] Noda H, Niimi M, Kawaguchi E. High-performance JPEG steganography using quantization index modulation in DCT domain. Pattern Recognition Letters 2006; 27(5): 455-461. DOI: 10.1016/j.patrec.2005.09.008.

[4] Jiang Y, Zhang Y, Pei W, Wang K. Adaptive spread transform QIM watermarking algorithm based on improved perceptual models. AEU – International Journal of Electronics and Communications 2013; 67(8): 690-696. DOI: 10.1016/j.aeue.2013.02.005.
[5] Phadikar A. Multibit quantization index modulation: A high-rate robust data-hiding method. Journal of King Saud University – Computer and Information Sciences 2013; 25(2): 163-171. DOI: 10.1016/j.jksuci.2012.11.005.
[6] Hakka M, Kuribayashi M, Morii M. DCT-OFDM Based Watermarking Scheme Robust Against Clipping Attack. Proceedings of the 1st international workshop on Information hiding and its criteria for evaluation (IWIHC '14) 2014: 18-24. DOI: 10.1145/2598908.2598914.
[7] Fang Y, Huang J, Wu S. CDMA-based watermarking resisting to cropping. 2004 IEEE International Symposium on Circuits and Systems (IEEE Cat. No.04CH37512) 2004; 2: 25-28. DOI: 10.1109/ISCAS.2004.1329199.
[8] Huang Y-B, Zhang Q-Y, Liu Z, Di Y-J, Yuan Z. A dither modulation audio watermarking algorithm based on HAS. Research Journal of Applied Sciences, Engineering and Technology 2012; 4: 4206-4211.
[9] Khademi N, Akhaee MA, Ahadi SM, Moradi M, Kashi A. Audio Watermarking based on Quantization Index Modulation in the Frequency Domain. ICSPC 2007: 1127-1130. DOI: 10.1109/ICSPC.2007.4728522.
[10] Zolotavkin Y, Juhola M. A new two-dimensional quantization method for digital image watermarking. ICACT 2015: 155-160. doi:10.1109/ICACT.2015.7224776.
[11] Matam BR, Lowe D. Watermarking: How secure is the DM-QIM embedding technique? 2009 16th International Conference on Digital Signal Processing 2009: 1-8. DOI: 10.1109/ICDSP.2009.5201248.
[12] Matam BR, Lowe D. Watermark-only security attack on DM-QIM watermarking: Vulnerability to guided key guessing. In Book: Li BR, Ho ATS, eds. Crime prevention technologies and applications for advancing criminal investigation. IGI Global; 2012: 85-106. DOI: 10.4018/978-1-4666-1758-2.ch007.
[13] Wang Y, Moulin P. Steganalysis of block-structured stegotext. Proc SPIE 2004; 5306: 477-488. DOI: 10.1117/12.527745.
[14] Mitekin V. A new key recovery attack against DM-QIM image watermarking algorithm. Proc SPIE 2017; 10341: 103411A. DOI: 10.1117/12.2268550.
[15] Glumov NI, Mitekin VA. A new semi-fragile watermarking algorithm for image authentication and information hiding. Computer Optics 2011; 35(2): 262-267.
[16] Mitekin VA, Fedoseev VA. A new robust information hiding method for video. Computer Optics 2014; 38(3): 564–73.
[17] Mitekin V, Fedoseev VA. A new method for high-capacity information hiding in video robust against temporal desynchronization. Proc SPIE 2015; 9445: 94451A. DOI: 10.1117/12.2180550.
[18] Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications (Corresp.). IEEE Transactions on Information Theory 1984; 30(5): 776-780. DOI: 10.1109/TIT.1984.1056949.
[19] BOWS-2: Break our watermarking system. 2nd ed. Source: ⟨http://bows2.ec-lille.fr/⟩.
[20] Barni M, Bartolini F. Watermarking systems engineering: enabling digital assets security and other applications. New York, Basel: Marcel Dekker, Inc.; 2004. ISBN: 0-8247-4806-9.

### *Author's information*

**Vitaly Anatolyevich Mitekin** (b. 1983) graduated (2006) from Samara State Aerospace University (presently, Samara National Research University, short – Samara University), majoring in Applied Mathematics and Computer Science in 2006. He received his Candidate degree in Technical Sciences in 2009. Currently he is an associate professor at the Geoinformatics and Information Security department at Samara University and a research scientist at Image Processing Systems Institute of RAS – Branch of the FSRC "Crystallography and Photonics" RAS. His scientific interests include image processing and recognition, steganography and steganalysis, cryptography. E-mail: *vmitekin@gmail.com* .

**Victor Andreevich Fedoseev** (b. 1986) graduated (2009) from Samara State Aerospace University (presently, Samara National Research University, short – Samara University), majoring in Applied Mathematics and Computer Science. Candidate degree in Computer Science (2012). Currently he is an associate professor at the Geoinformatics and Information Security department at Samara University and a research scientist at Image Processing Systems Institute of RAS – Branch of the FSRC "Crystallography and Photonics" RAS. His scientific interests include image processing and analysis, digital watermarking and steganalysis. E-mail: *vicanfed@gmail.com* .

*Received November 14, 2017. The final version – December 20, 2017.*