

УДК 681.323(075)

А. П. Бахрушин, Г. И. Бахрушина, Р. И. Цой

РАЗРАБОТКА МЕТОДОВ ЗАЩИТЫ ВИДЕОПРОДУКЦИИ УСТОЙЧИВЫХ К ГЕОМЕТРИЧЕСКИМ АТАКАМ

В статье рассматриваются различные методы внедрения в исходные изображения цифровых водяных знаков (ЦВЗ) устойчивые к геометрическим атакам. В этой связи была исследована возможность внедрения ЦВЗ в частотной области исходного изображения и в пространственной. Для достижения их инвариантности к геометрическим атакам было предложено выполнять преобразование Фурье в полярно-логарифмической системе координат. Экспериментальные результаты показали, что наибольшая устойчивость ЦВЗ к геометрическим атакам достигается при внедрении спектральных образов ЦВЗ в исходные изображения в пространственной области.

Ключевые слова: цифровые водяные знаки, геометрические атаки, преобразование Фурье

Alexander P. Bahrushin, Galina I. Bahrushina, Rudolf I. Choi. DEVELOPMENT OF VIDEO PROTECTING METHODS RESISTANT TO GEOMETRIC ATTACKS (Far Eastern State Academy for Social and Humanity Studies, Pacific National University)

In this paper, different methods of digital watermarking, which are robust to geometric attacks are considered. In connection with that the opportunity of watermark embedding in frequency domain of the host image or in the spatial one was studied. To make these methods an invariant to geometric attacks it was proposed to fulfill the Fourier transform in Log-Polar Mapping. Experimental results have shown that the highest robustness of watermarking is reached when spectral patterns of the watermark are embedded into the host image in spatial domain.

Keywords: digital watermarks, geometric attacks, Fourier transform

Одной из актуальных проблем, возникающих при создании, хранении и передаче видеопродукции в цифровой форме, является защита ее авторских прав. Действительно, информационная продукция, представленная, например, в форме цифровых изображений, а также цифровых аудио или видеоданных, исключительно уязвима в плане ее неправомерного использования. Любой документ в цифровой форме может быть легко скопирован, обработан, размножен и распространен.

Один из возможных подходов к решению проблемы защиты информационной продукции от ее нелегального использования сводится к внедрению в нее невидимых структур, чтобы таким образом “пометить” ее владельца. Такая невидимая структура получила название “цифрового водяного знака” (ЦВЗ) по аналогии с водяными знаками, используемыми для защиты ценных бумаг и денежных купюр.

ЦВЗ могут содержать информацию об авторских правах или информацию об установлении соответствия копии оригиналу. Очевидно, что наличие водяных знаков в мультимедийных данных не должно быть явным, и их обнаружение может быть осуществлено только с помощью специально разработанных методов. Обычно водяные знаки внедряются в такие виды мультимедийных данных, как изображения, аудио и цифровое видео. Для эффективной защиты мультимедийных данных ЦВЗ должны отвечать следующим требованиям:

- скрытность, т.е. их практически невозможно обнаружить ни визуально, ни на слух;
- непредсказуемость местонахождения, вследствие чего возникают дополнительные трудности при попытках их нелегального обнаружения и извлечения криминальными лицами;
- простота обнаружения лицами, имеющими к ним санкционированный доступ;
- устойчивость к воздействиям случайного и намеренного характера, приводящим к искажению водяных знаков.

На рис. 1 представлена блок-схема процесса внедрения ЦВЗ в исходный мультимедийный сигнал. Согласно приведенной блок-схеме, цифровой водяной знак, который наиболее часто представляется в виде последовательности бинарных цифр, тем или иным образом замешивается в исходный мультимедийный сигнал с использованием ключа. Очевидно, что в результате этой процедуры мультимедийный сигнал претерпевает некоторые изменения, однако степень этих изменений устанавливается такой, чтобы они не воспринимались ни визуально, ни на слух.

На рис. 2 представлена блок-схема процесса извлечения водяного знака из мультимедийного сигнала. Как следует из рис. 2, доступ к водяному знаку возможен только при знании ключа. При отсутствии этой информации водяной знак невозможно ни извлечь, ни удалить, ни подделать. Поэтому вопрос, связанный с разработкой кодовых ключей, которые бы обеспечивали как внедрение водяных знаков, так и их надежное извлечение, является одним из важнейших.

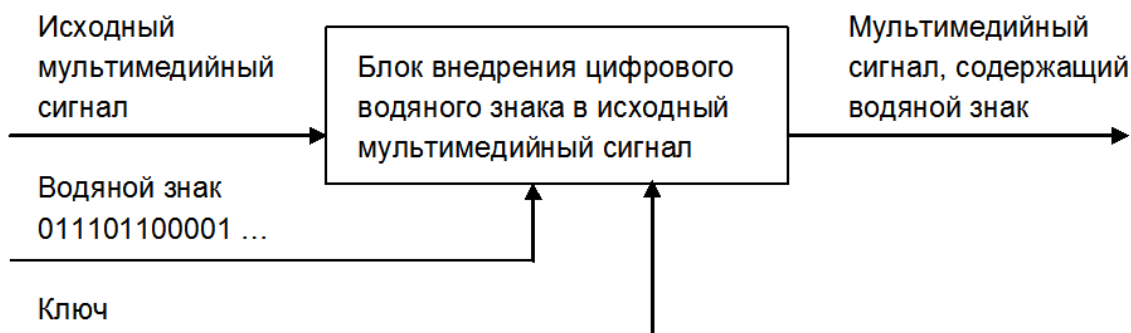


Рис. 1. Блок-схема процесса внедрения ЦВЗ в исходный мультимедийный сигнал

Основное требование, которому должна отвечать система защиты мультимедийных данных — это, прежде всего, требование высокой надежности. Действительно, в процессе, например, процедуры сжатия информации мультимедийный сигнал может претерпевать те или изменения, а, следовательно, в той или иной степени будет искажаться и внедренный в него водяной знак. Поэтому для надежной защиты мультимедийных данных от несанкционированного копирования разрабатываемый алгоритм извлечения водяных знаков не должны терять свою работоспособность даже после того, когда они претерпели значительные искажения.

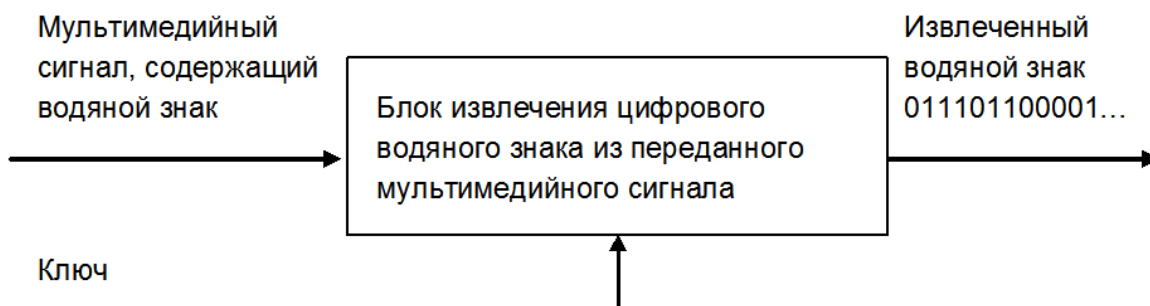


Рис. 2. Блок-схема процесса извлечения ЦВЗ из мультимедийного сигнала

Как уже отмечалось, ЦВЗ могут быть внедрены как в одномерные сигналы — в виде аудио продукции, так и в двумерные — в виде изображений. Однако в отличие от одномерного случая, при решении задачи защиты двумерных сигналов в виде изображений возникают дополнительные трудности. Действительно, в этом случае система защиты мультимедийных данных должна быть устойчивой не только, например, к воздействию различного рода помех и (или) процедуре сжатия информации, но также должна обладать свойством инвариантности к таким геометрическим преобразованиям, как пространственный сдвиг изображения в горизонтальном и (или) вертикальном направлениях, его поворот и изменение масштаба.

Рассмотрим вопросы построения системы защиты мультимедийных данных в виде дискретизированных изображений, которая была бы устойчива к перечисленным геометрическим преобразованиям. В этой связи, прежде всего, необходимо остановиться на некоторых специфических особенностях этих преобразований. Предположим, что исходное изображение состояло из $N_1 \times M_1$ пикселей. Допустим, что в результате изменения масштаба имело место уменьшение линейных размеров изображения, и оно стало иметь размер $N_2 \times M_2$, причем $N_2 \ll N_1$ и $M_2 \ll M_1$. Очевидно, что в этом случае вновь полученное изображение будет иметь меньшее разрешение и, соответственно, меньшее разрешение будет иметь встроенный в это изображение ЦВЗ. Как известно, уменьшение разрешения изображения, прежде всего, приводит к потере мелких деталей, т.е. к урезанию высокочастотных составляющих амплитудно-частотного спектра изображения. Другими словами, процедура уменьшения линейных размеров изображения в данном смысле эквивалентна низкочастотной фильтрации изображения, которая выполняется, например, при его сжатии. С другой стороны, увеличение размеров изображения может привести к удалению его приграничных областей. Таким образом, в результате изменения масштаба изображения не только изменяются его размеры, но также может измениться конфигурация изображения и его амплитудно-частотный спектр, что неизбежно приведет к искажению ЦВЗ. Уместно заметить, что, как правило, все вновь разработанные алгоритмы по защите мультимедийных знаков, прежде всего, проверяются на устойчивость по отношению к процедуре сжатия информации, как наиболее разрушительной для ЦВЗ.

Поворот изображения на некоторый произвольный угол также приводит к его структурным изменениям. Так, например, при повороте изображения на углы не кратные 90° прямые линии преобразуются в ступенчатые кривые, за счет которых в спектре изображения появляются дополнительные высокочастотные составляющие, что равносильно воздействию на изображение высокочастотных помех. Следует отметить, что если ЦВЗ был внедрен в спектр изображения именно в области высоких частот, то, очевидно, что в этом случае ЦВЗ претерпит те или иные искажения. Кроме того, поворот изображения, также как его увеличение, может привести к изменению его конфигурации — к срезанию приграничных областей.

Аналогичная ситуация может возникнуть и при смещении изображения по горизонтали и (или) по вертикали.

Таким образом, возникает задача извлечения из анализируемого изображения ЦВЗ не только с неизвестным пространственно-угловым положе-

нием и масштабом, но и искаженного в том или ином смысле в результате выполненных геометрических преобразований.

Один из методов извлечения ЦВЗ из изображения, над которым были произведены геометрические преобразования, сводится, прежде всего, к попытке определить, каким конкретно геометрическим преобразованиям было подвергнуто изображение, с тем, чтобы привести его к исходному состоянию и только после этого приступить к извлечению ЦВЗ. С этой целью в изображение вместе с информационным ЦВЗ встраивается так называемый регистрационный ЦВЗ, который, как и информационный ЦВЗ, не должен восприниматься визуально [1]. Особенностью данного метода является то, что во все изображения, подлежащие защите, внедряется один и тот же регистрационный ЦВЗ. Поэтому в случае обнаружения регистрационного ЦВЗ лицами, занимающимися незаконным тиражированием мультимедийных данных, этот знак может быть удален из всей партии видео продукции, в результате чего проблема обнаружения информационных ЦВЗ, имеющих произвольную пространственно-угловую ориентацию, значительно усложнится.

Другой подход к решению проблемы извлечения ЦВЗ состоит в том, что внедряемому в исходное изображение ЦВЗ придается такая структура, которую можно было бы легко распознать. Например, в работе [2] предлагается один и тот же ЦВЗ повторно внедрять в изображение в различных его областях. В этом случае автокорреляционная функция двумерного сигнала в виде изображения с внедренными в него ЦВЗ будет иметь пики, соответствующие местоположениям этих ЦВЗ. Какие-либо изменения значений этих пиков могут быть использованы для выявления характера геометрических преобразований.

В работе [3] предлагается еще один метод, согласно которому сначала над исходным изображением производится процедура нормализации, и только после ее выполнения в него внедряется ЦВЗ. По завершении внедрения ЦВЗ нормализованное изображение преобразуется к своему исходному состоянию. При анализе изображения на наличие в нем ЦВЗ оно опять подвергается процедуре нормализации, и только затем выполняются действия по обнаружению и извлечению ЦВЗ. Очевидно, что процедура нормализации исходного изображения должна быть инвариантной по отношению к возможным геометрическим преобразованиям. Для ее выполнения могут быть использованы, например, геометрические моменты изображения.

Рассматриваемый в данной работе подход к решению проблемы извлечения ЦВЗ из изображения, над которым были произведены геометрические преобразования, основан на альтернативной стратегии, исключающей использование регистрационных ЦВЗ, а также процедуры нормализации исходного изображения. Идейной основой разработанной стратегии является

теория распознавания образов. Действительно, в рамках этой теории на протяжении нескольких последних десятилетий велись интенсивные исследования по построению математических моделей распознавания изображений инвариантных к их пространственно-угловому положению и масштабу. Так, например, в работе [4] данная задача решается на основе использования инвариантных признаков в виде моментов различных порядков. Принципиально другой подход к решению данной проблемы основан на идее использования в качестве признаков, описывающих распознаваемые изображения, составляющих амплитудно-частотного спектра, полученного с помощью прямого преобразования Фурье (ППФ) [5,6,7]:

$$\dot{S}(u, v) = \sum_{u=0}^{N-1} \sum_{v=1}^{M-1} s(l, k) \exp \left[-i(ul + vk) \right],$$

где u и v — номера гармонических составляющих вдоль координатных осей l и k , соответственно, $u = \overline{0, N-1}$, $v = \overline{0, M-1}$;

$s(l, k)$ — значение яркости изображения в точке (l, k) .

Заметим, что в соответствии с основным свойством прямого преобразования Фурье амплитудно-частотный спектр, полученный при использовании системы экспоненциальных базисных функций, обладает свойством инвариантности по отношению к циклическим сдвигам изображения на величины d и b вдоль координатных осей, т.е. если $s(l, k) \leftrightarrow \dot{S}(u, v)$, то

$$s(l-d, k-b) \leftrightarrow \exp(-iud - ivb) \dot{S}(u, v), \quad (1)$$

и соответственно

$$|\dot{S}(l, k)| = |\exp(-iud - ivb)| |\dot{S}_s(u, v)|, \quad (2)$$

где $|\dot{S}_s(u, v)|$ - спектр сдвинутого изображения.

Из выражения (1) также следует, что сдвигу изображения соответствует операция умножения его комплексного спектра $\dot{S}(u, v)$ на множитель с линейной фазой $\exp(-iud - ivb)$.

Рассмотрим наиболее общий случай, когда изображение, представленное двумерным сигналом $s(k, l)$, подвергается таким геометрическим преобразованиям, как сдвиг, поворот на угол α и сжатие или растяжение на величину σ . В этом случае можно записать:

$$\hat{s}(l, k) = s(\sigma(l \cos \alpha + k \sin \alpha) - d, \sigma(-l \sin \alpha + k \cos \alpha) - b).$$

Амплитудно-частотный спектр данного изображения можно получить с помощью прямого преобразования Фурье:

$$\left| \hat{S}(u, v) \right| = \frac{1}{\sigma^2} \left| S \left(\frac{u \cos \alpha + v \sin \alpha}{\sigma}, \frac{-u \sin \alpha + v \cos \alpha}{\sigma} \right) \right|. \quad (3)$$

Очевидно, что спектра $\left| \hat{S}(u, v) \right|$ не зависит от параметров сдвига d и b .

Рассмотрим возможность получения спектра, обладающего свойством инвариантности не только к пространственному, но также к угловому положению изображения и его масштабу. Для этого выполним переход от декартовых координат (ДК) к полярно-логарифмическим координатам (ПЛК):

$$k = \exp \rho \cos \beta, \quad l = \exp \rho \sin \beta,$$

где $\exp \rho$ — радиус-вектор в ПЛК;

β — угол поворота радиуса-вектора.

Тогда выражение (3) можно переписать в виде:

$$\left| \hat{S}(u, v) \right| = \frac{1}{\sigma^2} \left| S(\sigma^{-1} \exp \rho \cos (\beta - \alpha), \sigma^{-1} \exp \rho \sin (\beta - \alpha)) \right|.$$

С учетом того, что

$$\sigma^{-1} \exp \rho \cos (\beta - \alpha) = \exp(-\ln \sigma) \exp \rho \cos (\beta - \alpha) = \exp(\rho - \ln \sigma) \cos (\beta - \alpha)$$

получаем:

$$\left| \hat{S}(u, v) \right| = \frac{1}{\sigma^2} \left| S(\exp(\rho - \ln \sigma) \cos (\beta - \alpha), \exp(\rho - \ln \sigma) \sin (\beta - \alpha)) \right|.$$

Или

$$A(\rho, \beta) = \left| \hat{S}(\rho, \beta) \right| = \frac{1}{\sigma^2} \left| S(\rho - \ln \sigma, \beta - \alpha) \right| \quad (4)$$

Из (4) следует, что изменение масштаба изображения в σ раз и его поворот на угол α приводит к смещениям полученного спектра $A(\rho, \beta)$ вдоль координатных осей ρ и β , соответственно. Поэтому после повторного ППФ над матрицей, представляющей спектр $A(\rho, \beta)$, можно получить новый спектр $\hat{A}(u, v)$, обладающий свойством инвариантности к пространственно-угловому положению изображения и его масштабу, как показано на рис. 3.

Для перехода к исходному изображению необходимо в обратной последовательности сначала выполнить обратное преобразование Фурье (ОПФ), затем осуществить переход от ПЛК к ДК и снова повторить процедуру ОПФ.

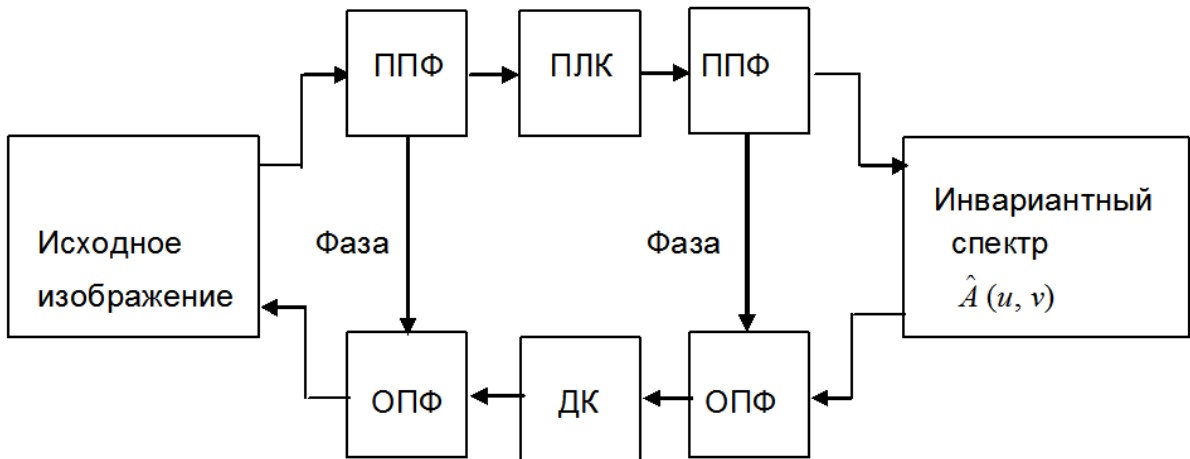


Рис. 3. Алгоритм формирования инвариантного спектра $\hat{A}(u, v)$ с последующим переходом в пространственную область

На рис. 4 представлен алгоритм внедрения ЦВЗ в исходное изображение, а на рис. 5 — алгоритм извлечения ЦВЗ из изображения, имеющего произвольные пространственно-угловую ориентацию и масштаб.

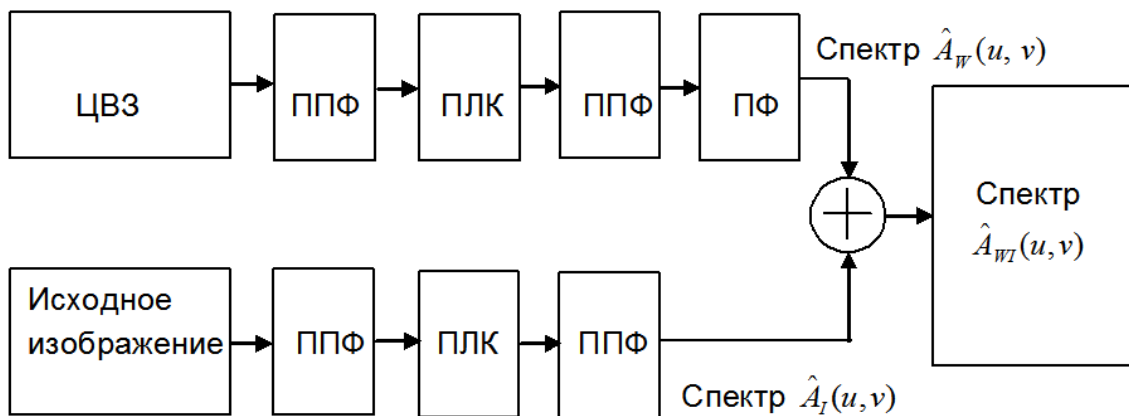


Рис. 4. Алгоритм внедрения ЦВЗ в исходное изображение в частотной области

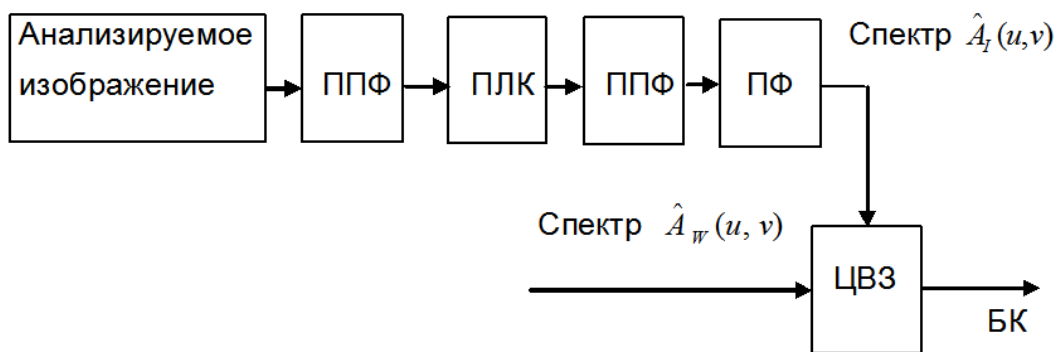


Рис. 5. Алгоритм извлечения ЦВЗ из анализируемого изображения

В соответствии с алгоритмом, представленном на рис. 4, параллельно формируются два спектра — двумерный спектр $\hat{A}_w(u, v)$, представляющий собой описание ЦВЗ в спектральной области, и двумерный спектр $\hat{A}_I(u, v)$, являющий собой спектральный образ исходного изображения. Процедуру суммирования этих спектров, в результате которой формируется новый спектр $\hat{A}_{wI}(u, v)$, можно рассматривать как процедуру внедрения ЦВЗ в исходное изображение в заданной частотной области, параметры которой определяются с помощью полосового фильтра (ПФ). Для получения изображения с встроенным в него ЦВЗ в пространственной области выполняются обратные преобразования в соответствии с алгоритмом, отображенным на рис. 3.

На рис. 5 представлен алгоритм извлечения ЦВЗ из анализируемого изображения. Согласно предлагаемому алгоритму, на входы блока корреляции (БК), с одной стороны, подается отфильтрованный с помощью ПФ спектр анализируемого изображения $\hat{A}_I(u, v)$, с другой, — спектр $\hat{A}_w(u, v)$.

Так как данные спектры являются инвариантными по отношению к геометрическим преобразованиям изображения, то процедура их сопоставления практически сводится к вычислению нормализованного коэффициента корреляции: если он превышает некоторый установленный порог, то принимается решение о наличии на анализируемом изображении ЦВЗ и в той или иной форме выдается его изображение.

При практической реализации описанных алгоритмов возникает ряд трудностей. Во-первых, амплитудно-частотный спектр изображения $A(u, v) = |\hat{S}(u, v)|$ должен отвечать условию симметрии:

$$A(u, v) = A(N - u, M - v). \quad (5)$$

Во-вторых, спектр $A(\rho, \beta)$, определенный в полярно-логарифмической системе координат, в соответствии с условием (5.20), должен быть представлен в виде симметричной матрицы, состоящей из двух идентичных половин:

$$A(\rho, \beta) = A(\rho, \pi + \beta).$$

Здесь точка с координатами $(N/2, M/2)$ является центром вращения изображения.

Отметим также, что в результате переходов из одной системы координат в другую возникает проблема установления поэлементного соответствия между матрицами, сформированными в различных системах координат,

от решения которой в значительной степени зависит качество изображения, в которое внедряется ЦВЗ.

С целью преодоления отрицательных последствий от смены систем координат можно воспользоваться теми или иными методами интерполяции. Как известно, для успешного решения задачи интерполяции, прежде всего, необходимо, чтобы анализируемый сигнал был представлен выборкой достаточно большого объема. Для получения удовлетворительного качества изображения матрица, сформированная в полярно-логарифмической системе координат, должна, как минимум, состоять из 512×512 элементов.

Следует также заметить, что хорошие результаты интерполяции могут быть достигнуты только в тех случаях, когда значения соседних элементов матрицы близки друг к другу. При выполнении преобразований Фурье последнее условие практически не выполняется, так как значения амплитуд спектра в области низких частот, как правило, резко превышают значения амплитуд в области средних и, в особенности, в области высоких частот.

Поэтому в данной работе с целью сохранения качества исходного изображения предлагается перечисленным преобразованиям подвергать только ЦВЗ, как показано на рис. 6.

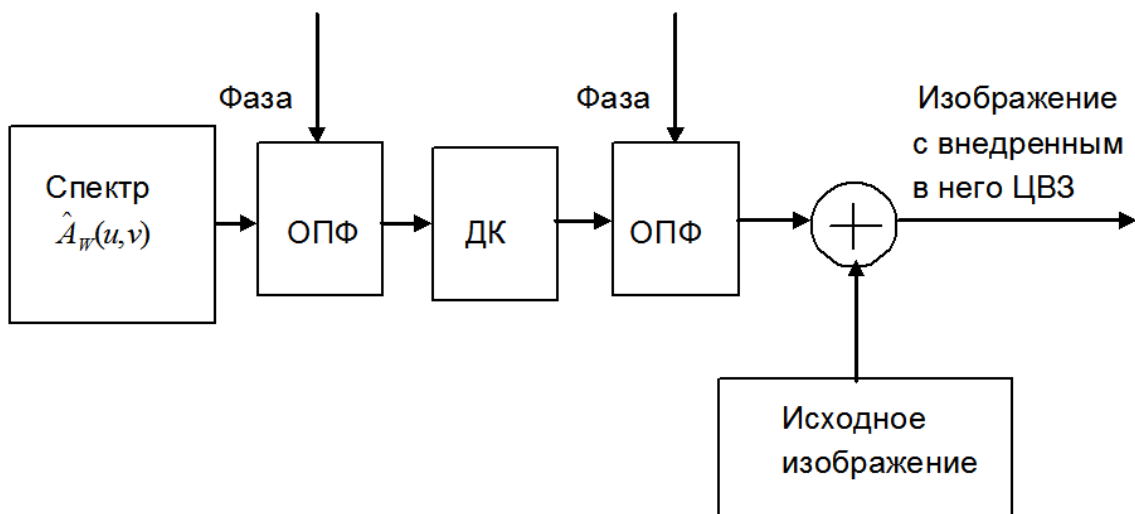
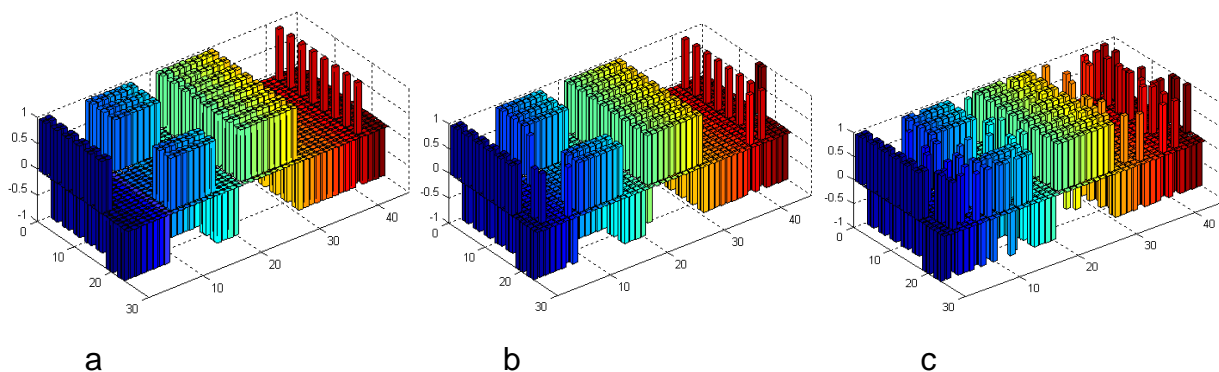


Рис. 6. Алгоритм внедрения ЦВЗ в исходное изображение в пространственной области

В этом случае ЦВЗ, представленный в заданной полосе частот в виде инвариантного к геометрическим преобразованиям спектра $\hat{A}_w(u, v)$, после ряда преобразований внедряется в исходное изображение не в частотной, а в пространственной области. В результате отпадает необходимость в выполнении над исходным изображением различных преобразований, которые отрицательным образом могли бы отразиться на его качестве и для реали-

зации которых потребовались бы значительные временные затраты. На рис.6 представлен алгоритм внедрения ЦВЗ в исходное изображение в пространственной области.

С целью апробации схем, представленных на рис. 4 и рис. 6, были проведены экспериментальные исследования в течение которых ЦВЗ, размером 24×46 пикселей и числом уровней квантования равным трем (см. рис.7-а), внедрялся в тестовые изображения “Барбара” и “Лена”, размером 512×512 пикселей с числом уровней квантования 256. Для оценки степени искажения исходного изображения после внедрения в него ЦВЗ и выполнения над ним преобразований Фурье в полярно-логарифмической системе координат использовался показатель PSNR. Степень схожести между эталонным изображением ЦВЗ и извлеченным оценивалась с помощью нормализованного коэффициента корреляции ρ , для схемы, представленной на рис. 6 и $\hat{\rho}$, для схемы, представленной на рис. 4.



**Рис. 7. Эталонный ЦВЗ (а),
извлеченный ЦВЗ при повороте исходного изображения на 30° (b),
извлеченный ЦВЗ при изменении масштаба на величину 0.6 (с)**

При внедрении ЦВЗ в исходные изображения в частотной области (см. рис. 4) и выполнении над ними различных преобразований их качество резко снижалось и для этих изображений показатель PSNR составлял величину порядка 25. В то же время при внедрении ЦВЗ в исходные изображения в пространственной области их качество практически оставалось прежним и для этих изображений показатель PSNR составлял величину порядка 40. Таким образом, экспериментальные исследования подтвердили предположения о резком снижении качества исходного изображения при выполнении над ним преобразований Фурье в полярно-логарифмической системе координат.

На рис. 7-б и 7-с представлены ЦВЗ, извлеченный из исходного изображения при его различном угловом положении масштабе.

Таблица

В приведенной ниже таблице отражены данные, характеризующие зависимость нормализованных коэффициентов ρ и $\hat{\rho}$ от геометрических атак и JPEG атаки

Угол	00	10	100	300	450	600	900
ρ	1.00	1.00	1.00	1.00	1.00	1.00	1.00
$\hat{\rho}$	0.99	0.82	0.86	0.79	0.71	0.65	0.86
Масштаб	0.5	0.6	0.7	0.8	0.9	1.1	1.2
ρ	0.54	0.76	0.86	0.88	0.90	0.96	0.96
$\hat{\rho}$	-	0.78	0.83	0.85	0.88	0.90	0.84
JPEG	5 %	10 %	20 %	30 %	40 %	50 %	60 %
ρ	0	0..90	0..90	0..92	0..94	0..94	0..95
$\hat{\rho}$	0..32	0.76	0..86	0.94	0..96	0..97	0..98

Как следует из представленных в таблице данных, наибольшие значения коэффициенты корреляции достигают при внедрении ЦВЗ в исходные изображения в пространственной области при всех видах атак. Кроме того, показатель PSNR в этом случае также достигает больших значений.

Литература

1. Pereria S. and Pun T. Fast robust template matching for affined resistant image watermarks. In Proc. 3-rd Int. Information Hiding Workshop, 1999, pp. 207—218.
2. Honsinger and Daly. Method for detecting rotation. and magnification in images. U.S. Patent, 5835639, 1998.
3. Alghoniemy V. And Tewfic J/ Geometric distortion correlation through image normalization. In Proc. Int. Conf. Multimedia Expo, vol.3, 2000, pp.1291—1294.
4. Hum K. Visual pattern recognition by moment invariants. IEEE Trans. Inform. Theory, vol. IT-8, pp. 179—187, 1962.
5. Ruanaidh J.O. and Pun T. Rotation, Scale and translation invariant spread spectrum digital image watermarking. Signal processing, Vol.9, no 6, pp. 1123—1129. October 2000.
6. Choong-Hoon Lee, Heung-Kyu Lee. "Image watermarking resistant to combined geometric and removal attacks," International Journal of Image and Graphics, vol. 5, No. 1 pp. 1—29, 2004.
7. Dong Zheng, Yan Liu, Jiying Zhao, Abdulmotaleb E. Saddik. A survey of RST invariant image watermarking algorithms. ACM Comput. Surv., Vol. 39, No. 2. 2007, pp. 137—153.