Метод защиты изображений от изменений с возможностью восстановления наиболее значимых фрагментов

О.А. Спиридонова[1], В.А. Федосеев[1,2]

[1]Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34А, Самара, Россия, 443086
[2]Институт систем обработки изображений РАН - филиал ФНИЦ «Кристаллография и фотоника» РАН, Молодогвардейская 151, Самара, Россия, 443001

Аннотация. В работе предлагается метод защиты изображений от несанкционированных локализованных изменений с возможностью приближённого восстановления наиболее значимых фрагментов, которые автоматически выбираются на предварительном этапе. Защита осуществляется за счёт встраивания полухрупких цифровых водяных знаков, которые позволяют построить маску изменений, а также содержат информацию, необходимую для восстановления искажённого изображения. Благодаря должному выбору системы встраивания ЦВЗ, а также порядка кодирования данных, предложенный метод позволяет сохранить защитный водяной знак при кадрировании изображения, а также при сжатии его алгоритмом JPEG. В качестве примера рассмотрено применение разработанного метода для защиты изображений дорожной обстановки от несанкционированной корректировки регистрационных номеров попавших в кадр автомобилей. Результаты апробации метода показали его работоспособность для решения заявленных задач.

1. Введение

Проблема аутентификации (проверки подлинности) изображений, чрезвычайно актуальная в наши дни [1], может состоять в решении следующих задач (по мере усложнения) [2, 3]:

1) определение факта искажений в изображении,
2) определение объёма внесенных искажений,
3) локализация искажений,
4) восстановление исходного содержимого искаженных областей.

В настоящей работе рассматривается метод решения последней, самой сложной задачи. Для этого применяется методика активной защиты изображения с использованием цифровых водяных знаков (ЦВЗ). В большинстве систем аутентификации изображений, использующих ЦВЗ, водяной знак содержит лишь информацию, необходимую для локализации искажений. Лишь редкие системы [4-6] предполагают возможность встраивания в качестве водяного знака данных, необходимых для восстановления возможных искажений. При этом, как правило, в изображение встраивается его закодированная копия низкого разрешения. Однако в этом случае есть риск потерять важные детали.

Поэтому в настоящей работе мы исходим из того, что на изображении есть содержательно значимые области, которые необходимо защитить от изменений в первую очередь. К таким областям могут относиться лица и фигуры людей (в основном, переднего плана), детали их одежды, примечательные приметы, облегчающие геолокацию съёмки, и пр. Как правило, значимость тех или иных фрагментов изображения определяется характером съёмки и возможной мотивацией злоумышленника. В данной работе для примера рассматривается съёмка дорожной обстановки камерой наблюдения или видеорегистратором, и поэтому в роли наиболее значимых областей рассматриваются автомобильные номера. Очевидно, что если подобное изображение используется для расследования правонарушения, то небольшая искусственная коррекция зоны номерного знака может иметь далеко идущие последствия. При этом, если мы будем защищать такое изображение водяным знаком, содержащим копию всего изображения низкого разрешения, при восстановлении знак может оказаться неразборчивым.

Поэтому в настоящей работе используется иной подход: в ЦВЗ включаются только предварительно выделенные значимые области, что позволяет сохранить их в более высоком качестве.

Чтобы метод защиты изображения был применим на практике, необходимо обеспечить его стойкость к типовым операциям, которые могут применяться к изображению без цели умышленного искажения локальной области. В настоящей работе в качестве таких операций мы рассмотрим кадрирование изображения с последующим сжатием в формате JPEG. В предлагаемом методе стойкость к ним обеспечивается свойствами базовой системы встраивания ЦВЗ, а также порядком распределения встраиваемой информации по пространству изображения.

2. Описание предлагаемого метода

Как отмечалось выше, в качестве значимых областей в данной работе рассматриваются области регистрационных номеров автомобилей. Для их локализации разработан ряд эффективных методов, например, [7, 8]. Для исследований в рамках настоящей работы мы использовали собственный алгоритм, основанный на локальных направленных фильтрах.

Ввиду требования стойкости встраиваемой защитной информации к JPEG-сжатию, для встраивания ЦВЗ выберем полухрупкую систему, инвариантную к сжатию JPEG в диапазоне значений параметра качества QF выше выбранной пороговой величины QF_1. Таким свойством обладает ряд систем, например, [4, 5, 9]. Подробный обзор и сравнительное исследование этих и других подобных систем содержится в статье [10]. Как показано на рисунке 1, их схема во многом повторяет основные этапы сжатия JPEG [11]: разделение на блоки размером 8×8, блочное дискретное косинусное преобразование, за которыми следует квантование с внесением дополнительной информации (ЦВЗ). Вслед за этим осуществляется возврат к исходному представлению.

Ещё одна ключевая характеристика, обусловливающая выбор ЦВЗ-системы, – это возможность встраивать большое число бит информации в один блок. При базовых настройках ни одна из систем [4, 5, 9] не позволяет встроить более 10 бит, в то время как принципиально желательно иметь возможность встроить до 30-35 бит, чтобы уменьшить число блоков 8×8, содержащих встроенные фрагменты значимых областей, а также закодировать эти фрагменты с более высоким качеством. В работе [10] описан метод выбора дополнительных коэффициентов ДКП в блоке для встраивания большего числа бит, обеспечивающий наилучшее качество результирующего изображения. С его помощью можно встроить произвольное число бит информации в каждый блок от 1 до 63. Разумеется, повышение этого значения приводит к ухудшению качества защищённого изображения.

Для единообразия будем формировать встраиваемую информацию о значимых областях тоже как архив JPEG: то есть делить их на блоки 8×8 и сжимать до определённого показателя качества QF_2. В следующем разделе экспериментальным путём определяется допустимый уровень QF_2 для выделенных информативных фрагментов.

Принцип предлагаемого алгоритма состоит в том, чтобы сжатое содержимое блоков значимых областей встраивать как ЦВЗ в менее значимые блоки. Очевидно, что даже сжатый

блок всё равно не может быть гарантированно представлен 10-20 битами в приемлемом качестве (с учётом необходимости встраивания вспомогательной информации), поэтому содержимое одного блока делится на фрагменты фиксированной длины I_{info} бит, каждый из которых встраивается в другой блок, не относящийся к области номерного знака (см. иллюстрацию этого подхода на рисунке 2).

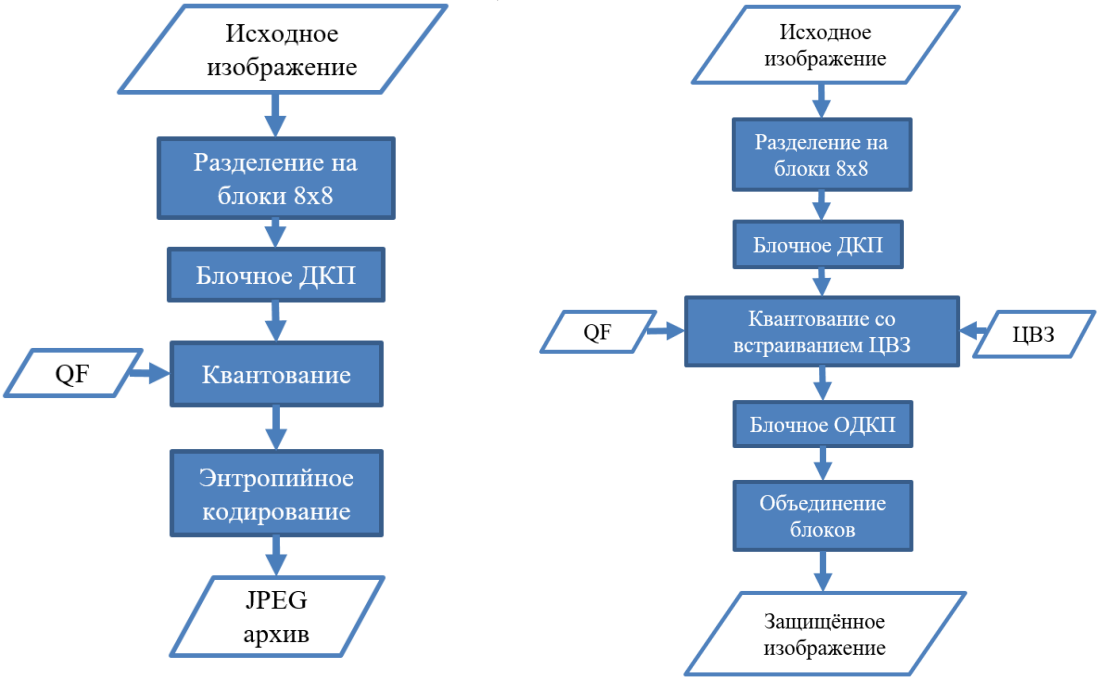

Рисунок 1. Схема сжатия JPEG (слева) и адаптированной к JPEG ЦВЗ-системы (справа).

Рисунок 2. Иллюстрация смещения частей закодированной информации из блока.

Для идентификации местоположения к фрагменту необходимо добавить его индекс в кодируемом блоке, для чего потребуются дополнительные I_k бит, а также смещение закодированного блока относительно того, в который осуществляется встраивание, для чего необходимо отвести ещё I_{shift} бит. Наконец, ещё I_{check} бит отводится для встраивания проверочных бит, определяемых на основе ключа и известных на этапе аутентификации изображения. Они нужны для проверки наличия несанкционированных изменений в текущем блоке. Если извлечённые проверочные биты не совпадают с известными, значит текущий блок признаётся искажённым, и извлечение встроенной в него информации о других блоках не производится. Очевидно, что должно быть выполнено следующее неравенство:

$$I_{info} + I_{shift} + I_k + I_{check} < 63.$$

Причём, желательно, чтобы эта сумма была существенно меньше 63 для снижения визуальных искажений.

Отметим, что кодирование не абсолютного, а относительного смещения между блоками вносит вклад в защиту ЦВЗ от кадрирования. Дополнительно для этой цели может осуществляться избыточное встраивание по принципу расширения спектра [12, 3], когда один и тот же фрагмент информации о блоке значимой области встраивается в несколько блоков, находящихся на значительном удалении друг от друга.

Итоговый алгоритм аутентификации изображения с возможностью восстановления значимых фрагментов:

Этап предварительной защиты изображения

Шаг 0. На изображении каким-либо алгоритмом выделяются области регистрационных знаков.

Шаг 1. Строится маска выделенных областей с округлением по сетке 8×8.

Шаг 2. Блоки, попавшие маску, сжимаются алгоритмом JPEG с показателем качества QF_2.

Шаг 3. При помощи секретного ключа формируется псевдослучайная последовательность блоков, не относящихся к найденной маске, в которые будет встраиваться информация из значимых областей; устанавливается соответствие между блоками.

Шаг 4. Для каждого из выбранных ключом блоков формируется собственный встраиваемый ЦВЗ длиной $I_{info} + I_{shift} + I_k + I_{check}$ бит. В остальные блоки будет встраиваться только проверочная информация длиной I_{check} бит. Проверочная информация должна различаться для этих двух типов блоков.

Шаг 5. Осуществляется встраивание сгенерированных ЦВЗ в каждый блок при помощи выбранной полухрупкой системы. При этом используется параметр качества QF_1, обеспечивающий стойкость к JPEG-сжатию.

Этап проверки подлинности принятого изображения

Шаг 1. Извлечение встроенных ЦВЗ-последовательностей из каждого блока.

Шаг 2. Проверка соответствия извлечённых последовательностей одной из двух допустимых. (и заданных секретным ключом). Построение маски изменений на основе результатов проверки.

Шаг 3. Если маска изменений показывает подлинность всех блоков, завершить работу с результатом «Изображение подлинное».

Шаг 4. Восстановить координаты блоков значимых фрагментов, закодированных в виде ЦВЗ. На основе этого сформировать маску значимых областей.

Шаг 5. Если маска изменений не пересекается с маской значимых областей, заверить работу с результатом "Изображение содержит следы изменений, но области регистрационных знаков не затронуты" и выходным результатом в виде маски изменений.

Шаг 6. Для блоков, относящихся к пересечению маски изменений и маски значимых областей, восстановить содержимое из извлечённых ЦВЗ-последовательностей. Завершить работу с результатом "Изображение содержит следы изменений, затронуты области регистрационных знаков" и выходным результатом в виде маски изменений и восстановленного изображения.

3. Анализ допустимого уровня сжатия значимых областей

Для анализа допустимого уровня сжатия QF_2 областей номерных знаков был проведён эксперимент. На первом этапе из потока данных, снятых видеорегистратором, было выделено множество различных фрагментов, содержащих регистрационные знаки. Размеры полученных фрагментов составили от 20 до 43 пикселей по высоте и от 70 до 160 пикселей по ширине. Среди них вручную были отброшены те изображения, на которых номер визуально не распознаётся. Оставшиеся 500 изображений коллекции далее сжимались алгоритмом JPEG с показателями качества $QF = 1,2,\dots,100$. Для каждого показателя качества вычислялась средняя длина двоичной строки архива, приходящаяся на один блок. В результате построен график зависимости длины строки от значения QF (см. рисунок 3).

Помимо этого, оценивалась визуальная различимость символов номера. Наименьшее значение показателя качества, при котором все символы во всех тестовых изображениях оказались различимы, оказалось равным 15. Это значение в дальнейшем использовалось при тестировании всего метода. Согласно рисунку 2, при таком уровне сжатия длина строки в среднем составляет 24,61 бита, однако она недостаточно мала, чтобы поместиться в одном блоке размера 8×8 в качестве ЦВЗ с учётом проверочных бит и информации о смещении.

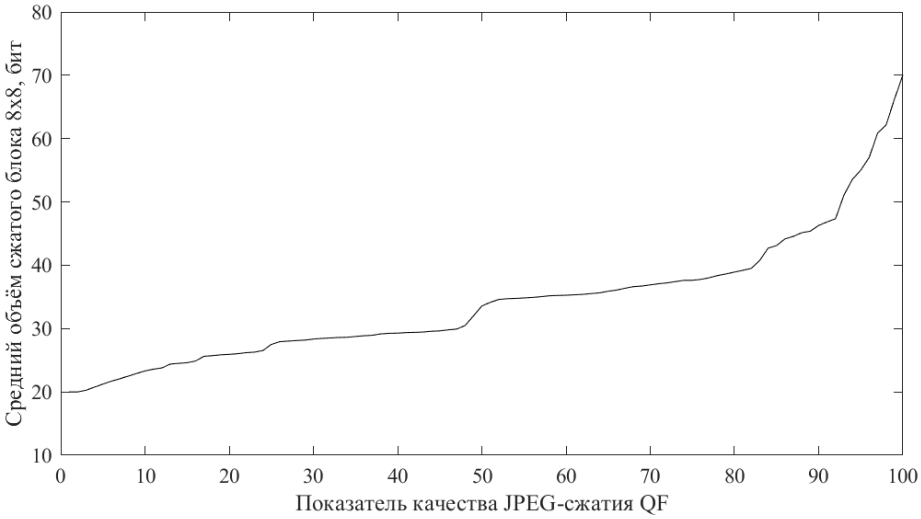

Рисунок 3. Исследование среднего количества информации, требуемого для кодирования одного блока 8×8 в формате JPEG.

4. Апробация предложенного метода

При апробации разработанного метода мы использовали ЦВЗ-систему Preda & Vizireanu [9] и значения, $QF_1 = 70$, $QF_2 = 15$. Фрагменты последовательностей ЦВЗ имели длины $I_{info} = 10$, $I_{shift} = 14$ (по 7 бит на сдвиг по вертикали и горизонтали), $I_k = 2$, $I_{check} = 6$. Последнее число означает, что вероятность пропуска изменённого блока в результате случайного совпадения извлечённой последовательности в данном случае составляет $1/2^6 \approx 0{,}015$. При кодировании области регистрационного номера для цветных изображений использовалась только компонента яркости Y в цветовом пространстве YCbCr.

На рисунке 4 показан пример кодируемого блока, отмеченного на рисунке 2, а в таблице 1 – три ЦВЗ, предназначенных для восстановления этого блока.

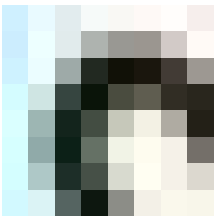

Рисунок 4. Увеличенный блок размера 8×8 из области регистрационного знака.

Таблица 1. Кодирование в виде ЦВЗ блока, изображённого на рисунке 4.

Составная часть ЦВЗ		Строки для кодирования		
		Фрагмент 1	Фрагмент 2	Фрагмент 3
Проверочные биты		‘010100’	‘110101’	‘100011’
Сдвиг блока	Δx	‘0100010’	‘1101110’	‘1111000’
	Δy	‘0101001’	‘0100011’	‘1010110’
Индекс фрагмента блока		‘01’	‘10’	‘11’
Фрагмент блока		‘0000001100’	‘0000000101’	‘1111110000’
Полный вид строки		‘01010001000100101001010000001100’	‘11010111011100100011010000000101’	‘10001111110001010110111111110000’

На рисунках 5-7 показан результат проверки работоспособности метода восстановления искажённой значимой информации. Рисунки показывают, что размытие или полная замена фрагмента не являются помехой для корректного восстановления изображения регистрационного знака из ЦВЗ.

Рисунок 5. Изображение со встроенным защитным ЦВЗ.

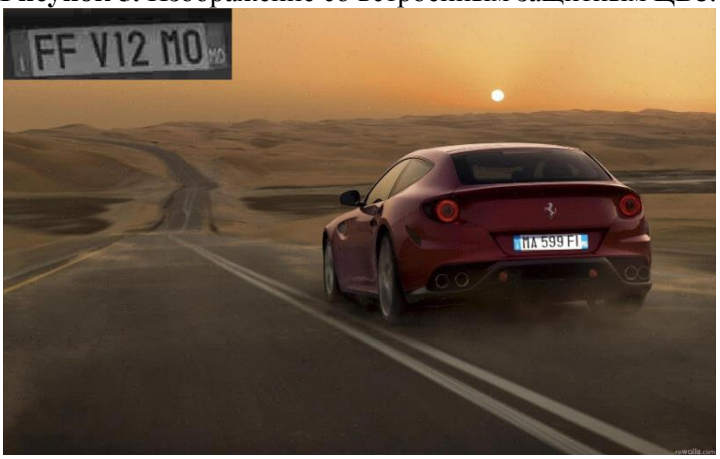

Рисунок 6. Изображение с полностью измененной областью регистрационного знака. В углу укрупнённо показан результат восстановленная.

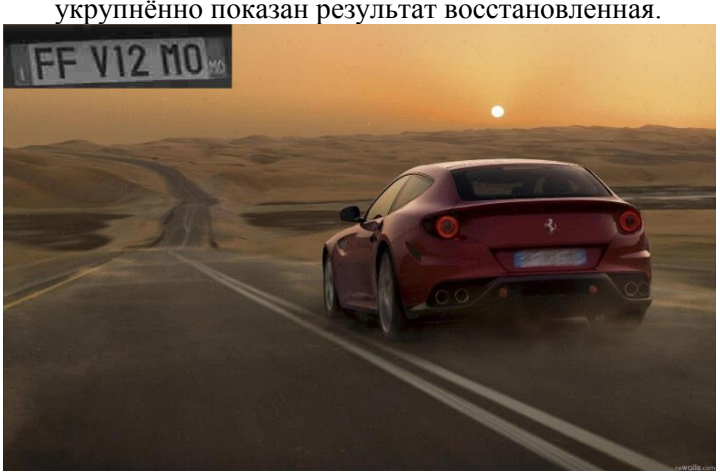

Рисунок 7. Изображение с размытием области регистрационного знака. В углу укрупнённо показан результат восстановленная.

На рисунке 8 укрупненно показаны фрагменты двух примеров изображений с водяным знаком для случаев встраивания его в яркостную компоненту и в компоненту Cr, а также соответствующие им значения PSNR. Эти примеры иллюстрируют, что при встраивании

водяных знаков большого объёма изображения, безусловно, испытывают деградацию, но, во-первых, PSNR всё равно остаётся на приемлемом уровне, а во-вторых, качество изображения может быть улучшено за счёт корректировки метода кодирования или изменения значений его параметров.

Рисунок 8. Визуализация искажений, вызванных встраиванием ЦВЗ: слева – встраивание в компоненту яркости, PSNR=32,69; справа – встраивание компоненту Cr, PSNR=38,83.

5. Заключение

В работе предложен метод защиты изображений от несанкционированных локализованных изменений с возможностью приближённого восстановления наиболее значимых фрагментов. Защита осуществляется за счёт встраивания полухрупких ЦВЗ, которые позволяют построить маску изменений, а также содержат информацию, необходимую для восстановления искажённого изображения. Благодаря должному выбору системы встраивания ЦВЗ, а также порядка кодирования данных, предложенный метод позволяет сохранить защитный водяной знак при кадрировании изображения, а также при сжатии его алгоритмом JPEG. Результаты апробации метода показали его работоспособность для решения заявленных задач. В дальнейшем планируется провести углубленное экспериментальное исследование предложенного метода при различных значениях его параметров, а также осуществить попытку сокращения объёма встраиваемого ЦВЗ с целью снижения визуальных искажений.

6. Благодарности

Исследование выполнено при поддержке РНФ (проект18-71-00052) в части разделов 1-2, 4, а также РФФИ (проект 19-29-09045) в части раздела 3.

7. Литература

[1] Haouzia, A. Methods for image authentication: a survey / A. Haouzia, R. Noumeir // Multimedia Tools and Applications. – 2008. – Vol. 39(1). – P. 1-46. DOI: 10.1007/s11042-007-0154-3.

[2] Cox, I. Digital Watermarking and Steganography: Morgan Kaufmann / I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker – Elsevier, 2008. – 624 p.

[3] Федосеев, В.А. Теоретические основы стеганографии и цифровых водяных знаков: учеб. пособие / В.А. Федосеев, В.А. Митекин – Самара: Издательство Самарского университета, 2017. – 132 с.

[4] Lin, C.-Y. Semifragile watermarking for authenticating JPEG visual content / C.-Y. Lin, S.-F. Chang, 2000. – P. 140-151. DOI: 10.1117/12.384968.

[5] Wang, H. A Novel Fast Self-restoration Semi-fragile Watermarking Algorithm for Image Content Authentication Resistant to JPEG Compression / H. Wang, A. Ho, X. Zhao // Digital Forensics and Watermarking. – 2011. – Vol. 7128. – P. 72-85. DOI: 10.1007/978-3-642-32205-1_8.

[6] Fridrich, J. Images with self-correcting capabilities / J. Fridrich, M. Goljan // Proceedings International Conference on Image Processing (Cat. 99CH36348). – 1999. – Vol. 3. – P. 792-796. DOI: 10.1109/ICIP.1999.817228.

[7] Montazzolli, S. Real-Time Brazilian License Plate Detection and Recognition Using Deep Convolutional Neural Networks / S. Montazzolli, C. Jung // 30th SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI), 2017. – P. 55-62. DOI: 10.1109/SIBGRAPI. 2017.14.
[8] Wang, R. License plate detection using gradient information and cascade detectors / R. Wang, N. Sang, R. Huang, Y. Wang // Optik. – 2014. – Vol. 125(1). – P. 186-190. DOI: 10.1016/ j.ijleo.2013.06.008.
[9] Preda, R.O. Watermarking-based image authentication robust to JPEG compression / R.O. Preda, D.N. Vizireanu // Electronics Letters. – 2015. – Vol. 51(23). – P. 1873-1875. DOI: 10.1049/el.2015.2522.
[10] Егорова, А.А. Классификация и сравнительное исследование систем аутентификации JPEG-изображений, основанных на встраивании полухрупких водяных знаков / А.А. Егорова, В.А. Федосеев // Компьютерная Оптика. – 2019. – Т. 43, № 3. – С. 419-433. DOI: 10.18287/2412-6179-2019-43-3-419-433.
[11] Сэломон, Д. Сжатие данных, изображений и звука – Москва: Техносфера, 2004.
[12] Cox, I.J. Secure spread spectrum watermarking for multimedia / I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon // IEEE Transactions on Image Processing. – 1997. – Vol. 6(12). – P. 1673-1687. DOI: 10.1109/83.650120.

A method for protecting images from changes with informative fragment recovery option

O.A. Spiridonova[1], V.A. Fedoseev[1,2]

[1]Samara National Research University, Moskovskoe Shosse 34A, Samara, Russia, 443086
[2]Image Processing Systems Institute of RAS - Branch of the FSRC "Crystallography and Photonics" RAS, Molodogvardejskaya street 151, Samara, Russia, 443001

Abstract. The paper proposes a method of protecting images from unauthorized localized changes with the possibility of an approximate recovery of the most significant fragments that are automatically selected at the preliminary stage. Protection is provided by embedding semi-fragile digital watermarks, which allow us to construct a mask of changes. The watermark also contains the information necessary to restore a distorted image. Due to the proper choice of the watermarking system, as well as the data encoding order, the proposed method is able to save a protective watermark when cropping the image, as well as when compressing it with the JPEG algorithm. As an example, the application of the developed method for protecting images of the road situation from unauthorized adjustment of car license plate zones is considered. The results of testing the method has shown its efficiency for solving the stated problems.