

УДК 004.056

А.И. Демидчук, Ю.А. Чернявский

## АЛГОРИТМ ПОИСКА В ИЗОБРАЖЕНИЯХ СКРЫТЫХ ДАННЫХ, ВСТРОЕННЫХ МЕТОДОМ КОХА – ЖАО

Дается краткое описание метода стеганографического сокрытия данных Коха – Жао. Описывается алгоритм анализа изображений формата JPEG для установления факта скрытой передачи данных и приводятся результаты применения к тестовому набору изображений.

### Введение

Цифровая стеганография объединяет методы скрытой передачи данных в объектах цифрового вида. Чаще всего в качестве так называемых стеганографических контейнеров используются цифровые данные, содержащие некоторую избыточность информации: изображения, аудио- и видеоданные, хотя также может использоваться обычный текст, файлы и т. д. [1]. При формировании цифровой подписи для объектов интеллектуальной собственности незначительный объем данных встраивается так, чтобы информация сохранялась при различных модификациях объекта. Методы стеганографии могут применяться и для скрытого копирования секретных данных, а также в средствах коммуникации преступных и террористических формирований.

Данная работа посвящена описанию критериев оценки JPEG-изображений на предмет наличия в них скрытой информации, внедренной методом Коха – Жао.

### 1. Метод встраивания Коха – Жао

Жао Цянь и Экхард Кох предложили выполнять встраивание скрываемого сообщения в процессе JPEG-сжатия [2, 3], как показано на рис. 1.

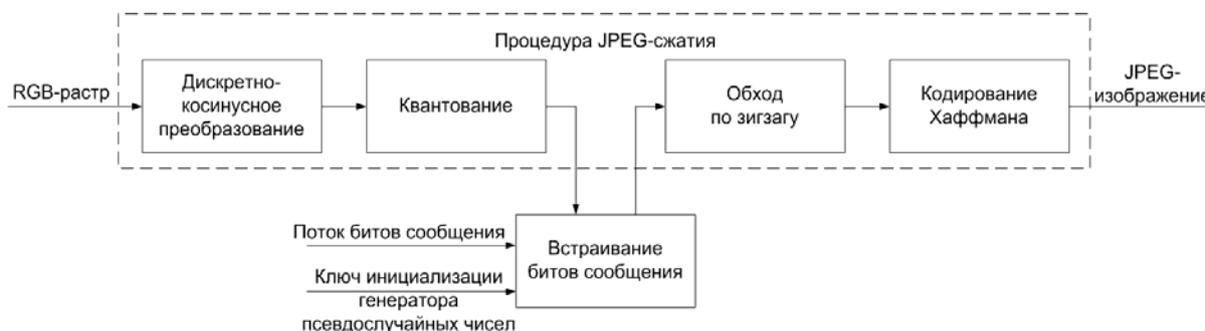


Рис. 1. Встраивание битов сообщения в процессе JPEG-сжатия изображения

На первом этапе выполняется базовая процедура сжатия изображения в JPEG, которая состоит из дискретно-косинусного преобразования (ДКП) блоков пикселей размерностью  $8 \times 8$  и операции квантования. Затем в полученные блоки коэффициентов выполняется встраивание битов скрываемого сообщения и завершается процедура сжатия JPEG.

В методе Коха – Жао для встраивания используются квантованные коэффициенты ДКП, соответствующие области средних частот. Введем следующие обозначения:  $c_i$  –  $i$ -й бит встраиваемого сообщения,  $b$  – блок фрагмента изображения  $8 \times 8$  пикселей,  $B$  – последовательность блоков  $b$ , выбранных псевдослучайным образом.

#### Алгоритм записи (встраивания) данных:

1. Если  $i \geq n$ , где  $n$  – количество битов сообщения, то выход.
2. Выбирается блок  $b$  с использованием генератора псевдослучайных чисел.
3. Если  $b$  находится в  $B$ , то переход к шагу 2; в противном случае добавляется  $b$  к  $B$ .

4. Вызывается функция  $check\_write(b, ci)$  для проверки блока на соответствие критериям допустимости встраивания: если функция возвращает FALSE (т. е. блок не удовлетворяет выдвинутым условиям), то переход к шагу 2.

5. Вызов функции  $write(b, ci)$  для встраивания бита  $ci$  в блок  $b$ .

6. Увеличение  $i$ , переход к шагу 1.

Номера элементов блока  $b$ , которые соответствуют области средних частот и для которых вычисляются коэффициенты ДКП, представлены на рис. 2. Здесь  $k$  и  $l$  – индексы элементов блока  $b$  по вертикали и горизонтали соответственно, для которых измеряются коэффициенты ДКП. Эти индексы изменяются в диапазоне  $[0, 7]$  для случаев сжатого изображения.

				$l$				
	0	1	2	3	4	5	6	7
0			2	3				
1		9	10	11				
2	16	17	18					
$k$ 3								
4								
5								
6								
7								

Рис. 2. Область встраивания

Обозначим  $m \in \{2, 3, 9, 10, 11, 16, 17, 18\}$  индекс коэффициента в области средних частот (выделена серым цветом на рис. 2), которая предложена для встраивания битов сообщения. Бит секретного сообщения встраивается путем модификации отношений трех квантованных коэффициентов в каждом подходящем блоке. Отношения между выбранными коэффициентами делятся на три группы (рис. 3), представляющие закодированные '0', '1' и недействительные комбинации.

	$(k_1, l_1)$	$(k_2, l_2)$	$(k_3, l_3)$	
	$H$	$M$	$L$	} Представление '1'
	$M$	$H$	$L$	
	$H$	$H$	$L$	
	$M$	$L$	$H$	} Представление '0'
	$L$	$M$	$H$	
	$L$	$L$	$H$	} Недопустимое представление
	$H$	$L$	$M$	
	$L$	$H$	$M$	
	$M$	$M$	$M$	

Рис. 3. Кодирование отношений трех коэффициентов, выбранных псевдослучайно из области встраивания

Символы  $H$ ,  $M$ ,  $L$  обозначают соответственно большее, среднее и меньшее значения коэффициента.

**Алгоритм проверки допустимости использования блока  $b$  для записи бита  $ci$  при реализации функции  $check\_write(b, ci)$ :**

1. С использованием заранее заданного ключа псевдослучайным образом выполняется выбор трех позиций элементов для блока  $b$  по ранее заданной таблице позиций. Они именуется  $m_1$ ,  $m_2$  и  $m_3$ .

2. К блоку  $b$  применяется ДКП и квантование с показателем качества сжатия  $Q$ . Параметрами  $YQ(m_1)$ ,  $YQ(m_2)$ ,  $YQ(m_3)$  обозначим квантованные коэффициенты в указанных позициях.

3. При встраивании бита  $ci = 1$  проверяем условие: если  $\text{MIN}(|YQ(m_1)|, |YQ(m_2)|) + D < |YQ(m_3)|$  (где  $|YQ(m_u)|$  – абсолютное значение коэффициента  $YQ(m_u)$  при  $u \in 1..3$ ,  $\text{MIN}$  –

минимальное значение из двух величин,  $D$  – пороговое значение разности между выбранными коэффициентами), то блок  $b$  помечается как недопустимый:

– блок  $b$  модифицируется в соответствии со значениями для недопустимых комбинаций (рис. 3);

– выполняется операция, обратная квантованию, и обратное ДКП;

– возвращается значение FALSE.

4. При встраивании бита  $ci = 0$  проверяем условие: если  $\text{MAX}(|YQ(m_1)|, |YQ(m_2)|) > |YQ(m_3)| + D$  (где MAX – максимальная величина из двух значений), то блок  $b$  помечается как недопустимый:

– блок  $b$  модифицируется в соответствии со значениями для недопустимых комбинаций (рис. 3);

– выполняется операция, обратная квантованию, и обратное ДКП;

– возвращается значение FALSE.

5. В противном случае возвращается TRUE.

## 2. Метод анализа

Данный метод основан на расчете среднеквадратичного отклонения (СКО) блока ДКП коэффициентов и анализе гистограммы распределения коэффициентов СКО для блоков изображения.

Анализ изображения можно разделить на следующие этапы:

– получение квантованных коэффициентов ДКП;

– проверка случая встраивания с пороговым значением  $D > 1$ ;

– проверка случая встраивания с пороговым значением  $D = 1$ .

## 3. Получение квантованных коэффициентов ДКП

На первом этапе анализа изображение  $Im$  декодируется по алгоритму JPEG и формируется множество квантованных коэффициентов для каждого из компонентов  $Im(Col)$  блоков изображения  $b_{8 \times 8}$ , где  $Col \in \{Y, Cb, Cr\}$  – компонент цвета или яркости. Далее из каждого блока множества  $B_{8 \times 8}$  выбирается по восемь коэффициентов и формируется множество блоков  $B_8 = B_{8 \times 8}(m)$  при  $m \in \{2, 3, 9, 10, 11, 16, 17, 18\}$  (см. рис. 2), в которые согласно описанию метода допустимо встраивание бита информации [2, 3].

## 4. Проверка случая встраивания с пороговым значением $D > 1$

К каждому блоку  $b_8$  из множества  $B_8$  применяется операция вычисления СКО:

$$s = \sqrt{\frac{1}{z-1} \sum_{j=1}^z (x_j - \bar{x})^2}, \quad (1)$$

где  $z = 8$  – количество выбранных согласно алгоритму встраивания коэффициентов ДКП;  $x_j$  –  $j$ -й коэффициент;  $\bar{x}$  – среднее значение коэффициента в анализируемой группе.

Для всех блоков  $B_8$  целого изображения вычисляются СКО и формируется массив коэффициентов среднеквадратичных отклонений  $S$ . Затем на основе полученного множества коэффициентов определяются гистограммы распределения среднеквадратичных отклонений для коэффициентов больше нуля  $H_{STD}(S)$ ,  $S > 0$ . В случае учета нулевых коэффициентов максимум гистограммы будет располагаться в точке 0, так как в рассматриваемых позициях многих блоков ДКП располагаются нулевые значения коэффициентов. Такие блоки согласно алгоритму не участвуют во встраивании битов сообщения.

На рис. 4 приведены примеры гистограмм распределения коэффициентов СКО для пустых изображений и изображений, содержащих скрытую информацию (стегаизображений), при встраивании сообщения по методу Коха – Жао с порогом  $D \in \{1, 2, 3\}$ .

Далее по гистограмме находится максимум, т. е. находится значение СКО, которое чаще всего встречается:

$$s_{max} = \arg \max_s [H_{STD}(s)]. \quad (2)$$

Максимальное значение СКО сравнивается с пороговым значением  $\zeta$ :

$$s_{max} \leq \zeta \Rightarrow Im(Col) \notin \{STEGO\};$$

$$s_{max} > \zeta \Rightarrow Im(Col) \in \{STEGO\}.$$

Если  $s_{max} > \zeta$ , то анализируемый компонент изображения содержит скрытую информацию, в противном случае это обычное изображение.

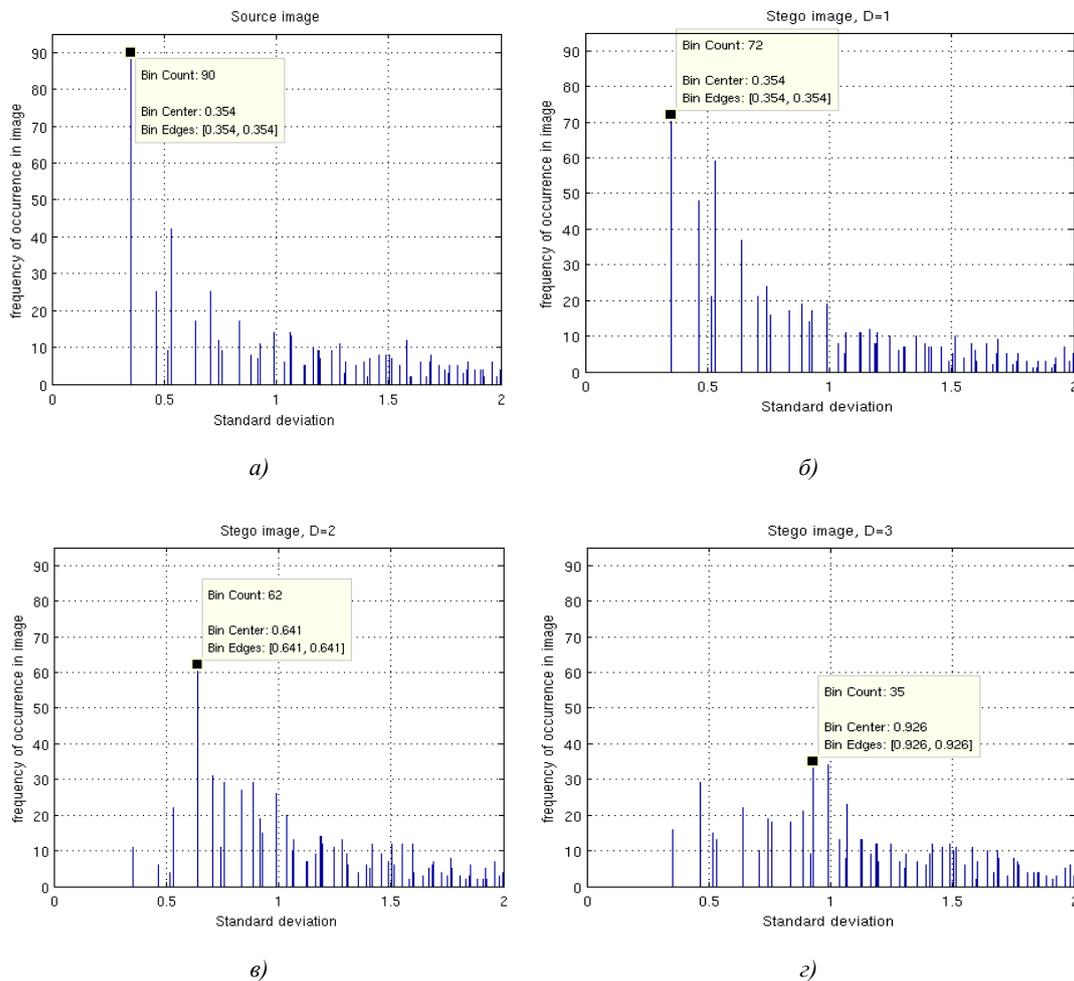


Рис. 4. Гистограммы распределения коэффициентов СКО:  
 а) исходное изображение; б) контейнер заполнен с порогом  $D = 1$ ;  
 в) контейнер заполнен с порогом  $D = 2$ ; г) контейнер заполнен с порогом  $D = 3$

В результате экспериментальных исследований, проведенных более чем для 400 изображений при различных пороговых значениях  $D$  и с разной плотностью заполнения контейнера, определено оптимальное пороговое значение  $\zeta = 0,354$ .

При проведении предварительного тестирования разработанного метода на тестовом множестве получено 100 % правильных результатов анализа стегоизображений, содержащих сообщения, встроенные с пороговым значением  $D \geq 2$  (ошибка второго рода равна 0); для  $D = 1$

эта оценка принимает значение порядка 90–95 %, а для пустых изображений количество ложных срабатываний составляет 5,4 %.

Предварительный анализ полученных результатов (табл. 1) выявил необходимость введения дополнительного ограничивающего условия для более точной оценки возможного встраивания с порогом  $D = 1$ .

Таблица 1  
Результаты оценки ошибок первого и второго рода, %

Величина порога $D$	Этап 1
$D = 0$ (пустой контейнер)	$e1 = 5,4$
$D = 1$	$e2 = 99$
$D = 2$	$e2 = 0$
$D = 3$	$e2 = 0$

*Примечание:*  $e1$  – ошибка первого рода, т. е. оценка отношения ложных срабатываний на пустые изображения к общему числу пустых изображений;  $e2$  – ошибка второго рода, т. е. оценка отношения пропущенных стегоизображений как пустых контейнеров к общему числу поданных на анализ стегоизображений.

### 5. Повышение эффективности анализа. Случай встраивания с пороговым значением $D = 1$

После анализа гистограмм на (см. рис. 4) было предложено применить ко всему анализируемому множеству изображений  $I_{D=1}$  при пороге  $D = 1$  и пустых изображений  $I_0$  следующую оценку:

$$P_{Hmax} = \frac{N_{Smax}}{N} \times 100 \%, \quad (3)$$

где  $N_{Smax} = \max[H_{STD}(s)]$  – максимум гистограммы распределения коэффициентов СКО;  $N$  – общее количество коэффициентов СКО, которое равно количеству блоков изображения  $B_{8 \times 8}$ , переданных на анализ. Эта оценка показывает долю наиболее встречающихся коэффициентов СКО в общем количестве коэффициентов.

Из рис. 5 видно, что для заполненных контейнеров существует пороговое значение  $R = 35$ . При превышении этого значения можно утверждать, что изображение содержит скрытую информацию.

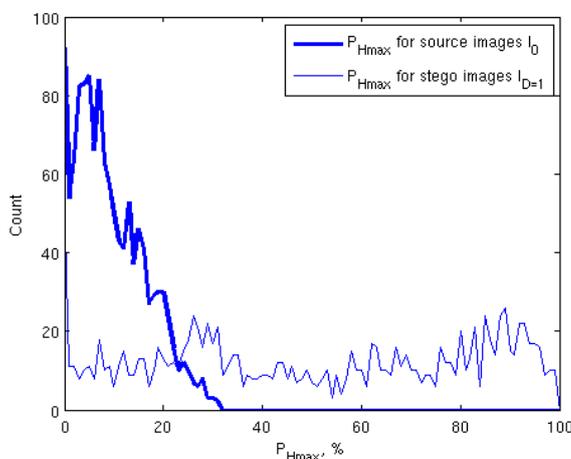


Рис. 5. Гистограммы распределения значений  $P_{Hmax}$  для множеств  $I_0$  и  $I_{D=1}$

Для минимизации влияния статистических колебаний, имеющихся в исследуемой выборке изображений, к полученным значениям функций распределения  $P_{Hmax}$  в диапазоне  $[0, 35]$  была применена операция нахождения аппроксимирующего полинома десятой степени методом наименьших квадратов (рис. 6).

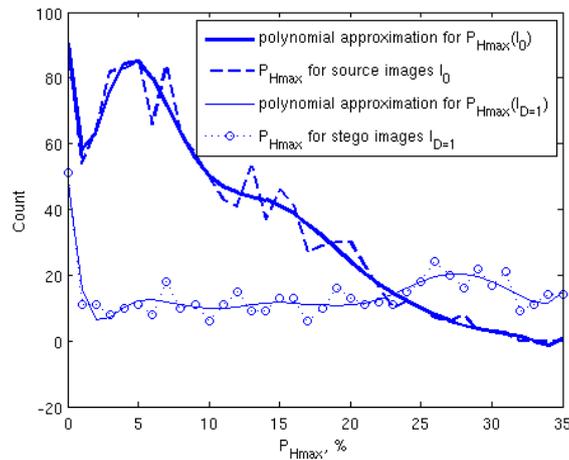


Рис. 6. Аппроксимированная часть гистограммы в диапазоне  $[0, 35]$

При условии, что отношение  $P_{Hmax}$  находится в диапазоне  $[0, R]$ , изображение содержит скрытую информацию с вероятностью, которая определяется отношением количества  $\text{Count}(P_{Hmax, D=1})$  стегоконтейнеров из тестового набора изображений с  $D = 1$  к общему числу изображений с данным значением  $P_{Hmax}$ :

$$P_s = \frac{\text{Count}(P_{Hmax, D=1})}{\text{Count}(P_{Hmax, D=1}) + \text{Count}(P_{Hmax, 0})}. \quad (4)$$

Применяя формулу (4) к статистическим данным (см. рис. 6), для исследуемого изображения строится график зависимости вероятности появления скрытой информации от параметра  $P_{Hmax}$  (рис. 7).

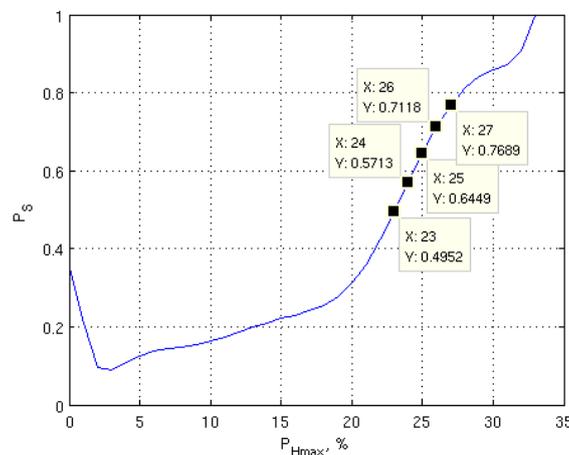


Рис. 7. График зависимости вероятности появления скрытой информации в изображении от значения  $P_{Hmax}$

График на рис. 7 позволяет сделать следующий вывод. Изображение с вероятностью  $P_S = 0,65$  содержит скрытое сообщение, если  $P_{Hmax} = 25\%$ . Чем выше величина  $P_{Hmax}$ , тем выше вероятность того, что в изображение была встроена информация.

## 6. Результаты

В качестве тестового набора были использованы 418 изображений с различным разрешением от  $384 \times 288$  до  $3089 \times 2084$  (набор  $I_0$ ). Для формирования множества контейнеров, содержащих скрытые изображения, к каждому изображению применялась процедура встраивания информации методом Коха – Жао последовательности данных, полученных с генератора псевдослучайных чисел. Встраивание производилось отдельно в каждый компонент цветовой схемы. Контейнеры заполнялись на 100 % при пороговых значениях  $D = 1, 2, 3$ . Каждое из множеств состояло из 418 изображений. Эффективность различных методов стегоанализа оценивалась определением ошибок первого рода  $e1$  и второго рода  $e2$ .

Для сравнения в табл. 2 приведены результаты оценки встраивания информации на тестовых наборах изображений методами стегоанализов OutGuess и JPHide, входящих в состав программы Stegetect [4], которые также применяются для оценки JPEG-изображений. В состав Stegetect входят методы оценки встраивания информации JSteg, Invisible Secrets и F5. Однако результаты анализа тестовых наборов изображений для этих методов в таблицу не включены, так как их применение не выявило ни одного встраивания.

Таблица 2  
Результаты сравнения эффективности анализа стегоконтейнеров, %

Порог встраивания	OutGuess	JPHide	Анализ Коха – Жао
$D = 0$	$e1 = 0,2$	$e1 = 2,2$	$e1 = 5,4$
$D = 1$	$e2 = 99,5$	$e2 = 97,8$	$e2 = 15,6$
$D = 2$	$e2 = 100$	$e2 = 94,5$	$e2 = 0$
$D = 3$	$e2 = 100$	$e2 = 94,5$	$e2 = 0$

## Заключение

Предложенный критерий оценки изображений для выявления наличия встроеной информации методом Коха – Жао в JPEG-изображения дает высокий показатель (порядка 90 %) верных результатов в том случае, если встраивание выполнялось с порогом более единицы. Оценка с порогом встраивания  $D = 1$  дает результат с большей ошибкой второго рода. Для пустых контейнеров ошибка первого рода примерно равна 20 %.

Таким образом, использование предложенных критериев оценки изображения в формате JPEG на предмет определения наличия скрытой информации методом Коха – Жао при определенных условиях обеспечивает эффективное решение задач стегоанализа. По сравнению с существующими методами, ориентированными на другие алгоритмы встраивания, значительно повышается достоверность анализа.

Дальнейшее повышение показателя достоверности анализа также может быть достигнуто путем выполнения автоматической классификации изображений по плотности контрастных переходов с использованием для каждого из них отдельного порогового значения.

## Список литературы

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.
2. Zhao, J. Embedding Robust Labels into Images for Copyright Protection / J. Zhao, E. Koch // Proc. of the Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies. – Munich, Vienna, 1995. – P. 242–251.

3. Zhao, J. Towards Robust and Hidden Image Copyright Labeling / J. Zhao, E. Koch // IEEE Workshop on Nonlinear Signal and Image Processing. – Greece, 1995. – P. 123–132.

4. OutGuess [Electronic resource]. – Mode of access : <http://www.outguess.org>. – Date of access : 11.12.10.

**Поступила 10.11.11**

*Белорусский государственный университет  
информатики и радиоэлектроники,  
Минск, П. Бровка, 6  
e-mail: demidchuk.aleksey@gmail.com,  
chernyavskiy@academy.edu.by*

**A.I. Demidchuk, Y.A. Chernyavskiy**

**AN ALGORITHM FOR DETECTING IMAGES WITH HIDDEN DATA  
EMBEDDED WITH KOCH – ZHAO STEGANOGRAPHIC METHOD**

This paper provides a brief description of the steganographic data hiding technique suggested by Koch – Zhao. It describes the algorithm of analysis of images in JPEG format to establish the fact of hidden communication and the results of application to a test set of images. The result allows to recommend this method for primary selection of files for subsequent detailed analysis.