ЦИФРОВАЯ СТЕГАНОГРАФИЯ В ГРАФИЧЕСКИХ ФАЙЛАХ

Влацкая И.В., канд. техн. наук, доцент, Зубаиров С.И.
Оренбургский государственный университет

Стеганография – наука и искусство о скрытой передаче информации путем сохранения в тайне самого факта передачи. Термин ввел Иоганн Тритемий, ученый, теолог, алхимик и оккультист, в своем труде «Стеганография». Стеганография имеет свое место в обеспечении безопасности: она не исключает криптографию, а дополняет её. Информация, скрытая средствами стеганографии сильно снижает вероятность обнаружения факта самой передачи, а если скрываемое сообщение было еще и зашифровано, то это уже иной, более высокий уровень защиты.

Существуют несколько направлений стеганографии, а именно:

– Классическая стеганография;

– Компьютерная стеганография – одно из направлений классической стеганографии, использующее специальные свойства компьютерных форматов данных;

– Цифровая стеганография – одно из направлений классической стеганографии, основанное на сокрытии информации в цифровых объектах, приводящее к их искажению. Обычно эти искажения незаметны для человека, так как находятся за пределами чувствительности.

Последнее направление было выбрано в качестве рассмотрения в данной работе, а именно цифровая стеганография в изображениях.

Среди всех методов для сокрытия информации в изображениях выделяются следующие:

– Скрытие данных в пространственной области изображения: данные внедряются в области исходного изображения, поэтому отсутствуют сложные вычислительные операции;

– Скрытие данных в частотной области изображения: наиболее известные методы – на основе ДКП (дискретного косинусного преобразования) и вейвлет-преобразования, так как они используются при сжатии изображений с потерями. Использование метода с преобразованием, которому будет подвергаться изображение со временем, повышает его стойкость к искажениям. В данной работе применяется метод на основе ДКП, так как в дальнейшем изображение подвергается JPEG-компрессии, а именно метод относительной замены величин коэффициентов ДКП - метод Коха и Жао.

Суть метода Коха и Жао состоит в изменении отношения между абсолютными значениями коэффициентов ДКП в среднечастотной области изображения. На первом шаге мы должны разбить исходное изображение на блоки 8*8 пикселей, а именно выделить компоненту B (синий цвет), цветовой схемы RGB (см. рисунок 1).

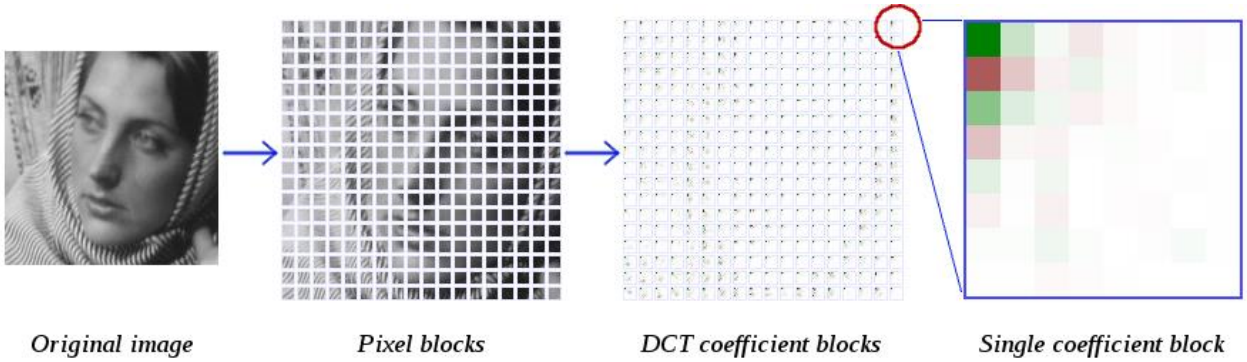

Рисунок 1 – Получение коэффициентов ДКП

Выбирается именно B-компонента пикселя, так как человеческий глаз менее чувствителен к изменениям синего цвета. Для получения коэффициентов ДКП применяется формула (см. рисунок 2).

$$\Omega(\upsilon,\nu)=\frac{\zeta(\upsilon)\cdot\zeta(\nu)}{\sqrt{2N}}\cdot\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}C(x,y)\cdot\cos\left[\frac{\pi\cdot\upsilon\cdot(2x+1)}{2N}\right]\cdot\cos\left[\frac{\pi\cdot\nu\cdot(2y+1)}{2N}\right]$$

Рисунок 2 – Формула получения коэффициентов ДКП

Где Ω(u,v) – коэффициент ДКП, C(x,y) – элемент оригинального изображения размерностью N*N; x,y – пространственные координаты пикселей изображения; u,v – координаты в частотной области; если x = 0 □(x) = 1/√2, иначе □(x) = 1.

Для восстановления B-компоненты используется формула (см. рисунок 3).

$$S(x,y)=\frac{1}{\sqrt{2N}}\cdot\sum_{\upsilon=0}^{N-1}\sum_{\nu=0}^{N-1}\zeta(\upsilon)\cdot\zeta(\nu)\cdot\Omega(\upsilon,\nu)\cdot\cos\left[\frac{\pi\cdot\upsilon\cdot(2x+1)}{2N}\right]\cdot\cos\left[\frac{\pi\cdot\nu\cdot(2y+1)}{2N}\right]$$

Рисунок 3 – Формула восстановления компоненты цвета пикселя из коэффициентов ДКП

Где S(x,y) – элемент восстановленного по коэффициентам ДКП изображения, Ω(u,v)– коэффициент ДКП; x,y – пространственные координаты пикселей изображения; u,v – координаты в частотной области; если x = 0 □(x) = 1/√2, иначе □(x) = 1.

Среднечастотная область выбирается, так как встраивание в ВЧ приводит к гарантированному разрушению при JPEG компрессии, а встраивание в НЧ

приводит к видимым искажениям изображения. На рисунке СЧ область выделена жирным шрифтом (см. рисунок 4).

-603	203	11	45	-30	-14	-14	**-7**
-108	-93	10	49	27	6	**8**	**2**
-42	-20	-6	16	17	**9**	**3**	3
56	69	7	-25	**-10**	**-5**	-2	-2
-33	-21	17	**8**	**3**	-4	-5	-3
-16	-14	**8**	**2**	-4	-2	1	1
0	**-5**	**-6**	-1	2	3	1	1
9	**5**	-6	-9	0	3	3	2

Рисунок 4 – Блок коэффициентов ДКП 8*8

Информация встраивается побитно, причем в один блок b из коэффициентов ДКП 8*8 встраивается только один бит m_b. Выбираются два коэффициента из СЧ области: $\Omega_b(u_1,v_1)$ и $\Omega_b(u_2,v_2)$. Для встраивания нуля добиваются разницы абсолютных значений, большей некоторого значения P, для единицы же – меньше значения –P (см. рисунок 5).

$$\begin{cases} \left|\Omega_b(\upsilon_1,\nu_1)\right| - \left|\Omega_b(\upsilon_2,\nu_2)\right| > P, \text{ при } m_b = 0; \\ \left|\Omega_b(\upsilon_1,\nu_1)\right| - \left|\Omega_b(\upsilon_2,\nu_2)\right| < -P, \text{ при } m_b = 1. \end{cases}$$

Рисунок 5 – Формулы встраивания бита информации

При извлечении информации исходим из неравенств (см. рисунок 6).

$$\begin{cases} m_b^* = 0, \text{ при } \left|\Omega_b^*(\upsilon_1,\nu_1)\right| > \left|\Omega_b^*(\upsilon_2,\nu_2)\right|; \\ m_b^* = 1, \text{ при } \left|\Omega_b^*(\upsilon_1,\nu_1)\right| < \left|\Omega_b^*(\upsilon_2,\nu_2)\right|. \end{cases}$$

Рисунок 6 – Формулы для извлечения бита информации

При запуске программы, пользователю доступны две функции: скрытие данных в изображении и извлечение данных из изображения (см. рисунок 7).

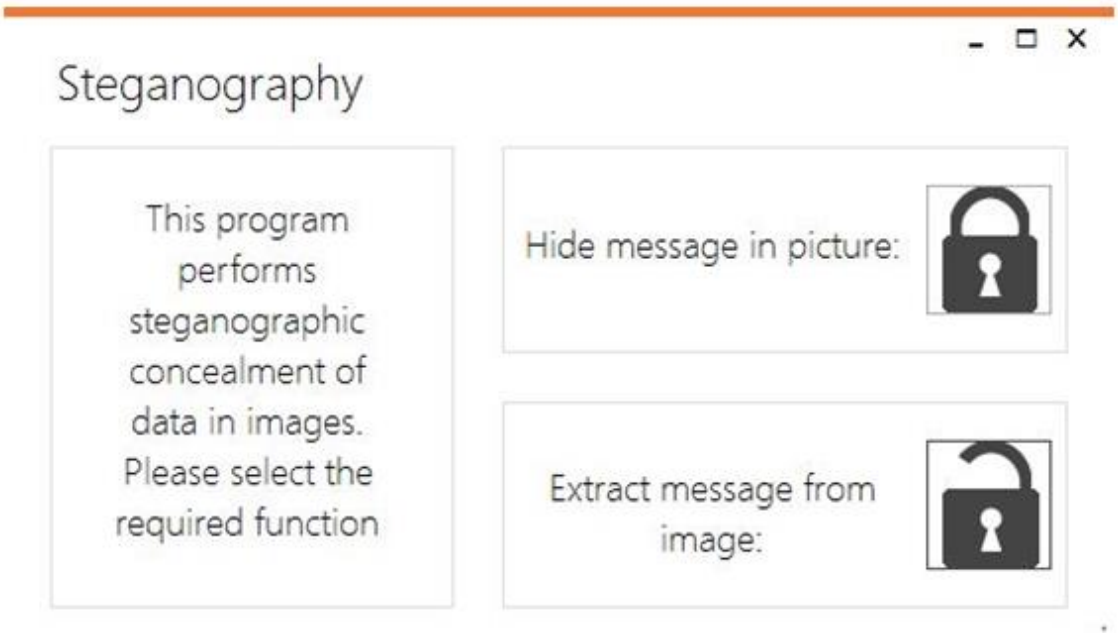

Рисунок 7 – Интерфейс программного средства

При скрытии данных в изображении, пользователь должен выбрать изображение в качестве контейнера для скрытия и ввести сообщение в текстовое поле, пометив окончание сообщения символом *. Под текстовым полем можно

увидеть текущую и максимальную длины сообщений для выбранного изображения. Также имеется возможность сохранения изображения и сброса установок (см. рисунок 8).

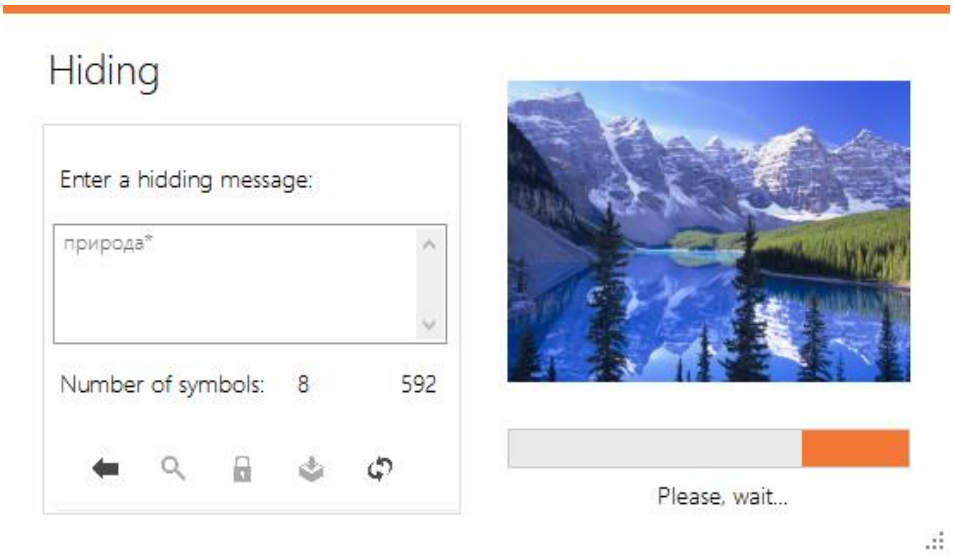

Рисунок 8 – Скрытие данных в изображении

При извлечении данных из изображения, пользователь выбирает изображение со скрытым сообщением. После чего можно запустить процесс извлечения. Также имеется возможность сброса установок (см. рисунок 9).

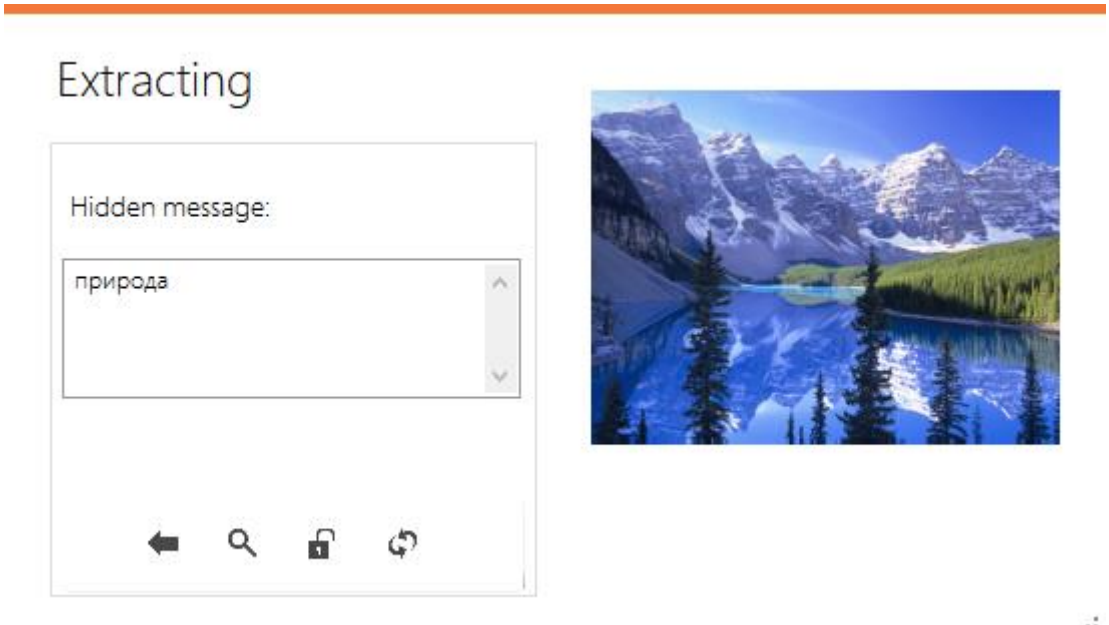

Рисунок 9 – Извлечение данных из изображения

Список литературы

1. *Кохановић Г.Ф., Пузыренко А.Ю.Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко; М.: МК-Пресс, 2006. — 288 с. ISBN: 966-8806-06-9.*
2. *Материалы сайта http://professorweb.ru*
3. *Материалы сайта https://msdn.microsoft.com*
4. *Материалы сайта https://habrahabr.ru*