А. А. Алимов, Г. И. Борзунов, В. Ю. Ефимов

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ СОКРЫТИЯ ДАННЫХ В ВИДЕОПОСЛЕДОВАТЕЛЬНОСТЯХ ФОРМАТА MPEG-2

В ходе исследований были рассмотрены алгоритмы, приведенные в работах [1] и [2]. Алгоритм [1] не предусматривает возможности контроля уровня искажений изображения, что соответственно негативно влияет на незаметность. Кроме того, он обладает ограниченной надежностью в том смысле, что остается возможность ложного обнаружения скрытых данных в том месте, куда их не внедряли. Алгоритм [2] решает проблему неконтролируемых искажений алгоритма [1], но также не имеет защиты от ложного срабатывания. В итоге на основе этих алгоритмов был разработан модифицированный алгоритм, который имеет 2 ключевых параметра $C_{\downarrow}min^{\uparrow}* \in [2,64]$, $D^{\uparrow}* \in [1, +\infty)$. $C_{\downarrow}min^{\uparrow}*$ определяет порог, начиная с которого можно изменять коэффициенты ДКП в сторону увеличения частоты. D^* можно охарактеризовать как величину создаваемого различия между первоначальными значениями коэффициентов и их конечными значениями. Имеется условие для внедрения информации в каждую конкретную пару областей изображения. Для каждой области из этой пары коэффициенты ДКП должны, с учетом ограничения $C_{\downarrow}min^{\uparrow}*$, в совокупности составлять величину, соответствующую D^*. При исследовании модифицированного алгоритма были выполнены тесты на незаметность, стойкость, надежность и количество встраиваемой информации при разных значениях параметров $C_{\downarrow}min^{\uparrow}*$, D^*. Так как незаметность — сугубо субъективный параметр, то введем следующие категории незаметности (см. таблицу 1).

Таблица 1. Категории незаметности

Обозначение	Описание
А	Искажения либо незаметны вообще, либо воспринимаются как потери качества ввиду ограничения скорости видеопотока.
Б	Искажения можно увидеть при изучении кадров по отдельности, воспринимаются как размытость: нечеткость текста, контуров.
В	Искажения заметны при непрерывном просмотре и воспринимаются как сильная размытость.

Результаты исследования незаметности применения алгоритма приводятся в таблице 2. Вычислительный эксперимент показал (см. таблицу 2), что незаметность больше зависит от D^*, чем от $C_{\downarrow}min^{\uparrow}*$.

Таблица 2. Незаметность применения алгоритма при различных $C_{\downarrow}min^{\uparrow}$, $D^{\uparrow}$**

$C_{\downarrow}min^{\uparrow}$* \ $D^{\uparrow}$*	1	5	10	25	50	100
2	А	Б	Б	Б	В	В
5	А	А	А	Б	Б	Б
10	А	А	А	А	А	А
30	А	А	А	А	А	А

Другим важнейшим параметром является количество встроенной информации. Заметим, что при значениях параметров $C_{\downarrow}min^{\uparrow}$*, $D^{\uparrow}$*, соответствующих категории А незаметности, достигается еще и большая удельная скорость внедрения (см. таблицу 3).

Таблица 3. Удельная скорость внедрения информации при различных $C_{\downarrow}min^{\uparrow}$, $D^{\uparrow}$* (байт встроенной информации / мегабайт несущей информации)*

$C_{\downarrow}min^{\uparrow}$* \ $D^{\uparrow}$*	1	5	10	25	50	100
2	102	99	96	90	83	73
5	95	88	83	72	61	48
10	82	69	61	47	36	24
30	44	30	23	14	9	6

Алгоритм имеет достаточно высокую надежность: для всех проведенных тестов при различных комбинациях $C_{\downarrow}min^{\uparrow}$*, $D^{\uparrow}$* внедренная информация в точности соответствовала извлеченной. Однако в файлах, не содержащих стеганограммы, при различных $C_{\downarrow}min^{\uparrow}$*, $D^{\uparrow}$* были обнаружены случайные биты. Эта особенность ложного срабатывания говорит о том, что злоумышленник не сможет быть уверенным в присутствии стеганограммы, извлекая из контейнера некоторые значения $C_{\downarrow}min^{\uparrow}$*, $D^{\uparrow}$* или даже случайно их угадав. Стойкость алгоритма неудовлетворительна: при использовании декодера [3] для комбинаций $C_{\downarrow}min^{\uparrow}$*, $D^{\uparrow}$*, соответствующих категориям А и Б, число считанных бит отклонялось приблизительно на 10 % от количества внедренных бит, и примерно половина считанной информации была неверной. Атака перекодированием оказалась сложнее внедрения информации, хотя теоретически оба алгоритма имеют временную сложность, равную O(n).

СПИСОК ЛИТЕРАТУРЫ:

1. *Langelaar G., Lagendijk R., Biemond J.* Real-time Labeling Methods for MPEG Compressed Video // 18th Symposium on Information Theory in the Benelux. 1997.
2. *Васильева Е.* Цифровая стеганография. 2006. [Электронный ресурс]. URL: http://rain.ifmo.ru/cat/.
3. Format Factory. [Электронный ресурс]. URL: www.formatoz.com.