

УДК 004.056.5

А.А. Яковенко

Одеський національний політехнічний університет, Одеса

**ПОМЕХОУСТОЙЧИВЫЕ СТЕГАНОГРАФИЧЕСКИЕ АЛГОРИТМЫ
НА ОСНОВЕ ДИСКРЕТНОГО КОСИНУСНОГО ПРЕОБРАЗОВАНИЯ**

Проблема анонимности в современных компьютерных сетях в последнее время привлекает все боль-

ше и больше внимания. Наряду с VPN-службами, обеспечивающими анонимность с помощью шифрова-

ния трафика, становятся востребованными службы, осуществляющие стеганографическую обработку информации, при которой скрывается сам факт передачи информации. Наиболее распространены стеганографические алгоритмы, позволяющие организовать скрытый обмен сообщениями, погружая их в передаваемые мультимедийные файлы или потоки.

К существующим стеганографическим алгоритмам предъявляются определенные требования по размеру скрытого сообщения относительно мультимедийного контейнера-носителя, также считается необходимым обеспечение невозможности детектирования скрытого сообщения в носителе без знания секретного ключа. К сожалению, большинство из этих алгоритмов имеют существенный недостаток, связанный с тем, что после некоторой обработки мультимедийного носителя (например, изображения) скрываемая в нем информация либо полностью теряется, либо безвозвратно искажается. Таким образом, производя автоматическую обработку мультимедийных файлов на сетевом узле, можно гарантированно избавиться от угрозы прохождения скрытой информации. Основными типами такой обработки для изображений является: добавление незначительного пиксельного шума, незначительное изменение тоновой кривой, изменение параметров сжатия изображения, а также незначительно масштабирования изображения.

Среди алгоритмов, разработанных специально для того, чтобы противостоять удалению скрываемой информации, можно выделить классы, способные противостоять добавлению шума и модификации тоновой кривой. На данный момент алгоритмы, позволяющие сохранять скрытое сообщение при повторном сжатии изображения и произвольном изменении его размеров, малочисленны и имеют сильные ограничения.

Предлагается алгоритм внедрения скрытой информации в изображения, основанный на дискретном косинусном преобразовании (ДКП). В то время, как в широко распространенных стандартах сжатия изображений используются блоки ДКП фиксированного размера (обычно 8x8 пикселей), в предлагаемом алгоритме дискретному косинусному преобразованию подвергается либо макроблок изображения, содержащий 2^{2n} блоков ДКП, либо все изображение.

С одной стороны, подсчет ДКП для больших блоков – довольно сложная с вычислительной точки зрения задача. С другой стороны – в результате преобразования изображение представляется в виде коэффициентов ДКП, некоторые из которых остаются неизменными при изменении параметров сжатия изображения. Например, все коэффициенты ДКП, отвечающие за пространственные частоты меньше 8-ми пикселей в периоде, остаются неизменными, независимо от того, какие настройки сжатия JPEG используются. Это позволяет произвести внедрение информации, которая будет сохраняться в изображении носителя, независимо от того, с какими настройками это изображение будет подвергаться повторному сжатию.

При использовании макроблока размером с изображение, некоторая часть низкочастотных коэффициентов ДКП остается неизменной, независимо от параметров изменения размеров изображения. Таким образом, информация, внедренная в эти коэффициенты, остается неизменной даже при изменении пиксельных размеров изображения.

Таким образом, разработаны алгоритмы, позволяющие производить внедрение скрытого сообщения, которое не удаляется из изображений-носителей при изменении настроек их сжатия, а также при их масштабировании в некоторых пределах.