Применение стеганографии в системах видеоконференции.

Аннотация.

В работе описана стеганографическая система, которая позволяет встраивать информацию в потоковое видео с целью ее скрытной передачи. Метод сокрытия данных основан на изменении коэффициентов дискретного косинусного преобразования (ДКП), используемого при сжатии с потерями.

Методы стеганографии позволяют скрытно передавать данные, при этом тайной является сам факт существования такого сообщения. Скрываемое сообщение встраивается в некоторый безобидный, не привлекающий внимание объект (стегоконтейнер). Затем этот объект открыто транспортируется адресату. Наиболее популярными стегоконтейнерами являются аудиозаписи, изображения и видео.

Дискретное косинусное преобразование используется во многих популярных стандартах кодирования видео: MPEG-2 (примеры таких алгоритмов приведены в [1]), MPEG-4, H.261. В настоящей работе приведен метод внедрения информации в видео, сжимаемое по стандарту H.261, являющемуся наиболее распространенным стандартом сжатия в системах видеоконференции и рекомендованным Comite Consultatif International Telegraphique et Telephonique (CCITT)[2].

В [3] приведено описание ДКП при сжатии видеопоследовательностей. Каждый кадр передаваемого видео разбивается на блоки размером 8*8 пикселов. Блок можно представить в виде матрицы, элементами которой являются 64 целочисленных коэффициента ДКП. Многие из коэффициентов равны нулю, особенно высокочастотные. Коэффициент ДКП с индексом (0,0) содержит информацию о яркости блока. Он называется коэффициентом постоянного тока, и представляет среднее значение по блоку пикселов. Другие коэффициенты ДКП являются коэффициентами переменного тока. Коэффициенты f(k,n) ДКП вычисляются по формуле (1), где F(x,y) – значение яркости блока.

$$f(k,n)=\frac{C(k)\cdot C(n)}{2}\sum_{x=0}^{7}\sum_{y=0}^{7}F(x,y)\cos(\frac{p(2x+1)k}{16})\cos(\frac{p(2y+1)k}{16}) \qquad (1)$$

Обратное преобразование происходит по формуле

$$F(x,y)=\frac{C(k)\cdot C(n)}{2}\sum_{k=0}^{7}\sum_{n=0}^{7}f(k,n)\cos(\frac{p(2x+1)k}{16})\cos(\frac{p(2y+1)k}{16}) \qquad (2)$$

$$F(x,y)=\frac{C(k)\cdot C(n)}{2}\sum_{k=0}^{7}\sum_{n=0}^{7}f(k,n)B_{k,n}(x,y), \qquad (3)$$

где $B_{k,n}(x,y)$ – базовые изображения ДКП (см. рис 1)

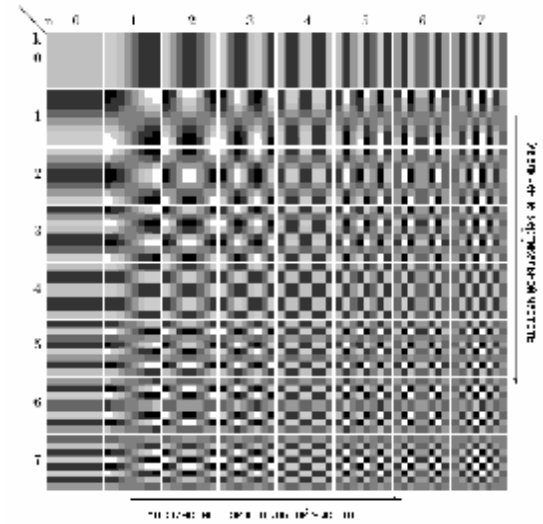

рис. 1 – Базовые изображения ДКП

ДКП концентрирует энергию в области низких частот, а так как человеческий глаз менее чувствителен к высокочастотным колебаниям, то ВЧ компоненты могут быть оцифрованы более грубо. Возникающие при этом погрешности округления можно использовать стеганографических целях. Так, в работе [4] приведен алгоритм внедрения цифрового водяного знака в изображение в области ДКП, не вносящий значительных искажений в исходное изображение.

Очевидно, что замена в формуле (1) выражения 2y+1 на 2y+1.2 эквивалентно небольшому сдвигу по горизонтали базового изображения $B_{k,0}$ при восстановлении исходного кадра. Опыты показали, что возникающие при этом изменения изображения практически не заметны для человеческого глаза. В результате этой замены мы переходим от матрицы с элементами {f(k,n)} к матрице с элементами {f(k’,n’)}.

Для любого n>0 верны соотношения:

$$k'=k,\ n'=n-1,\ \Delta(f(k,n))=\left|f(k,n)-f(k',n')\right|, \qquad (4)$$

$$\frac{\Delta(f(k,n))}{f(k,n)} \approx n \cdot 3\% \quad (5)$$

Так как коэффициенты ДКП являются целыми числами, то изменение коэффициента ДКП не может быть меньше единицы (то есть, из $\Delta(f(k,n)) \neq 0 \Rightarrow \Delta(f(k,n)) \geq 1$).

Алгоритм.

1. Встраивание сообщения. В данном алгоритме в каждый блок с номером (i) размера 8*8 осуществляется встраивание не более одного бита стегосообщения.

На первом шаге определяется, является ли рассматриваемый блок (i) «подходящим» для встраивания стегосообщения. Блок является «подходящим», если они содержат коэффициенты ДКП f(k,n), для которых выполнено соотношение

$$\Delta(f(k,n)) = f(k,n) \cdot 3\% \cdot n \geq 1. \quad (6)$$

Если таких коэффициентов в блоке несколько, то среди них выбирается наибольший (выбранный коэффициент обозначим через $f_i(\max)$).

Далее для «подходящего» блока (i) вычисляется значение «четности» (сумма всех коэффициентов блока по модулю 2). Если «четность» блока равна знаку бита скрываемого текста, то такой блок передается неизменным. Иначе четность блока меняется на противоположную, за счет изменения значения коэффициента $f_i(\max)$ по формуле:

$$f_i(\max) = \begin{cases} f_i(\max) - 1, & f_i(\max) > 0 \\ f_i(\max) + 1, & f_i(\max) < 0 \\ 1, & f_i(\max) = 0 \end{cases}. \quad (7)$$

Ключом, позволяющим извлечь скрытое сообщение, является вектор первоначальной четности блоков.

2. Извлечение сообщения. Легко показать, что при изменении четности указанным выше способом блок продолжает оставаться «подходящим» (по критерию (6)), поэтому адресат сможет легко вычислить, какие блоки являются стегоконтейнерами. Далее, имея вектор четности, он может извлечь стегосообщение.

Заключение.

Представленная в работе стегосистема использует естественные отклонения в яркости, которые естественным образом возникают при съемке видео на камеру. Потенциальный злоумышленник может выявить наличие сигнала, попиксельно сравнив оригинальное видео со стегоконтейнером. Поэтому необходимо, чтобы оригинал никогда не передавался в открытом виде, чего не трудно добиться в случае видеоконференции. Данный стеганографический метод работает в режиме реального времени, обладает достаточно малой вычислительной сложностью. Операция по внедрению данных не увеличивает размер сжатых видеоданных и не затрудняет передачу видеопотока по каналу фиксированной скорости.

Литература

1. Грибунин В. Г., И. Н. Оков, И. В. Туринцев - Цифровая стеганография (М., Солон-Пресс, 2002 г.)
2. CCITT Recommendation H.261, Video Codec For Audiovisual Services, Genf, 1990
3. Ватолин Д., Ратушняк А., Смирнов М., Юкин В. – Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. (М., Диалог – МИФИ, 2003 г.)
4. Benham D., Memon N., Yeo B.-L., Yeng M. Fast Watermarking of DCT-based compressed images // Proc of the international conference on Image Science, Systems and Technology, 1997, P 243-252