

комплектность и обозначение документов, разрабатываемых на стадиях создания автоматизированных систем.

ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» устанавливает термины и определения основных понятий в области автоматизированных систем (АС) и распространяется на АС, используемые в различных сферах деятельности (управление, исследование, проектирование и т.п., включая их сочетание), содержанием которых является переработка информации.

ГОСТ 34.603-92 « Информационная технология. Виды испытаний автоматизированных систем» Настоящий стандарт распространяется на автоматизированные системы (АС), используемые в различных видах деятельности (исследование, проектирование, управление и т.п.), включая их сочетания, создаваемые в организациях, объединениях и на предприятиях. Стандарт устанавливает виды испытаний автоматизированных систем и общие требования к их проведению. Испытания автоматизированной системы представляют собой процесс проверки выполнения заданных функций системы, определения и проверки соответствия требованиям технического задания количественных и (или) качественных характеристик системы, выявления и устранения недостатков в действиях системы, в разработанной документации.

Итак, интенсивное развитие средств вычислительной техники инициировало широкое развитие, повсеместное внедрение и использование корпоративных порталов. Он, в свою очередь, формирует открытую и прозрачную информационную среду, в которую включены информационные ресурсы, приложения и системы различных подразделений организации. Автоматизация процессов обработки данных в нем позволяет повысить оперативность взаимодействия и протекания процессов обмена данными.

Список использованных источников

1. Christopher C. Shilakesand Julie Tylman, Enterprise Information Portals, "Merrill Lynch, Inc., New York, NY, November 16, 1998.
2. Мухина Ю. Р. Корпоративный информационный портал как средство управления образовательным процессом вуза // Управление в современных системах. 2014. №2 С.44-48.
3. Межгосударственный стандарт ГОСТ 34.003-90 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения" (утв. постановлением Госстандарта СССР от 27 декабря 1990 г. N 3399)//[Электронный ресурс]: Консультант Плюс.
4. Государственный стандарт СССР ГОСТ 15971-90 "Системы обработки информации. Термины и определения" (утв. и введен в действие постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 26 октября 1990 г. N 2698)//[Электронный ресурс]: Консультант Плюс.
5. Городецкая О.Ю., Гобарева Я.Л. CRM - система как стратегия управления бизнесом компании // ТДР. 2014. №4 С.169-172.
6. Цветков В. Я., Троян Ф. М. Стm-как специализированная система управления // Образовательные ресурсы и технологии. 2015. №2 (10) С.48-53.
7. Бахтина Т.Б., Смирнова Н.В. Еgr-система как инструмент достижения конкурентного преимущества в банковском бизнесе // Инновационная наука. 2015. №7-1 С.80-83
8. Варшавская А. А., Протасова А. А. Проблема выбора ERP-системы // Статистика и экономика. 2013. №4 С.163-165.
9. Мансурова Н. А., Пылина М. С. Стратегии внедрения систем электронного документооборота в организациях // Экономические исследования. 2013. №3 С.2.

ПРИМЕНЕНИЕ МЕТОДОВ СТЕГАНОГРАФИИ ДЛЯ ЦИФРОВОЙ ПОДПИСИ ДОКУМЕНТОВ

Мишина О.О.

г. Белгород, ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»

11.03.02 – «Инфокоммуникационные технологии и системы связи»

Азизова Д.Г.

г. Белгород, ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»

09.04.03 – «Прикладная информатика»

Аннотация. В статье рассматривается стойкость дополнительной информации, закодированной в монохромные изображения, для которых оценивалось качество внедрения на основе изменений коэффициентов ДКП в разных частотных областях изображения.

Ведение электронного документооборота, подразумевает обработку документов не только в текстовом виде, но и в виде изображений. При этом возникает задача сортировки и защиты документации, которая предполагает кодирование в структуре документа дополнительной информации. Естественно целесообразно кодировать дополнительную информацию без увеличения объема. Такое кодирование возможно при использовании методов стеганографии. Недостатком методов стеганографии при увеличении объема кодируемой информации является возникновение специфических искажений, соответствующих выбранному методу и уменьшение стойкости информации к цифровым преобразованиям.

Известно прямое дискретное косинусное преобразование (формула 1) и обратное дискретное косинусное преобразование (1).

Прямое ДКП:

$$\Phi = \mathbf{D} \cdot \mathbf{F} \cdot \mathbf{D}^T \quad (1)$$

где \mathbf{F} – блок изображения размера $[N \times M]$, со значениями пикселей $f_{n,m}$;

Φ – блок коэффициентов дискретного-косинусного преобразования;
размера $[U \times \Omega]$, со значениями $\phi_{u,\omega}$;

\mathbf{D} – матрица дискретного-косинусного преобразования (ДКП), $\mathbf{D} = \{d_{u,\omega}\}$,
 $u = 1, 2, \dots, U$ $\omega = 1, 2, \dots, \Omega$.

Обратное ДКП:

$$\tilde{\mathbf{F}} = \mathbf{D}^T \cdot \Phi \cdot \mathbf{D} \quad (2)$$

где $\tilde{\mathbf{F}}$ – блок изображения, восстановленного из частотных коэффициентов ДКП.

$$d(u, \omega) = \frac{1}{\sqrt{N \times M}} C(u) C(\omega) \sum_{n=1}^N \sum_{m=1}^M \cos \left[\frac{\pi(2n+1)u}{2N} \right] \cos \left[\frac{\pi(2m+1)\omega}{2M} \right] \quad (3)$$

где u, ω – шаг дискретной частоты $u = 1, 2, \dots, U$ $\omega = 1, 2, \dots, \Omega$; $C(l)$ – коэффициенты:

$$C(l) = \begin{cases} \frac{1}{\sqrt{2}}, & l = 1 \\ 1, & l > 1 \end{cases}, \quad l \text{ соответствует } u \text{ или } \omega. \quad (4)$$

Матрица \mathbf{D} , состоящая из элементов (3), хранит набор ортогональных функций косинуса в дискретном виде, которые необходимы для осуществления преобразования (1) и (2). Этот математический аппарат положен в основу метода Коха-Жао.

На рисунке 1 представлена известная частотная модель изображения, в которой осуществлено разделение матрицы коэффициентов ДКП на частотные области. Так, самые низкие частоты расположены в левом верхнем углу изображения, а высокие частоты – в правом нижнем. Известно, что наиболее эффективным является кодирование информации в области средних частот, так как низкие частоты содержат наибольшую часть энергии изображения и внесение изменений будет визуально заметно, а высокие наиболее подвержены искажениям, вносимых цифровыми преобразованиями, в частности операциями округления при сохранении на носитель информации. Они так же наиболее сильно изменяются при других процедурах обработки изображений.

DCT

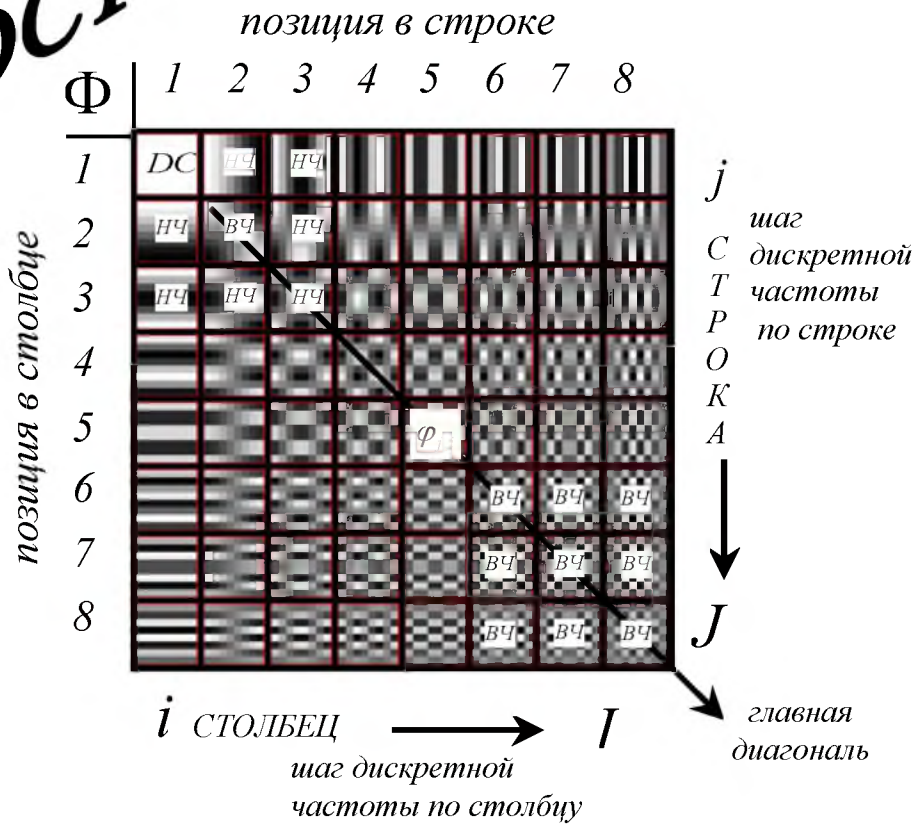


Рисунок 1 – Модель разбиения DCT на частотные области

Алгоритм кодирования дополнительной информации построенный на методе Коха-Жао:

1) из исходного изображения F размером $[M \times K]$ выделяем блок $[8 \times 8]$;

2) для значений пикселей выделенного блока получаем коэффициенты ДКП:

$$\Phi = D \cdot F \cdot D^T.$$

3) в выделенном блоке выбираем коэффициент ДКП $\phi_{i,j}$, задавая его координаты (i, j) ;

4) кодируем бит информации $b_m \in \{0,1\}$, $m = 1, 2, \dots, M$ в выбранном коэффициенте $\phi_{i,j}$ путем замены знака, принадлежащего коэффициенту ДКП;

$$\tilde{\phi}_{i,j} = (2 \cdot b_m - 1) \cdot |\phi_{i,j}|,$$

где $\tilde{\phi}_{i,j}$ – измененный в соответствии с кодируемым битом e_m коэффициент ДКП;

5) осуществляем обратное ДКП-преобразование:

$$\tilde{F} = D^T \cdot \Phi \cdot D.$$

6) все преобразованные блоки объединяем в изображение \tilde{F} с закодированной информацией.

7) Запись изображения.

Алгоритм декодирования дополнительной информации построенный на методе Коха-Жао:

1) изображения с закодированной информацией разбиваем на блоки \tilde{F} размером $[8 \times 8]$;

2) для каждого блока осуществляем разложение на коэффициенты ДКП:

$$\tilde{\Phi} = D \cdot \tilde{F} \cdot D^T$$

3) декодируем бит:

$$\tilde{e}_m = (\text{sign}(\tilde{\phi}_{i,j}) + 1) / 2$$

где $\text{sign}(\)$ – операция определяющая знак $\tilde{\phi}_{i,j}$; \tilde{b}_m - значение декодируемого бита.

Метод Коха-Жао, использующий дискретно-косинусное разложение приводит к искажениям не позволяющим считать символы, поэтому емкость изображения при стеганографическом кодировании невелика, при этом стойкость внедренной информации в три раза выше.

Для определения эффективности работы метода использовались показатели оценивающие искажения, вносимые в изображение при их кодировании и декодировании стеганографическим методом. Для выявления статистики, были посчитаны следующие метрики, базирующиеся на отличие между контейнером – оригиналом и контейнером результатом.

Среднеквадратическая ошибка (mean squared error – MSE), отражает изменение энергии пикселей:

$$MSE = \frac{1}{K \cdot M} \sum_{k=1}^K \sum_{m=1}^M (f_{k,m} - \tilde{f}_{k,m}), \quad (5)$$

где $f_{k,m}$ – пиксель исходного изображения; $\tilde{f}_{k,m}$ – пиксель изображения содержащего дополнительную информацию; M – количество пикселей в столбце; K – количество пикселей в строке.

Оценка определяющая порядок изменения энергии по отношению к общей энергии (signal-to-noise ratio – SNR):

$$SNR = 10 \cdot \log_{10} \frac{255^2}{MSE}. \quad (6)$$

Коэффициент корреляции (ρ), оценивающий степень схожести двух изображений, по нормированной взаимной энергии этих сигналов:

$$\rho = \frac{\sum_{m=1}^M \sum_{k=1}^K \left(f_{m,k} - \frac{1}{M \cdot K} \sum_{m=1}^M \sum_{k=1}^K f_{m,k} \right) \sum_{m=1}^M \sum_{k=1}^K \left(\tilde{f}_{m,k} - \frac{1}{M \cdot K} \sum_{m=1}^M \sum_{k=1}^K \tilde{f}_{m,k} \right)}{\sqrt{\sum_{m=1}^M \sum_{k=1}^K \left(f_{m,k} - \frac{1}{M \cdot K} \sum_{m=1}^M \sum_{k=1}^K f_{m,k} \right)^2 \sum_{m=1}^M \sum_{k=1}^K \left(\tilde{f}_{m,k} - \frac{1}{M \cdot K} \sum_{m=1}^M \sum_{k=1}^K \tilde{f}_{m,k} \right)^2}}. \quad (7)$$

Качество изображения (IF)

$$IF = 1 - \sum_{k,m} (f_{k,m} - \tilde{f}_{k,m})^2 / \sum_{k,m} (f_{k,m})^2. \quad (8)$$

Нормированная взаимная корреляция (NC):

$$NC = \sum_{m=1}^M \sum_{k=1}^K (f_{m,k} \cdot \tilde{f}_{m,k}) / \sum_{m=1}^M \sum_{k=1}^K (f_{m,k}^2). \quad (9)$$

Энергия фрагмента ($\|\mathbf{F}\|^2$):

$$\|\mathbf{F}\|^2 = \sum_{m=1}^M \sum_{k=1}^K (f_{m,k})^2. \quad (10)$$

Стоит отметить формула (7) относится к группе показателей основанных на корреляции между оригинальным и синтезируемым изображением. Формулы (5) и (6) относятся к разностным показателям искажения. В основу данных выражений положен принцип различия между оригинальным и синтезируемым изображением. Формула (8) относится к разностным показателям искажения. Формула (9) относится к группе показателей основанная на корреляции. По моему мнению на восприятие искажений влияет энергия фрагмента формула (10). В основу данных выражений положен принцип различия между оригинальным и синтезируемым изображением.

Вероятность ошибки (BER):

$$BER = \frac{1}{N} \sum_{m=1}^M (b_m \oplus \tilde{b}_m). \quad (11)$$

где N – количество кодируемых/декодируемых бит; \oplus – операция «сумма по модулю два»; b_m – кодируемый бит; \tilde{b}_m – декодируемый бит.

В работе проводится анализ стеганографических методов и параметров кодирования, позволяющих с наименьшими искажениями кодировать дополнительную информацию в изображениях соответствующих текстовым документам. В качестве базы документов использовались монохромные изображения, полученные путем сканирования текста (формата А4, с разрешением 300dpi, формат хранения bmp).

Таблица 1 – Анализ эффективности метода DCT для изображения

Распол. коэф.	MSE	$PSNR$	IF	NC	ρ	BER
НЧ область	83.15	28.93	0.96	0.97	0.98	0.11
СЧ область	6.76	39.83	0.99	0.99	0.99	0.14
ВЧ область	1.89	45.36	0.99	0.99	0.99	0.15

Таблица 1 отображает обобщенные результаты кодирования. При этом самая низкая вероятность ошибки при извлечении, внедренной информации (Ber) наблюдается в НЧ-области матрицы ДКП, но при этом велики количественные значения показателей, оценивающих скрытность. При переходе в ВЧ- область вероятность ошибки возрастает, однако сокращается количество вносимых искажений в изображение. В связи с этим, область средних частот будет предпочтительней для кодирования информации в изображении.

Кратко можно под итожить следующее:

- область средних частот будет предпочтительней для кодирования информации в изображении;
- в качестве мер оценивающих скрытность необходимо опираться на соотношение абсолютное изменение энергии (MSE) и отношение сигнал/шум (PSNR);
- форма искажений совпадает с визуальной моделью распределением ортогонального базиса;
- от выбранной области зависит только форма искажений, а стойкость и скрытность зависит от энергии приходящиеся на коэффициенты DCT;
- для получения меньших искажений и уменьшения вероятности ошибки, номер коэффициентов внедрения стоит выбирать адаптивно относительно энергии отрезка.

В результате анализа методов стеганографии для предлагается DRM-защиты документов хранимых в виде изображений, предлагается использовать методы декомпозиции, при этом, для достижения компромисса между скрытностью и стойкостью, предлагается помещать в блоки с энергией близкой к среднему значению.

Список использованных источников

1. Cox I. J. Senior Member, IEEE, Joe Kilian, F. Thomson Leighton, and Talal Shamoan, Member, IEEE, "Secure Spread Spectrum Watermarking for Multimedia," //IEEE Transactions on Image Processing. – 1997. – Т. 6. – №. 12.
2. Pan J.S., Huang H.C., Jain L.C. (ed.). Intelligent Watermarking Techniques: (With CD-ROM). – World scientific, 2004.
3. Жилияков Е.Г., Лихолоб П.Г., Балабанова Т.Н., Лихогодина Е.С. Технология скрытного кодирования геоданных в снимках земной поверхности //Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. – 2016. – Т. 37. – №. 2(223).
4. Wang Z., Bovik A. C., Evan B. L. Blind measurement of blocking artifacts in images //Image Processing, 2000. Proceedings. 2000 International Conference on. – Ieee, 2000. – Т. 3. – С. 981-984.
5. Исследование искажений, вызванных внедренной в изображение защитной информацией / Лихолоб П.Г., Лихогодина Е.С., Щепилова Д.В. // Проблемы передачи и обработки информации в сетях и системах телекоммуникаций. Материалы 18-й Международной научно-технической конференции. / – Москва: Научно-техническое издательство "Горячая линия-Телеком", 2015г. – С. 123-126.
6. Lykholob, P.G. Research of sensitivity of some measures of quality assessment of hidden information in the audio content [Текст] // Medvedeva, A.A. Likhogodina, E.S. Mishina, O.O. RESEARCH RESULT. Information technologies. №4. v.1. 2016. pp. 21-25 URL: http://rr.bsu.edu.ru/media/information/2016/4/3_it.pdf DOI: 10.18413/2518-1092-2016-1-4-21-24