

Стеганографический алгоритм, устойчивый к изменению формата видеофайла

С.В. Белим
belimsv@omsu.ru

П.Г. Черепанов
pcherepanov@gehtsoft.com

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация

В статье предложен алгоритм встраивания цифровых водяных знаков в видеофайлы. Алгоритм основывается на методе Коха ЖАо для изображений. Видеофайл рассматривается как трехмерный объект. Метод встраивания модифицирован на трехмерный случай. Используется модель YUV. Встраивание осуществляется в компоненту интенсивности. Предлагается встраивать не изображение, а его голограмму. Проведен компьютерный эксперимент по тестированию устойчивости встраиваемой информации к изменению цветовой модели.

Введение

Основная задача алгоритмов внедрения цифровых водяных знаков в изображения и видеофайлы состоит в создании меток, устойчивых к внешним воздействиям. Таким образом, основной целью атаки на цифровые водяные знаки является их уничтожение с минимальным искажением контейнера. Воздействие на контейнер может носить различный характер. Одна из атак состоит в изменении формата контейнера. Для встраивания цифровых водяных знаков используются алгоритмы стеганографии. Однако основная цель стеганографических алгоритмов в сокрытии самого факта передачи информации, в связи с чем не все стеганографические алгоритмы могут быть использованы как основа для цифровых водяных знаков. Вследствие этого для актуальной является задача разработки алгоритмов встраивания информации стеганографическими алгоритмами устойчивыми к изменению формата. В данной статье будут рассматриваться только алгоритмы встраивания в видеофайлы.

Наибольшее распространение для видеофайлов получил алгоритм встраивания, являющийся логическим продолжением подхода, развитого для изображений. Видеопоток разбивается на отдельные кадры, после чего производится встраивание частей цифрового водяного знака в последовательность изображений [1, 2]. Не смотря на высокую скорость работы, такой подход обладает существенными недостатками. Основной из них связан с проблемой синхронизации кадров, требующий встраивания дополнительной информации для однозначного извлечения цифрового водяного знака. В качестве таких дополнительных данных могут выступать статистические характеристики кадра [3, 4] и специальные метки синхронизации [2], также может применяться избыточное кодирование [5]. В связи с тем, что части цифрового водяного знака локализованы в достаточно малой области покадровое встраивание характеризуется низкой устойчивостью к изменению формата. Небольшие погрешности вычислений приводят к изменению большого количества битов цифрового водяного знака.

Copyright © by the paper's authors. Copying permitted for private and academic purposes.

In: Sergey V. Belim, Nadezda F. Bogachenko (eds.): Proceedings of the Workshop on Data, Modeling and Security 2018 (DMS-2018), Omsk, Russia, October 2018, published at <http://ceur-ws.org>

Для повышения устойчивости цифрового водяного знака необходимо использовать стеганографические алгоритмы, обеспечивающие равномерное распределение встраиваемой информации по всему видеопотоку. В этом случае локальное воздействие приводит к небольшому повреждению встроенной информации. Устойчивость цифрового водяного знака также может быть повышена с помощью алгоритмов его формирования.

Одним из возможных решений, распределяющих цифровой водяной знак по всем кадрам равномерно, является представление видеопотока в виде трехмерного объекта и построение стеганографических алгоритмов на основе трехмерных преобразований. Трехмерное дискретное косинусное преобразование впервые было использовано в статье [6]. В дальнейшем оно применялось в основном для оценивания качества кодирования видеопотока на основе исследования распределения коэффициентов преобразования [7, 8, 9, 10]. Алгоритмы встраивания стеганографических вставок в видеопоток, как трехмерный объект, были разработаны на основе различных технологий: статических и динамических временных компонентов небольшой волны вдоль оси времени [11], на основе трехмерного преобразования Фурье [12, 13], на базе трехмерного вейвлет-преобразования [14, 15, 16], на базе трехмерного дискретного косинусного преобразования [17, 18, 19].

В данной статье предложен алгоритм встраивания цифрового водяного знака в видеофайл, устойчивый к изменению формата.

1 Постановка задачи и решение

В качестве контейнера для стеганографической вставки будем использовать видеопоток с цветовой моделью YUV. Данная цветовая модель используется в большом количестве кодеков таких как NTSC, PAL, SECAM. В данной модели каждая точка представлена тремя цветовыми координатами: Y – яркость, U и V – цветоразностные компоненты. Яркостная компонента Y определяет черно-белое изображение, а компоненты U и V содержат информацию, позволяющую восстановить цвет каждой точки. При изменении кодировки наибольшие изменения происходят в цветоразностных компонентах, тогда как яркостная составляющая остается практически неизменной. Поэтому в качестве контейнера для встраивания будем использовать преобразования яркостной координаты точек видеопотока.

Для встраивания в видеопоток цифрового водяного знака как в трехмерный контейнер, модифицируем метод Коха-Жао [21]. В основе данного метода лежит дискретное косинусное преобразование. Для изображений преобразование носит двумерный характер. В нашем же случае необходимо использовать трехмерный аналог. Для этого разобьем весь видеопоток на кубические блоки по $N \times N \times N$ пикселей. Таким образом в каждый блок попадут пиксели из N последовательных кадров. Разбиение будем осуществлять слева-направо и сверху-вниз. Введем обозначение f^i для i -го блока. Вычислим спектральные коэффициенты дискретного косинусного преобразования для каждого из блоков:

$$f_{u,v,k}^i = \frac{\xi(u)\xi(v)\xi(k)}{\sqrt{8/N^3}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \sum_{z=0}^{N-1} f_{x,y,z}^i \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi v(2y+1)}{2N}\right) \cos\left(\frac{\pi k(2z+1)}{2N}\right),$$

где

$$\xi(u) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{if } u > 0 \\ 1, & \text{if } u = 0. \end{cases}$$

Здесь введены обозначения: $f_{x,y,z}^i$ – значение яркости пикселя в исходном блоке в точке (x, y, z) , $f_{u,v,k}^i$ – спектральный коэффициент дискретного косинусного преобразования в точке (u, v, k) .

В результате будет получен набор коэффициентов дискретного косинусного преобразования, объединенных в трехмерные матрицы размером $N \times N \times N$. В каждую из таких матриц встраивается один бит цифрового водяного знака. В области низкочастотных компонент, расположенной в окрестности точки $(0, 0, 0)$, хранятся основные данные видеопотока. Встраивание в эту область приводит к наибольшим визуальным искажениям. В высокочастотной области, расположенной в окрестности точки (N, N, N) , визуальные искажения при встраивании будут наименьшими. Однако данные коэффициенты подвергаются наибольшим изменениям при изменении кодировки. Поэтому оптимальным решением будет осуществлять встраивание в среднечастотную область.

Возьмем две точки в среднечастотной области (u_1, v_1, k_1) и (u_2, v_2, k_2) . Зададим пороговое значение для разности модулей коэффициентов P . Встраиваемое сообщение m представим в виде битовой строки. Пусть

i -ый бит имеет значение m_i . Для встраивания бита m_i в блок $f_{u,v,k}^i$ необходимо вычислить вспомогательные функции:

$$\begin{aligned}\omega_1^i(u_1, v_1, k_1) &= |f_{u_1, v_1, k_1}^i|, \\ \omega_2^i(u_2, v_2, k_2) &= |f_{u_2, v_2, k_2}^i|, \\ Z_1^i(u_1, v_1, k_1) &= \begin{cases} -1, & \text{if } f_{u_1, v_1, k_1}^i < 0 \\ 1, & \text{if } f_{u_1, v_1, k_1}^i \geq 0. \end{cases} \\ Z_2^i(u_2, v_2, k_2) &= \begin{cases} -1, & \text{if } f_{u_2, v_2, k_2}^i < 0 \\ 1, & \text{if } f_{u_2, v_2, k_2}^i \geq 0. \end{cases}\end{aligned}$$

Для встраивания пересчитаем коэффициенты дискретного косинусного преобразования

$$\begin{aligned}\Omega^i(u_1, v_1, k_1) &= \begin{cases} P + \omega_2^i(u_2, v_2, k_2) + 1, & \text{if } (\omega_1 - \omega_2) \leq P \text{ and } m_i = 0, \\ \omega_1^i(u_1, v_1, k_1), & \text{if } (\omega_1 - \omega_2) > P \text{ and } m_i = 1. \end{cases} \\ \Omega^i(u_2, v_2, k_2) &= \begin{cases} P + \omega_1^i(u_1, v_1, k_1) + 1, & \text{if } (\omega_1 - \omega_2) \geq P \text{ and } m_i = 1, \\ \omega_2^i(u_2, v_2, k_2), & \text{if } (\omega_1 - \omega_2) < P \text{ and } m_i = 0. \end{cases} \\ F^i(u_1, v_1, k_1) &= Z_1^i(u_1, v_1, k_1) \cdot \Omega^i(u_1, v_1, k_1), \\ F^i(u_2, v_2, k_2) &= Z_2^i(u_2, v_2, k_2) \cdot \Omega^i(u_2, v_2, k_2).\end{aligned}$$

Далее выполним обратное дискретное косинусное преобразование для получения блоков видеопотока с встроенным цифровым водяным знаком:

$$F_{x,y,z}^i = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} \sum_{k=0}^{N-1} \frac{\xi(u)\xi(v)\xi(k)}{\sqrt{8/N^3}} F_{u,v,k}^i \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi v(2y+1)}{2N}\right) \cos\left(\frac{\pi k(2z+1)}{2N}\right),$$

Далее блоки собираются в видеопоток в обратном порядке.

Для извлечения цифрового водяного знака необходимо по аналогии с процедурой встраивания разбить видеопоток на блоки размером $N \times N \times N$ и применить к ним дискретное косинусное преобразование. Для выделения i -го бита m_i используем следующие соотношения:

$$\begin{aligned}\omega_1^i(u_1, v_1, k_1) &= |F_{u_1, v_1, k_1}^i|, \\ \omega_2^i(u_2, v_2, k_2) &= |F_{u_2, v_2, k_2}^i|, \\ m_i &= \begin{cases} 0, & \text{if } (\omega_1^i(u_1, v_1, k_1) \geq \omega_2^i(u_2, v_2, k_2)), \\ 1, & \text{if } (\omega_1^i(u_1, v_1, k_1) < \omega_2^i(u_2, v_2, k_2)). \end{cases}\end{aligned}$$

Алгоритм встраивания цифрового водяного знака может быть обобщен в виде следующего набора шагов:

1. Разбить видеопоток на блоки размером $N \times N \times N$ пикселей.
2. Выполнить трехмерное дискретное преобразование для каждого из блоков и получить матрицы коэффициентов.
3. Выбрать две точки из среднечастотной области, лежащих на побочной диагонали $(0, 0, N) - (N, N, 0)$.
4. Определить пороговое значение разности коэффициентов P .
5. Представить цифровой водяной знак в виде битовой строки и осуществить побитовое встраивание в последовательность блоков.
6. Выполнить обратное дискретное косинусное преобразование каждого из блоков.
7. Объединить полученные блоки в видеопоток.

Для извлечения цифрового водяного знака необходимо выполнить шаги с 1 по 3 данного алгоритма и далее извлечь биты цифрового водяного знака.

2 Получение голограммы цифрового водяного знака

Будем исходить из того, что встраиваемый цифровой водяной знак представляет собой некоторое изображение. В этом случае устойчивость цифрового водяного знака к различным атакам может быть существенно повышена, если встраивать не само изображение, а его цифровую голограмму. Цифровая голограмма [20]

позволяет восстанавливать исходное изображение даже по ее отдельной части. При этом снижается только интенсивность изображения.

Голограмма вычисляется как результат интерференции двух когерентных лучей – объектного и опорного. Под опорным лучом понимается волна, идущая напрямую от источника к приемнику. Объектный луч испытывает рассеяние на предмете, после чего попадает в приемник. В данном случае объектный луч отражается от встраиваемого изображения. Рассчитаем интенсивность итоговой волны в каждой точке голограммы:

$$\varepsilon(\tilde{x}, \tilde{y}) = \sum_{x=0}^N \sum_{y=0}^N 3I(x, y) \cos\left(\frac{d}{l}\right).$$

В качестве координат точек выбираются положения соответствующих пикселей на изображении и на голограмме: $(\tilde{x}, \tilde{y})$ – положение пикселя на голограмме, (x, y) – положение пикселя на изображении цифрового водяного знака, $I(x, y)$ – интенсивность пикселя цифрового водяного знака, λ – длина волны, d – расстояние между точками цифрового водяного знака и голограммы, вычисляемая по формуле:

$$d = \sqrt{(2x - \tilde{x})^2 + (2y - \tilde{y})^2 + (2z - \tilde{z})^2}.$$

Так как голограмма представляет собой двумерный объект, можно положить:

$$(2z - \tilde{z})^2 = 1.$$

Алгоритм получения цифрового водяного знака может быть представлен в виде следующих шагов:

1. Выберем интенсивность опорного луча в каждой точке голограммы равной 128, что составляет половину исходной интенсивности.
2. Определим длину волны опорного и объектного луча.
3. Для каждой точки голограммы рассчитаем интенсивность объектного луча.
4. Вычислим суммарную интенсивность лучей в каждой точке голограммы.

Восстановление исходного цифрового водяного знака может быть получена по тому же алгоритму при нулевом значении интенсивности опорного луча.

3 Компьютерный эксперимент

В компьютерном эксперименте изучалась устойчивость предложенного алгоритма встраивания цифрового водяного знака к изменению цветовой схемы видеоконтейнера. Исходный контейнер представлял собой видеопоток формата .mp4 с использованием кодека h.264 и цветовой моделью YUV420p. В качестве цифрового водяного знака было выбрано монохромное изображение «©». Встраивание производилось в канал яркости (Y). В компьютерном эксперименте поочередно встраивался сам цифровой знак и его цифровая голограмма. Полученный видеоконтейнер с цифровым водяным знаком перекодировался в цветовые модели YUV422, YUV410. Для размера блока было выбрано значение $N = 8$ в связи с тем, что тестируемые алгоритмы кодировки видеопотока используют блоки $8 \times 8 \times 8$. Такая согласованность повышает устойчивость цифрового водяного знака, так как исключает потерю данных при переходе из одного блока в другой. Для порогового значения P выбирались различные значения.

Надежность встраивания цифрового водяного знака оценивалась с помощью нормированной корреляции между исходным изображением цифрового водяного знака и цифровым водяным знаком после извлечения [22]:

$$NC = \frac{\sum_i W(i, j) \sum_j \tilde{W}(i, j)}{\sum_i \sum_j [W(i, j)]^2},$$

где $W(i, j)$ и $\tilde{W}(i, j)$ значения яркости пикселя во встроеном и извлеченном изображении соответственно. Значение NC лежит в интервале от 0 до 1. Единичное значение соответствует полному совпадению изображений.

Для оценки влияния встроеного цифрового водяного знака на видеопоток использовался стандартный подход измерения искажений [23], основанный на вычислении отношения сигнала к шуму (PSNR):

$$PSNR = 20 \log_{10} \frac{255}{\sqrt{MSE}},$$

Таблица 1: Результаты соотношения PSNR для предложенных методов

Величина порога	PSNR	NC
Предложенный метод (без голограммы)		
$P = 25$	37.0568 db	0.2249
$P = 26$	36.2759 db	0.2582
$P = 27$	36.1946 db	0.3030
Предложенный метод (с голограммой)		
$P = 25$	37.0568 db	0.4338
$P = 26$	36.2759 db	0.6657
$P = 27$	36.1946 db	0.7861

Таблица 2: Результаты значений PSNR

Метод	Значение PSNR
Предложенный метод (с голограммой)	36.1946 db
Предложенный метод (без голограммы)	36.1946 db
Работа [6]	32.587 db
Работа [7]	35.4263 db

где

$$MSE = \frac{1}{MK} \sum_i \sum_j [P(i, j) - \tilde{P}(i, j)]^2,$$

$P(i, j)$ и $\tilde{P}(i, j)$ значения яркости пикселя в исходном видеопотоке и с водяным знаком соответственно, а i и j — ширина и высота кадров в видеопотоке. Единицей измерения $PSNR$ служит децибел (db). Если $PSNR < 40$ db, то искажения визуально практически не заметны.

В таблице 1 представлены значения $PSNR$ и NC при различных пороговых значениях P для предложенного метода встраивания. Эксперимент проводился для 100 различных видеофайлов с последующим усреднением результатов.

Как видно из Таблицы 1 наилучшие результаты удается получить при пороговом значении $P = 27$, при котором произведение $NC \cdot PSNR$ имеет наибольшее значение.

В таблице 2 приведено среднее значение $PSNR$ для случаев непосредственного встраивания цифрового водяного знака и встраивания его голограммы. Также приведены аналогичные результаты, полученные с помощью вейвлет-преобразования в статьях [6, 7].

В таблице 3 приведены значения NC между исходным цифровым водяным знаком и извлеченным из видеофайла после изменения цветовой модели.

Из таблицы 3 видно, что использование цифровой голограммы существенно повышает устойчивость цифрового водяного знака по сравнению с прямым встраиванием.

Заключение

Результаты компьютерного эксперимента подтверждают устойчивость предложенного алгоритма к изменению цветовой модели и формата видеофайла. Устойчивость достигается с помощью встраивания в канал

Таблица 3: Значения нормированной корреляции при изменении цветовой модели видеофайла с встроенным цифровым водяным знаком

Цветовая модель	Нормированная корреляция (с голограммой)	Нормированная корреляция (без голограммы)
YUV422	0.74	0.2
YUV410	0.7212	0.19

яркости, содержащий «черно-белое» изображение. Использование в качестве контейнера цветоразностной компоненты, с одной стороны сопровождается меньшими визуальными искажениями, но, с другой стороны испытывают наибольшее искажение при переходе от одной цветовой модели к другой, что приводит к потере встроенных данных и невозможности извлечения цифрового водяного знака. Сравнение с аналогичными методами, представленными в работах [6, 7], показывает, что предложенный метод обладает более высоким уровнем надежности и вносит меньшие визуальные искажения. Тем не менее следует отметить, что предложенный метод дает заметные визуальные эффекты на областях при наличии на кадрах больших областей равномерной светлой заливки.

Список литературы

- [1] E.T. Lin, E.J. Delp Temporal synchronization in video watermarking. *IEEE Transactions on Signal Processing*, 52(10):3007–3022, 2004.
- [2] D. Delannay, B. Macq. Classification of watermarking schemes robust against loss of synchronization *Proceedings of SPIE 5306, Security, Steganography and Watermarking of Multimedia Contents VI*:581–591, 2004.
- [3] C. Chen, J.Ni, J. Huang. Temporal statistic based video watermarking scheme robust against geometric attacks and frame dropping. *Digital Watermarking. - Springer, 2009*:81–95.
- [4] S.W. Sun, P.C. Chang. Video watermarking synchronization based on profile statistics. *Proceedings of IEEE 37th Annual 2003 International Carnahan Conference on Security Technology*:410–413, 2003.
- [5] V.A. Mitekin, V.A. Fedoseev. A new robust information hiding method for video. *Computer Optics*, 38(3):564–573, 2014.
- [6] J. Roese, W. Pratt, G. Robinson. Interframe cosine transform image coding. *IEEE Transaction on Communication*, 25(11):1329–1339, 1977.
- [7] M. Bauer, K. Sayood. Video coding using 3 dimensional DCT and dynamic code selection. *Proceedings of Data Compression Conference*:451, 1995.
- [8] M. Servais, G. de Jager. Video compression using the three dimensional discrete cosine transform (3D-DCT). *Proceedings of the South African Symposium on Commun. and Signal Process*: 27–32, 1997.
- [9] R.K.W. Chan, M.C. Lee. 3D-DCT quantization as a compression technique for video sequences. *Proc. of International Conf. on Virtual Sys. and MultiMedia*: 188–196, 1997.
- [10] N. Bozinovic, J. Konrad. Motion analysis in 3D DCT domain and its application to video coding. *Signal Processing: Image Communication*, 20:510–528, 2005.
- [11] M. Swanson, B. Zhu, A.T. Tewfik. Multiresolution scene-based video watermarking using perceptual models. *IEEE Journal on Sel. Areas in Comm.*, 16(4):540–550, 1998.
- [12] F. Deguillaume, G. Csurka, J. O’Ruanaidh, T. Pun. Robust 3D DFT video watermarking. *Proc. SPIE, Security and Watermarking of Multimedia Content II*, 3971:346–357, 2000.
- [13] H. Liu, N. Chen, J. Huang, X. Haung, Y.Q. Shi. A robust DWT-based video watermarking algorithm. *IEEE International Symposium on Circuits and Systems*:631–634, 2002.
- [14] M. Kucukgoz, O. Harmanci, M.K. Mihcak, R. Venkatesan. Robust Video Watermarking via Optimization Algorithm for Quantization of Pseudo-Random Semi-Global Statistics. *Proc. SPIE, Security, Steganography, and Watermarking of Mult. Cont. VII*, 5681, 2005.
- [15] P. Campisi, A. Neri. Video watermarking in the 3DDWT domain using perceptual masking. *IEEE Int. Conference on Image Processing. Genoa, Italy*, 2005.
- [16] P. Campisi. Video watermarking in the 3D-DWT domain using quantization-based methods. *IEEE International Workshop on Multimedia Signal Processing. Shanghai, China*, 2005.

- [17] J.H. Lim, D.J. Kim, H.T. Kim, C.S. Won. Digital video watermarking using 3D-DCT and Intra-Cubic Correlation. *Proc. SPIE, Security and Watermarking Contents III.*, 4314:54–72, 2001.
- [18] P. Campisi, A. Neri. 3D-DCT video watermarking using quantization-based methods. *15th European Signal Processing Conference (EUSIPCO 2007)*, 2007.
- [19] P.G. Cherepanov, S.V. Belim. Robust Algorithm of Embedding of Digital Water Marks in a Video Stream. *CEUR Workshop Proceedings*. 1965, 2017 URL: <http://ceur-ws.org/Vol-1965/paper12.pdf>
- [20] M.V. Smirnov. Holographic approach to embedding hidden watermarks in a photographic image. *Journal of Optical Technology*, 72(6):464–468, 2005.
- [21] E. Koch, J. Zhao. Towards robust and hidden image copyright labeling. *IEEE Workshop on Nonlinear Signal and Image Processing*:452–455, 1995.
- [22] K.A. Navas, M. Sasikumar, S. Sreevidya. A benchmark for medical image watermarking. *Proceedings of 14th International Workshop on Systems, Signals and Image Processing, Maribor, Slovenia*:237–240, 2007.
- [23] Q. Huynh-Thu, M. Ghanbari. Scope of validity of PSNR in image/video quality assessment. *Electronics Letters*, 44(13):800–801, 2008.

Steganographic Algorithm Robusting to Video Format Transform

Sergey V. Belim, Pavel G. Cherepanov

In article the algorithm of digital watermarks inserting in video is suggested. The algorithm is based on Koch's and Zhao method for images. The video is considered as a three-dimensional object. The inserting method is modified on a three-dimensional case. The YUV model is used. Inserting is carried out in an intensity component. It is suggested to insert hologram of image. The computer experiment on testing of inserting data stability to the color model change is made.