STATISTICAL ANALYSIS OF STEGANOGRAPHIC ALGORITHMS IN IMAGE AND VIDEO CONTAINERS

RADOSTIN E. RAFAILOV, GEORGI V. VALCHEV

ABSTRACT: *The article presents a statistical analysis of steganographic algorithms applied to image and video containers. The study evaluates the performance, robustness, and detectability of various algorithms under different conditions. The research aims to provide a comprehensive understanding of the state of steganographic analysis by methodically presenting the most popular techniques. The findings serve as a valuable resource for further development and implementation of secure data embedding practices in digital media.*

KEYWORDS: *Steganography, information security*

DOI: https://doi.org/10.46687/CALV9734

СТАТИСТИЧЕСКИ АНАЛИЗ НА СТЕГАНОГРАФСКИ АЛГОРИТМИ ПРИ ИЗОБРАЖЕНИЯ И ВИДЕО КОНТЕЙНЕРИ *

РАДОСТИН Е. РАФАИЛОВ, ГЕОРГИ В. ВЪЛЧЕВ

АБСТРАКТ: *Статията представя статистически анализ на стеганографски алгоритми, приложени към изображения и видео контейнери. Изследването оценява производителността, устойчивостта и откриваемостта на различни алгоритми при различни условия. Изследването има за цел да предостави цялостно разбиране за състоянието на стеганографския анализ чрез методично представяне на най-популярните техники. Резултатите служат като ценен ресурс за по-нататъшно развитие и прилагане на практики за сигурно вграждане на данни в цифрови медии.*

1. Въведение

В съвременния дигитален свят, сигурността на информацията е от изключителна важност. С нарастващото използване на интернет, необходимостта от ефективни методи за защита на данните става все по-належаща. Един от тези методи е стеганографията – техника за скриване на информация в различни носители, като изображения и видео контейнери [1]. Съвременната стеганография има за цел да вгради информация в подходящ контейнер, така че тя да остане незабелязана от потребители, различни от предназначения получател. В компютърните системи и интернет пространството ежедневно циркулира огромен обем цифрова информация, което създава благоприятни условия за разработване на стеганографски алгоритми за изпращане или скриване на секретна информация. Стеганографските техники могат да се използват и за защита на данни в области като военните и правителствени комуникации, защита на авторските права, корпоративни комуникации, електронни гласувания, защита на медицинска информация, както и за контрол на данните в социалните мрежи и решаване на други задачи, свързани с осигуряване на информационната сигурност.

* Настоящата статия е частично финансирана от фонд „Научни изследвания“ на Шуменски Университет „Епископ К. Преславски“ по проект № РД-08-107/30.01.2024 г.

Проблемът със защитата на важна информация от нежелано разкриване е все още актуален в наши дни и съхранението на данните е приоритет. Една от ключовите актуалности на темата е във все по-растящата необходимост от сигурност на данните, която е изправена пред заплахи като хакерски атаки, киберпрестъпност и неразрешен достъп до лична или чувствителна информация.

2. Стеганографски методи, базирани на анализ на изображения и видео контейнери

През последните години все по-често се използват стеганалитични методи за проверка на надеждността на стеганографията. Чрез тях се изследва каква е възможността приложеният алгоритъм да бъде компрометиран. Изследването на стеганографските алгоритми се осъществява чрез различни емпирични тестове, фокусиращи се върху стандартни показатели на цифрови изображения и видео обекти със скрита информация в тях.

2.1 Визуален анализ

Визуалният анализ е сред най-разпространените методи за оценяване на стеганографски алгоритми. Неговата цел е да идентифицира визуални разлики между оригиналните графични и видео файлове и тези, съдържащи скрити данни. При анализ на видео контейнери, този метод изисква разделяне на видеото на отделни кадри.

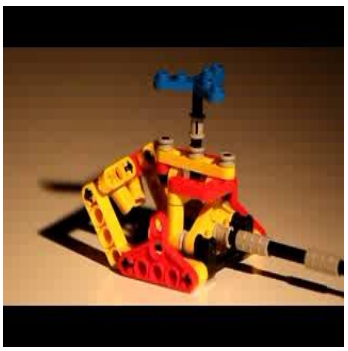
Фиг. 1 и Фиг. 2 показват сравнение между оригиналния графичен файл и този с вградена информация [2].

Фиг. 1 Оригинал

Фиг. 2 Стегофайл

Фиг. 3 и Фиг. 4 показват първия кадър на тестовия видео файл със съответния му кадър със скрита информация [3].

Фиг. 3 Оригинал



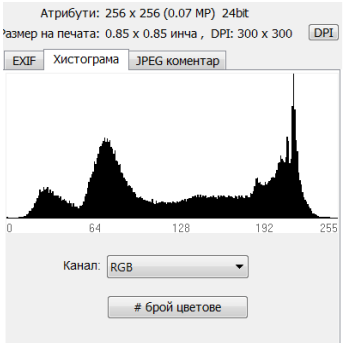
Фиг. 4 Стегофайл

Визуалният анализ демонстрира, че няма видими разлики между оригиналните и стеганографските файлове.

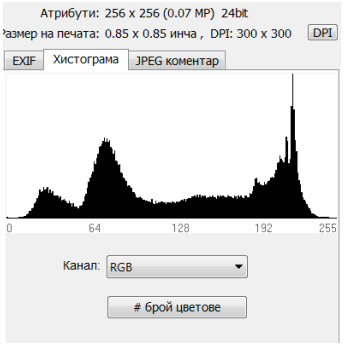
2.2 Хистограмен анализ

Хистограмите на цифрови изображения са графично представяне на разпределението на цветовете за червения, зеления и синия канал. При манипулация на изображението се променя и цветовото разпределение, което позволява да се оцени степента на промяна в цветовите стойности. Видимите разлики в хистограмите на стего изображенията в сравнение със стего контейнера могат да служат като индикатор за използвана стеганография. Необичайните пикове или липса на плавни преходи в хистограмата могат да издадат наличието на скрита информация.

На Фиг. 5 и Фиг. 6 е представен хистограмен анализ на тестовото изображение и съответния му стего файл [2].

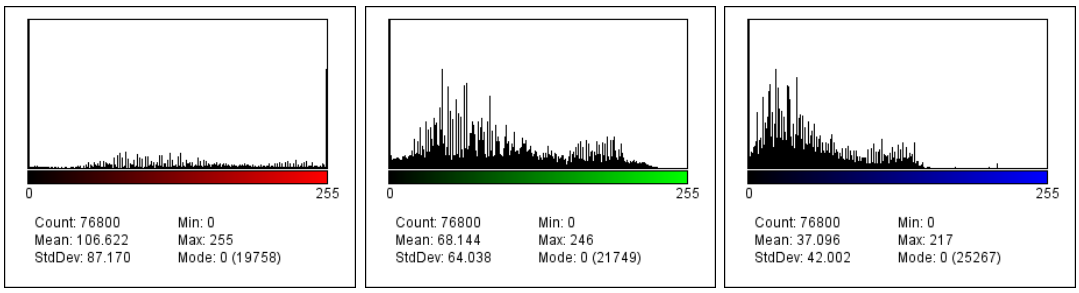


Фиг. 5 Оригинал

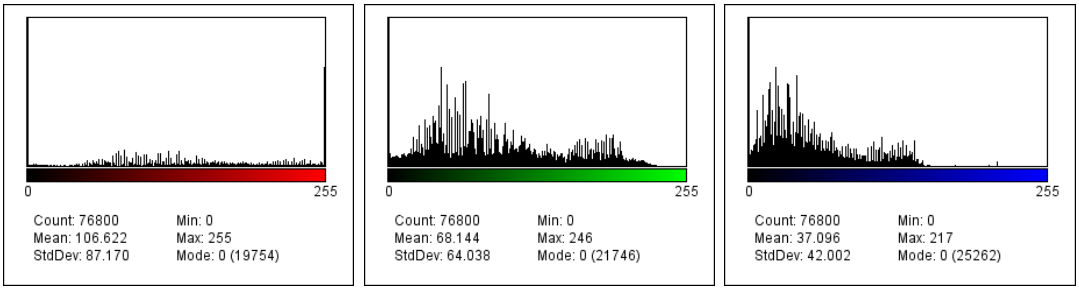


Фиг. 6 Стегофайл

Фиг. 7 и Фиг. 8 показват разпределението на цветовете на първия фрейм от оригиналния видео контейнер и съответния му фрейм с вградена информация [3].



Фиг. 7 Оригинал



Фиг. 8 Стегофайл

Хистограмният анализ показва, че стеганографските техники, използвани за вграждане на информация в контейнерните файлове, са успешни в скриването на данните без видима промяна в хистограмите на оригиналните и стего файловете.

2.3 Съотношение на пиков сигнал - шум – PSNR

PSNR (Peak Signal-to-Noise Ratio) е показател, който се използва за анализиране на качеството на реконструирани или обработени изображения и видеа спрямо оригиналите. В основната си функция той измерва съотношението между максималната сила на чистия сигнал и приложената намеса (шум). При анализ на цифрови изображения, PSNR отчита промяната в цветовите стойности. Промяната в качеството на изображението, вследствие на манипулация на пикселите, може да бъде индикация за стеганография. За изчисляване на PSNR се използва следната формула:

(1) $$PSNR = 10\log_{10}\frac{MAX^2}{MSE}\ (dB),$$

където MAX е максималната стойност на пиксела в изображението. За осембитови изображения, това е 255.

MSE (Mean Square Error) е средната квадратична грешка, измерваща средната разлика в цветовите стойности между пикселите на изображението и стего файла, разделена на общия брой пиксели. Тя се изчислява по следната формула:

(2) $$MSE = \frac{\sum_{x=1}^{N}\sum_{y=1}^{M}(p_{x,y}-s_{x,y})^2}{NM},$$

където $p_{x,y}$ и $s_{x,y}$ са съответните пиксели на изображението и стего файла [4].

По-високите стойности на PSNR показват по-ясен сигнал и стойностите над 60 dB се считат за приемливи за стеганографски анализ [3]. Стойности на PSNR под 20-30dB отчитат лошо качество на изображението.

Таблица 1 показва PSNR резултати от направени стеганографски изследвания подбрани изображения.

Таблица 1 Резултати от PSNR анализи

Изображения	Реф. [5]	Реф. [6]	Реф. [7]	Реф. [8]	Реф. [9]	Реф. [10]	Реф. [11]
1	48.0	45.0	43.94	60.51	54.34	52.99	73.98
2	–	44.0	43.95	72.48	53.32	52.79	74.10
3	–	44.0	43.95	69.61	53.32	52.73	74.04
4	–	–	43.93	71.12	–	52.72	74.16
5	47.0	45.0	43.93	69.77	–	53.09	74.09

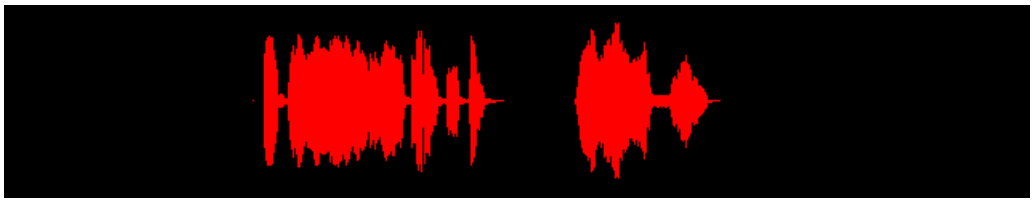
Резултатите от таблицата демонстрират, че стеганографията в контейнерите е била успешно приложена, тъй като не са получени PSNR стойности под 30 dB.

2.4 Анализ на звуковата вълна (Waveform analysis) при видео обекти

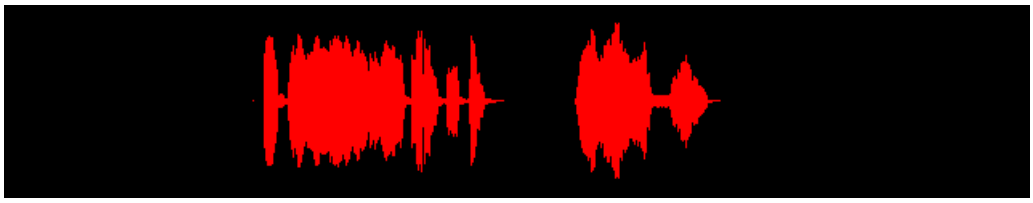
Формата на звуковата вълна представлява графично изображение на аудиосигнал или запис. Тя илюстрира промените в амплитудата в рамките на определен период. Амплитудата на сигнала се показва по оста y (вертикално), докато времето се отбелязва по оста x (хоризонтално). Повечето аудиозаписващи програми визуализират звуковите вълни, предоставяйки на потребителя представа за записаното. Ако вълната е ниска и не е добре изразена, това вероятно означава, че записът е много тих. Ако вълната запълва почти цялото

изображение, записът може да е бил прекалено силен. Промените във формата на вълната също са полезни за идентифициране на различни части от записа.

На Фиг. 9 и Фиг. 10 е представена звукова форма на оригинално аудио и съответното му аудио, в което има скрита информация [12].



Фиг. 9 Оригинално аудио



Фиг. 10 Стего аудио

От показания анализ се забелязва, че няма видими изменения на амплитудата между двата аудио записа.

3. Заключение

Статистическият анализ на стеганографските алгоритми за изображение и видео контейнери е от съществено значение за осигуряване на информацаионната сигурност в дигиталния свят. Статистическите методи позволяват на специалистите по сигурността да изследват и оценят тези техники, за да се уверят, че скритите съобщения са надеждни и сигурни. Това включва анализ на различни параметри на изображението или видеото, като честота на поява на пиксели с определена стойност, разпределение на цветовете и други. Освен това, анализите могат да помогнат при разработването на нови стеганографски алгоритми, които са по устойчиви на детекция и атаки. С развитието на технологиите, хакерите използват по-сложни методи за откриване на скрити съобщения, което изисква непрестанни иновации в тази област. Използването на напреднали математически и статистически модели осигурява по-високо ниво на защита и сигурност на данните.

Анализът на проблемите, свързани с внедряването и оценката на стеганографските подсистеми за защита на информацията, както и предложените подходи, подчертават важността от по-сериозно внимание при интегрирането на тези системи в цялостната информационна защита. Разгледаните стеганографски анализи са сред най-често срещаните подходи за тестване на устойчивостта и надеждността на стеганограски алгоритми и демонстрират начините, по които това може да бъде постигнато.

При анализирането на стеганографски алгоритми е важно да се подчертае значението на мултидисциплинарния подход, който включва съвместна работа между математици, компютърни инженери и специалисти по сигурността. По този начин могат да бъдат открити ефективни и комплексни решения, които да подобрят методите за защита, откриване и анализиране на стеганография.

ЛИТЕРАТУРА:

[1] Rafailov, R. (2024, November). Parallel steganographic algorithm based on least significant bit. In *E3S Web of Conferences* (Vol. 508, p. 04018). EDP Sciences.
[2] Stefanov, A., Valchev, G., & Rafailov, R. (2022, September). Sector steganographic algorithm with column modification on Raspberry hardware. In *AIP Conference Proceedings* (Vol. 2505, No. 1). AIP Publishing.
[3] Kordov, K., & Valchev, G. (2019). Video steganography with steganalysis. *Mathematical and Software Engineering*, *5*(1), 15-22.
[4] Железов, С., Кордов, К., Методи на стеганологичната подсистема за информационна защита, 240 стр., Университетско издателство Епископ Константин Преславски, Шумен, 2023, ISBN: 978-619-201-712-5
[5] Hemalatha S., U. Dinesh Acharya, A. Renuka (2013) Comparison of secure and high capacity of color image steganography techniques in RGB and YCBCR domains, I. J. Adv. Inf. Technol. (IJAIT), 3, 1–9.
[6] Hemalatha S., U. D. Acharya, A. Renuka, P. R. Kamath (2013). A secure color image steganography in transform domain, I.J. Cryptogr. Inf. Secur. (IJCIS), 3, 17–24.
[7] Jung K.-H., K.-Y. Yoo (2015) Steganographic method based on interpolation and LSB substitution of digital images, Multimed. Tools Appl., 74, 2143–2155.
[8] Majeed M. A., R. Sulaiman (2015) An improved LSB image steganography tech-nique using bit-inverse in 24 bit colour image, J. Theoret. Appl. Inf. Technol., 80, 342–348.
[9] Tomar G. (2012) Effect of Noise on image steganography based on LSB insertion and RSA encryption, IOSR J. Eng., 2, 473–477.
[10] Zhang S., T. Gao (2015) A novel data hiding scheme based on DNA coding and module-N operation, I. J. Multimed. Ubiq. Eng., 10, 337–344.
[11] Stoyanov, B. P., Zhelezov, S. K., & Kordov, K. M. (2016). Least significant bit image steganography algorithm based on chaotic rotation equations. *Comptes rendus de l'Academie bulgare des Sciences*, *69*(7), 845-850.
[12] Paraskevov, H., Valchev, G., & Rafailov, R. (2022, September). Steganographic algorithm in video with message encryption. In *AIP Conference Proceedings* (Vol. 2505, No. 1). AIP Publishing.

Радостин Рафаилов:
Шуменски университет „Епископ Константин Преславски“,
r.rafailov@shu.bg

Георги Вълчев:
georgivvulchev@gmail.com