ALGORITHM MODEL FOR STEGANOGRAPHIC DATA PROTECTION IN VIDEO CONTAINERS

GEORGI V. VALCHEV **KRASIMIR M. KORDOV**

ABSTRACT: *This paper presents an algorithm model for steganographic hiding of textual information in video containers using pseudorandom number generators. The developed model determines a random selection of frames and positions within them for dispersed embedding of secret data in the video file.*

KEYWORDS: *Steganography, Video steganography, Data hiding.*

DOI: https://doi.org/10.46687/CNBP9350

МОДЕЛ НА АЛГОРИТЪМ ЗА СТЕГАНОГРАФСКА ЗАЩИТА НА ИНФОРМАЦИЯ ВЪВ ВИДЕО КОНТЕЙНЕРИ [*]

ГЕОРГИ В. ВЪЛЧЕВ **КРАСИМИР М. КОРДОВ**

АБСТРАКТ: *Настоящата статия представя модел на алгоритъм за стеганографско скриване на текстова информация във видео контейнери с използване на псевдослучайни генератори на числа. Разработеният модел определя случаен избор на кадри и позиции в тях за разпръснато вграждане на тайни данни във видео файла.*

1 Въведение

Защитата на информация е фундаментален проблем през последните хилядолетия в човешката история. Едно от научните направления, свързани със защита на информация е стеганографията. Буквалният превод на този термин от гръцки език е „тайнопис“ и през годините са разработвани различни методи за неговата реализация.

Развитието на технологиите променя вида на общодостъпната и използвана информация, като обикновената информация се заменя с дигитална, с цел по-лесно съхранение, обработка и достъпност. Масовото използване на цифрова информация изисква разработване на нови методи за стеганографска защита на данни.

Целта на съвременната стеганография е вграждане на информация в подходящ контейнер (файл), която не може да бъде засечена от потребител, различен от получателя. В компютърните системи и интернет пространството всяка секунда циркулира огромен обем цифрови данни, което предоставя условия за изграждане на стеганографски алгоритми за изпращане или скриване на секретна информация[1].

Най-често използваните файлове в компютърните системи ги правят подходящи носители (контейнери) на секретна информация. Това са текстовите файлове[2], цифровите изображения[3], аудио[4,5] и видео файловете[6]. През последните години изследователи на стеганографски алгоритми са разработвали и изследвали нови методи и алгоритми за скриване на информация предимно в тези видове контейнери. Използването на всеки вид файл изисква разбирането на неговата специфика и структура за успешно вграждане на скрита информация.

[*] Настоящата статия е частично финансирана по проект № РД-08-88/02.02.2026.

Настоящата статия е фокусирана върху реализацията на стеганографски алгоритъм чрез модифициране на кадри на видеофайл за скриване на тайни съобщения в двоичен вид.

2 Структура на видео файлове

Цифровите видео файлове представляват съвкупност от статични фреймове (кадри), които се възпроизвеждат последователно под формата на видео поток. Последователната смяна на кадрите създава възприемането им като движение. С развитието на цифровата обработка на различни файлови формати през последните години са разработени редица специфични видео формати, като всеки от тях се характеризира със своите методи за визуализация и „разширение“ (.mp4, .mkv, .avi, .mov и др.)[7].

Модерните видео файлове поддържат не само видео поток от кадри, но и допълнителни данни, като аудио поток, субтитри и метаданни. Кратка информация за тези структурни единици е представена в **Таблица 1**.

Таблица 1 - Структура на видеофайл

Структурна единица	Предназначение
Видео поток (Video Stream):	Поредицата от феймове (кадри), които образуват картината.
Аудио поток (Audio Stream):	Звуковият съпровод на видеото (може да бъде повече от един – например за различни езици)
Субтитри (Subtitles):	Текстови файлове с таймкодове за синхронизация
Метаданни (Metadata):	Допълнителна информация за файла – заглавие, автор, дата на създаване, резолюция, софтуер за редактиране, геолокация, данни за авторски права и др.

Видео потокът е най-обемната част от този вид файлове и с цел оптимизация на размера на файловете са разработени хардуерни и софтуерни алгоритми за компресия на данните, наречени кодеци (примери: H.264 (AVC), H.265 (HEVC), DivX и др.). Недостатък при компресията на файлове чрез видео кодеци е загубата на информация. Поради тази причина стеганографските алгоритми за скриване на данни са трудно приложими и успешната стеганография във видео контейнери се реализира най-лесно във файлове без компресия.

Други важни характеристики на видео потока са:

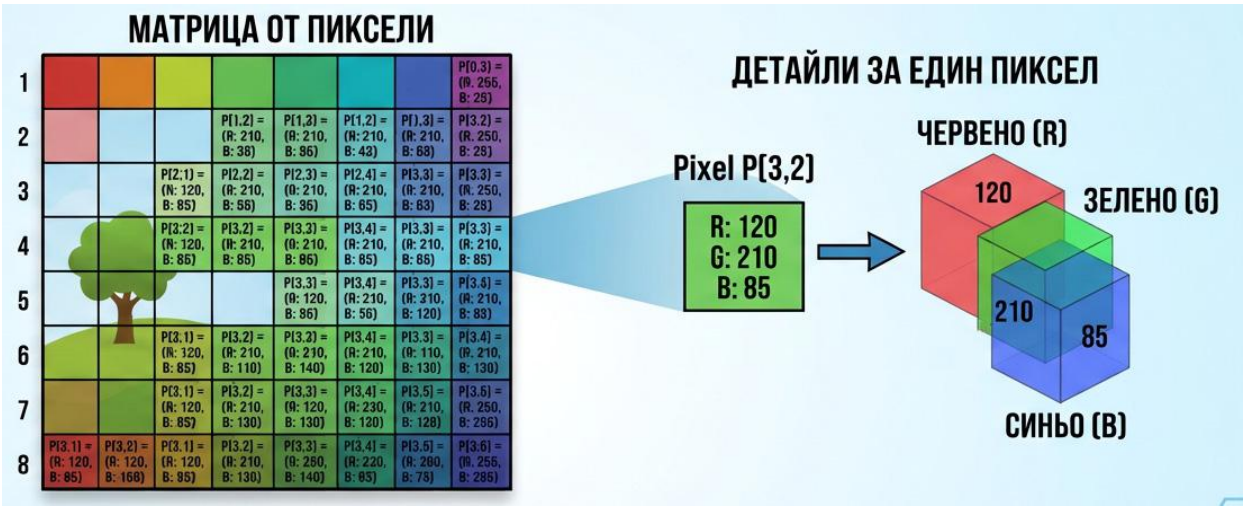
- **Резолюция** (Брой пиксели) – определя разделителната способност (размерите) на картината (например Full HD - 1920x1080 или 4K - 3840x2160).
- **Честота на кадрите** (Frame Rate) – определя броя на статичните изображения, които се сменят за една секунда (измерва се в fps – кадри в секунда, най-често използвани са 24, 30 или 60 fps).
- **Битрейт** (Bitrate) – определя количеството данни, които се обработват за една секунда (измерва се в Mbps или Kbps). По-високият битрейт означава по-добро качество, но и по-голям размер на файла.

Отчитайки структурните единици на видео файловете, потенциални възможности за скриване на информация са във кадрите и/или в звуковите файлове, изграждащи аудио потока. За разлика от стеганографските алгоритми в единично изображение, възможността за използване на множество кадри създава предпоставки за допълнителна сигурност при защитата на информация чрез равномерно разпределяне на тайните данни в различни позиции на видео файла.

3 Стеганография в цифрови изображения

Дигиталните изображения често се използват за контейнери на скрита информация посредством стеганографски алгоритми. Широкото използване на цифрови изображения нараства всяка година и след кратките текстови съобщения, най-често изпращаните файлове в интернет са именно цифровите изображения.

Структурата на тези графични файлове представлява матрица от пиксели с различни цветови стойности. Всеки пиксел се характеризира с местоположение, дефинирано в равнина със стойности за неговата хоризонтална и вертикална позиция в цифровото изображение. Цветовата стойност на пиксела се определя от конкретните стойности на червения, зеления и синия цвят (RGB) за съответния пиксел. Примерно описание на структура на цифрово изображение е показано на ***Фиг. 1***.



Фигура 1 – Структура на цифрово изображение

Стеганографските алгоритми използват минимална промяна на цветовите стойности на пикселите, която остава незабележима за човешкото око. Този метод коригира най-малко значимия бит (Least significant bit - LSB) в стойността на червения, зеления или синия цвят (или всеки от трите цвята) на пикселите и през последните години изследователи масово използват този начин за скриване на секретна информация в цифрови изображения[8]. Матричното разположение на пикселите позволява избирането на конкретни позиции, в които да бъде скривана двоична последователност.

Псевдослучайните генератори се използват за случайно извличане на числа[9]. Посредством секретен ключ, който представлява комбинация от конкретни стойности на начални параметри, се извлича винаги различна последователност от числа. При стеганографските алгоритми, използващи цифрови изображения, псевдослучайните генератори могат да се използват за определяне на случайни позиции на пикселите, в които да бъде скрита информация. Това добавя значителна сигурност на алгоритъма, защото поредността на вграждане е хаотична. Този метод се нарича „***разпръснато вграждане***“. При стандартно и последователно прочитане на цветовите стойности на пикселите за извличане на потенциални тайни вградени съобщения, опитът ще бъде неуспешен поради грешка в правилната последователност.

4 Модел на стеганографски алгоритъм във видео файлове

Отчитайки структурата на видеофайловете, методът на вграждане при използване на най-малко значимия бит (LSB) и възможността за използване на псевдослучаен генератор, се предлага следният стеганографски алгоритъм:

Стъпка 1: Секретната информация се трансформира в двоична последователност – Вектор T.

Стъпка 2: Броят на стойностите от T се разделя на броя на кадрите на видеофайла, за да се определи каква част от тайното съобщение ще бъде вградена във всеки кадър. Условно означаваме получената стойност с N.

Стъпка 3: Служебната информация (метаданните) от видеофайла V_1 се копира в нов видеофайл V_2 .

Стъпка 4: Генерира се случайно число от псевдослучайния генератор, за определяне на номер на кадър от видеофайла.

Стъпка 5: Избраният кадър се обработва като цифрово изображение. От псевдослучайния генератор се извличат две стойности, за избиране на случайна позиция на пиксел.

Стъпка 6: По метода на най-малко значимия бит, последните битове на червения, зеления и синия цвят се заменят със стойностите от Вектор T (вграждане на тайното съобщение).

Стъпка 7: До достигане на стойността на N се преминава към ***Стъпка 5***.

Стъпка 8: Готовият фрейм се записва във видеофайлът V_2 .

Стъпка 9: До изчерпване на двоичната последователност за скриване (във Вектор T) се преминава към ***Стъпка 4***.

Стъпка 10: Новополученият файл V_2 съдържа резултатния видеофайл с вградена тайна информация.

За извличане на тайната скрита информация е достатъчно да се приложи същият алгоритъм, като вместо вграждането в цветовите стойности на пикселите се използва прочитане и конструиране на вектор от стойностите на пикселите.

5 Заключение

Предложеният модел за стеганографска защита на секретна информация във видеофайлове предстои да бъде изследван за необходимата сигурност[10]. Този модел дава възможност на изследователи да модифицират алгоритми чрез използване на различни псевдослучайни генератори, за вграждане на данни само в конкретни цветови стойности, за вграждане на съобщения с различни дължини и т.н.

Допълнително изискване към предложения модел е видът на видеофайловете, като най-добри резултати се получават при файлове без компресия. Разработеният алгоритъм изисква и допълнителни изследвания за стеганографска сигурност чрез анализиране на различни показатели (визуален анализ, хистограмен анализ, корелационен анализ, съотношение сигнал-шум и др.).

Потенциалът на предложения модел може допълнително да се увеличи при използване на звуковите потоци на видеофайлове за скриване на секретна информация. Добавянето на криптографска защита на тайното съобщение[11] преди самото скриване на информация също допринася за засилване на информационната сигурност на стеганографския алгоритъм.

ЛИТЕРАТУРА:

[1] Zhelezov, S., Uzunova-Dimitrova, B., & Paraskevov, H. (2017). An approach for hiding steganography data within web applications. *Journal of Engineering and Applied Sciences*, *12*, 8251-8255.

[2] Zhelezov, S., Kordov, K., Nachev, A., Stoyanova, T., Uzunova-Dimitrova, B., & Pavlova, D. (2021, November). Study of the Efficiency Coefficient of the Steganographic Embedding in Text Containers Using the Letter Replacement Method. In *2021 3rd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA)* (pp. 680-684). IEEE.

[3] Kordov, K., & Zhelezov, S. (2021). Steganography in color images with random order of pixel selection and encrypted text message embedding. *PeerJ computer science*, *7*, e380.

[4] Zhelezov, S., Kordov, K., Nachev, A., Pavlova, D., Gindev, P., Litchkov, N., & Nesterov, K. (2024, November). A new approach for spread spectrum steganography in audio containers. In *2024 6th International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA)* (pp. 474-477). IEEE.

[5] Zhelezov, S., Kordov, K., Nachev, A., & Pavlova, D. (2023, November). Spread Spectrum Steganography In Audio Containers. In *2023 5th International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA)* (pp. 568-571). IEEE.

[6] Paraskevov, H., Valchev, G., & Rafailov, R. (2022, September). Steganographic algorithm in video with message encryption. In *AIP Conference Proceedings* (Vol. 2505, No. 1, p. 060013). AIP Publishing LLC.

[7] Kordov, K., & Dimitrov, G. (2021). A new symmetric digital video encryption model. *Cybernetics and Information Technologies*, *21*(1), 50-61.

[8] Rafailov, R., & Paraskevov, H. (2026). Parallel Color-Specific LSB Steganography: A New Approach for Data Hiding in BMP Images. *TEM Journal*, *15*(1), 83.

[9] Kordov, K. (2015). Signature attractor based pseudorandom generation algorithm. *Advanced Studies in Theoretical Physics*, *9*(6), 287-293.

[10] Paraskevov, H., Zhelezov, S., & Uzunova-Dimitrova, B. (2017). ROBUSTNESS OF THE SECRET MESSAGE IN STEGO FILE AGAINST FLIP AND ROTATION ATTACK. *Annals: Series on Mathematics & its Applications*, *9*(1), 5.

[11] Kordov, K. (2021). Text encryption algorithm for secure communication. *International Journal of Applied Mathematics*, *34*(4), 705.

докторант Георги Вълчев
ФМИ, Шуменски университет „Епископ Константин Преславски“
E-mail: georgivvulchev@gmail.com

проф. д-р инж. Красимир Кордов
Месторабота: Шуменски университет „Епископ К. Преславски“
ORCID ID: 0000-0002-4397-8303
E-mail: krasimir.kordov@shu.bg