# МЕТОД ЗА РАЗПРЪСНАТО СТЕГАНОГРАФСКО ВГРАЖДАНЕ С ИЗПОЛЗВАНЕ НА КРИПТОГРАФСКИ АЛГОРИТЪМ

***Станимир Железов, Красимир Кордов***

*Шуменски университет „Епископ Константин Преславски",*
*s.zhelezov@shu.bg, krasimir.kordov@shu.bg*

***Резюме**: В тази статия е предложен подход за изграждане на стеганографско вграждане в изображения на криптирана текстова информация. Описани са основните стеганографски направления и криптографски алгоритъм за защита на текст. Посочени са предимствата на използвания метод, който повишава нивото на сигурност при използването предложеният подход.*

***Ключови думи**: стеганография, криптография, разпръснато вграждане*

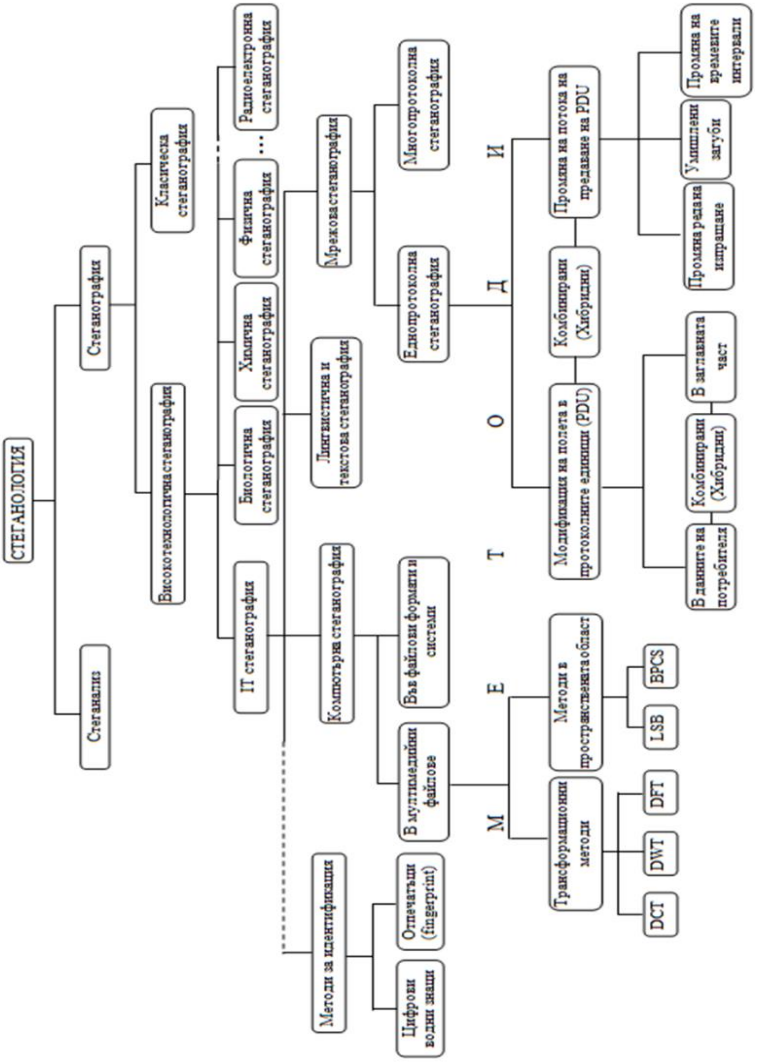
## 1. Въведение

През вековете са изобретени много техники и средства за защитата на важна информация от нежелано разкриване. Един от ефективните подходи за скриване на самото съществуване на такава информация, при нейното съхраняване или предаване, е стеганографията. [1]

Според съвременните схващания, класификацията на базата на използваните от нея технологии и подходи на стеганографията включва т.нар. класическа стеганография ( в някои трудове се среща като нискотехнологична стеганография) и високотехнологична стеганография. В състава на последната влизат компютърната стеганография, мрежовата стеганография, радиоелектронната, биологичната и други перспективни стеганографии. На Фиг. 1 е показана класификация на стеганографията на съвременния етап от нейното развитие [2].

От Фиг.1 е видно, че основен компонент на високотехнологичната стеганография е IT-стеганографията, която обхваща компютърната, мрежовата и текстовата (документна, лингвистична) стеганография. Терминът компютърна стеганография се използва за общо разглеждане на двете основни направления на съвременната компютърна стеганография - използването на специалните свойства на компютърните формати и използване на „излишък" в мултимедийните файлове, т.е. скриване на информация в преобразувани в дискретна форма сигнали, имащи непрекъсната аналогова природа [3]. Второто направление обхваща методите с използване на излишък в бинарното представяне на мултимедийната информация и върху него са фокусирани по-голямата част от съществуващите стего методи.

Всеки от мултимедийните контейнери има свои особености, и всеки от тях изисква използване на специфични за него методи за вграждане и извличане на скрита информация. Мултимедийната стеганография е едно от най-изследваните направления на компютърната стеганография.




*Фиг. 1- Класификация на стеганографията на съвременния етап от нейното развитие.*

Цифровите изображения, цифровата музика и цифровото видео се представят чрез матрици от числа, които кодират интензивността на цветовете или на звуковите сигнали в пространството и/или във времето. Младшите разряди на цифровите отчитания съдържат много малък полезен товар за текущите параметри на звуците и образите. Тяхното запълване с други данни не влияе съществено върху качеството на възприемане на изображението или на звука от хората [4].

В последните години множество научни разработки разглеждат възможностите за стеганографски обмен на чувствителна информация, които предоставят различните типове мултимедийни контейнери – графични файлове, аудио файлове и видео файлове. В голяма част от тях се залага на комбиниране на различни методи от стеганографията, а понякога с цел повишаване на сигурността се имплементират и криптографски методи. Типичен пример за това е използването на генератори на псевдо-случайни числа за разпръснато стеганографско вграждане [5] [6].

## 2. Криптографски алгоритъм

Криптографските алгоритми имат цел да защитят конкретна информация, като я трансформират в различен от първоначалният вид, с помощта на различни методи и средства [7]. Основният принцип е само получателят или получателите на информацията да могат да възстановят първоначалния ѝ вид, като това най-често се извършва чрез използването на секретен ключ.

Отчитайки факта, че развитието на компютърните системи и мрежи налага използваната информация да е в цифров вид, криптографските алгоритми през последните години са разработвани с предназначение за поточно побитово криптиране на цифрова информация.

Един от масово използваните подходи за поточно криптиране на данни са Псевдослучайните генератори на двоични последователности [8][9][10], които имат софтуерна реализация и свойството да произвеждат неограничен брой случайни битове. Основното изискване към псевдослучайните генератори (ПСГ) е знанието на произволна част от последователността да не може да се използва за определяне на следващите генерирани битове, т.е. те да бъдат случайни.

Използвайки ПСГ като криптографски примитиви за текстово криптиране, води до трансформиране на текста в нечетим вид, като тя може да бъде възстановена при декриптирането. В компютърните системи текстовото криптиране се извършва като се използва числовият ASCII еквивалент на символите, изграждащи текста.

Стеганографията вгражда в различни контейнери предимно тайни текстови съобщения, като криптирането на вградената текстова информация може

допълнително да повиши нивото на сигурност при реализацията на цялостен стеганографски алгоритъм.

## 3. Предложен метод

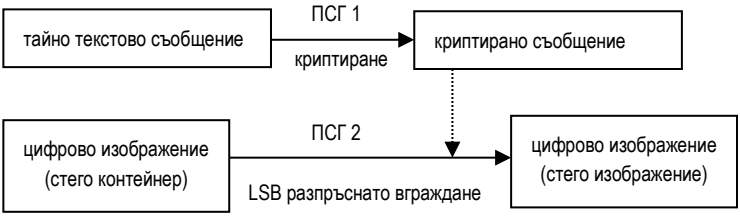
Най-често използваният стеганографски подход при вграждане в цифрови изображения е Least Significant Bit (LSB), при който най-младшият бит, на всеки цвят на пикселите от изображението, се използва за носител на скрита информация. Този метод е предпочитан, тъй като не оставя видими следи и почти не променя крайното стегоизображение с вградено тайно съобщение.

При последователно обхождане на позициите на пикселите (по редове или по колони) стеганографията лесно може да бъде открита, затова през последните години се използват алгоритми с разпръснато вграждане, при който последователността на използваните пиксели за скриване на информация е разбъркана.

При предложеният модел за стеганографско скриване на тайно текстово съобщение в цифрово изображение се използват два псевдослучайни генератора, които изпълняват следните функции:

- криптиране на тайното текстово съобщение преди вграждане;
- определяне на случайни позиции на пикселите на изображението, за реализация на разпръснатото вграждане.

Схемата на предложения метод е показана на Фиг. 2.




*Фиг. 2 – Метод за разпръснато стеганографско вграждане с използване на криптографски алгоритъм.*

Алгоритъмът на предложения метод се изразява в следното:

1. Тайното текстово съобщение се преобразува в двоичен вид;
2. Полученият двоичен вектор се криптира с помощта на първия псевдослучаен генератор (ПСГ 1);

3. След криптирането се получава двоичен вектор на криптираното съобщение;
4. Стего контейнерът се обхожда като матрица от пиксели;
5. С втория псевдослучаен генератор (ПСГ 2) се избират случайни пиксели за вграждане на тайното съобщение;
6. След извършване на вграждането се получава новото стего изображение.

Важно е да се отбележи, че за реализацията на този метод е необходимо и двамата комуникиращи да разполагат с ключовете (инициализиращите последователности на двата генератора).

## 4. Предимства на предложения подход

Предложеният модел за разпръснато стеганографско вграждане с използване на криптографски алгоритъм има следните предимства:

- Използването на псевдослучайни генератори изисква инициализиращи начални стойности, дефиниращи два секретни ключа, което повишава сигурността;
- Случайният избор на последователността на пикселите (чрез ПСГ 2 и секретен ключ 2) за вграждане на тайното съобщение, прави трудно уловимо използването на стеганография, чрез стандартните методи за анализ;
- Криптирането на тайното текстово съобщение (чрез ПСГ 1 и секретен ключ 1) допълнително затруднява противодействието на стеганографията, дори при знание за последователността на използваните пиксели;
- Използването на стандартния LSB подход, не променя видимо крайното стегоизображение и не разкрива следи от използвана стеганография.

## Заключение

Използването на комбинирани криптографски и стеганографски методи води до повишаване на нивото на сигурност при защитата на информацията и дава възможност за създаването на нови алгоритми в стеганографията и криптографията. В настоящата статия е предложен подход, който комбинира двете направления за изграждане на цялостен модел за разпръснато вграждане в цифрови изображения на криптирана текстова информация. Предложеният модел е описан и схематично онагледен и са посочени предимствата на посочената схема.

## Благодарности

Тази работа бе подкрепена от Европейския фонд за регионално развитие и Оперативна програма "Наука и образование за интелигентен растеж" по договор УНИТе № BG05M2OP001-1.001-0004 (2018-2023).

## Литература

1. С. Станев, С. Железов, Х. Параскевов и Х. Христов, Ръководство за упражнения по стеганография, Шумен: Университетско издателство „Епископ Константин Преславски", ISBN 978-619-201-011-9. 140 стр., 2015.
2. S. Stanev и K. Szczypiorski, „Steganography Training: a Case Study from University of Shumen in Bulgaria," International Journal of Electronics and Telecommunications, том 62, № 3, pp. 315–318., 2016.
3. Zhelezov, S., H. Paraskevov, H. Hristov, P. Boyanov, B. Uzunova, An architecture of steganological subsystem for information protection, Proceedings of 10-th International Conference ICBBM, Liepaya, Latvia, 2014, p. 123–128.
4. С. Железов., Станев, С. Первые результаты внедрения курса „Компютерная стеганография" в Шуменском университете//Трудове на международната научно-практическа конференция на ВДПУ „Коцюбински", Винница,Украйна, 2012, стр. 205–207.
5. K. Kordov, „A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture," Electronics, том Vol. 8, № No. 5, p. 530, 2019.
6. Kordov, Krasimir, and Lachezar Bonchev, "Using circle map for audio encryption algorithm." Mathematical and Software Engineering 3.2 (2017): 183–189.
7. С. Станев, А. Алексеев. Изучение криптографии и стеганографии в Поволжском государственном университете телекоммуникаций и информатики и Шуменском университете им. Епископа Константина Преславского Инфокоммуникационные технологии. 2015. Т. 13, № 1. С. 93–99. ISSN 2073-3909.
8. Kordov, K. M. (2014). Modified Chebyshev map based pseudo-random bit generator. In *AIP Conference Proceedings* (Vol. 1629, No. 1, pp. 432–436). American Institute of Physics.
9. Kordov, K. (2015). Modified pseudo-random bit generation scheme based on two circle maps and XOR function. *Applied Mathematical Sciences*, *9*(3), 129–135.
10. Kordov, K. (2015). Signature attractor based pseudorandom generation algorithm. *Advanced Studies in Theoretical Physics*, *9*(6), 287–293.

## METHOD FOR SPREAD SPECTRUM STEGANOGRAPHY WITH CTYPTOGRAPHIC ALGORITHM

***Резюме:*** *This article proposes an approach for building steganographic embedding in images of encrypted textual information. The main steganographic directions and cryptographic algorithm for text encryption are described. The advantages of the method are pointed out, which increases the level of security using the proposed approach.*