ГРАФИЧНО ИНТЕРПРЕТИРАНЕ НА ЦИФРОВИ ПРОДУКТИ И ПРИЛОЖЕНИЯ В СТЕГАНОГРАФИЯТА

Емануил Ст. Стоянов, Божидар Ст. Стоянов

GRAPHIC INTERPRETATION OF DIGITAL PRODUCTS AND APPLICATIONS IN STEGANOGRAPHY

Emanuil St. Stoyanov, Bozhidar St. Stoyanov

ABSTRACT: *Today, the generation of digital data is easier than it has ever been. These are the so-called digitally born products – documents, images, audio and video recordings, software, e-books, digital models, maps, etc. They are more and more widely employed nowadays in a variety of fields, such as business, science, art, education, digital communications, national security, intelligence service, military science, etc. Their global application has brought forth the need for their being reliably protected and has made it an issue of paramount importance in the modern world of information. This necessity has imposed the fast development of two contemporary sciences - cryptography and steganography. The present report treats one of the recent variations in the development of steganography - digital steganography, suggesting a universal idea for its application to all types of digital products.*

KEYWORDS*: Steganography, Watermark, Fingerprint, Secret Image, Stego Object, Cover Image, Embedding.*

1. Увод

Днес, повече от всякога е лесно да се генерират цифрови данни. Това са т. нар. „цифрово родени" продукти – документи, изображения, аудио- и видеозаписи, софтуер, електронни книги, цифрови модели, карти и т.н. Тяхното приложение се простира в различни области на нашето съвремие – бизнеса, науката, изкуството, образованието, цифровите комуникации, националната сигурност, разузнаването, военното дело и др. Заедно с това възникна необходимостта от тяхната надеждна защита, което е от

първостепенно значение в съвременния информационен свят. Това наложи бързото развитие на две съвременни науки – криптография и стеганография. Този доклад разглежда един от съвременните варианти на стеганографията – цифровата стеганография, и предлага една идея за нейното приложение към всякакви цифрови продукти.

2. Изложение

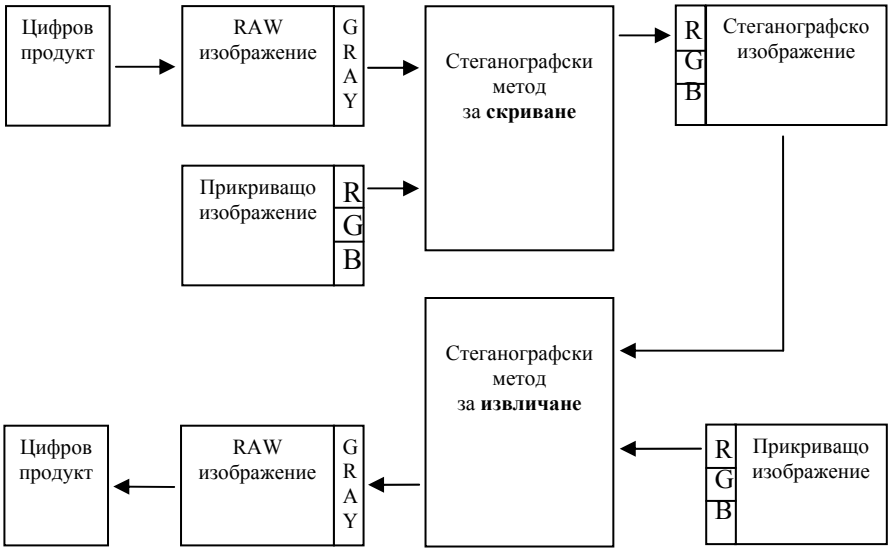
Стеганографията е древно изкуство [1] и наука за предаване на скрити данни по такъв начин, че никой освен получателя да не разбере за съществуването им. Особен интерес за нас представляват съвременните стеганографски методи, които се обобщават в направлението цифрова стеганография. Тя изучава възможностите за скриване на информация в друга, анализирайки особеностите в цифровото представяне на данни, както и слабостите на човешките възприятия [6]. Един от най-популярните съвременни методи за стеганографска защита е LSB (*Least Significant Bit*), основаващ се на използването на най-малко значимия бит [3] за представяне на скрити данни.

Методите за стеганографско скриване, които се използват в този доклад, са авторски и тяхното описание не е предмет на тази статия. Подробно са разгледани в [6]. В този доклад е предложен подход, който позволява те да могат да бъдат използвани във всяка област от съвременния живот, където в електронен вид се съхранява и употребява цифрово представена информация.

2.1. Метод за скриване на произволен цифров продукт в изображение

Стеганографските методи в този доклад работят изцяло с изображения. Това налага необходимостта всички източници да се сведат до изображения.

Цифровите продукти могат да се представят като единични файлове с размер K bytes. В случаите, когато са многокомпонентни (напр. софтуерните пакети) е възможно да се сведат до единствен файл чрез архивиране.



Фиг. 1 Принципна схема за прилагане на стеганографски методи към цифрови продукти

В основата на предлагания подход стои идеята [4], че всички файлове без значение от тяхното предназначение, структура или тип, се съхраняват в електронен вид като последователност от байтове. В случаите, когато техните размери отговарят на условието от формула (1), тогава те могат да бъдат интерпретирани като растерни изображения с размери MxN пиксела, чрез промяна на типа им в RAW формат, некомпресиран (8-bits, Grayscale). В контекста на цифровата стеганография, тези изображения са подходящи да бъдат обект на скриване и затова могат да бъдат наречени **секретни** (Secret Images). Процесът на скриване изисква да е налично и още едно изображение, наречено **прикриващо** (Cover Image). Нека то има размери PxQ пиксела. За да може Secret Image успешно да се „вплете” в Cover Image, задължително трябва да е изпълнено ограничението (2). Резултатът от тази операция е изображение неразличимо от

прикриващото, което е прието да се нарича **стеганографско изображение** или Stego Object.

(1) $$K = MN$$

(2) $$M \le P,\ N \le Q$$

По този начин, скриването на какъвто и да е цифров продукт се свежда до метод за вплитане на изображение в изображение. При обратния процес се извлича еквивалентно копие на вплетеното RAW изображение. Чрез повторна смяна на типа му към този, който е бил преди процеса на скриване се възстановява оригиналният вид на файла, неговите първоначални формат и структура, което осигурява правилното му интерпретиране и го прави точно копие на скрития цифров продукт (Secret Image). Фиг. 1 онагледява [4] описания по-горе подход на скриване и извличане на произволен цифров продукт с изображение.

Разглеждането на произволен файл като Grayscale изображение допуска той да бъде скрит само в един от RGB каналите на цветно изображение. Това напрактика означава, че в едно пълноцветно изображение могат да се скрият до 3 различни файла, удовлетворяващи условията (1) и (2).

Съществуват много и различни изисквания към качествата на разработваните стеганографски методи, по-важни от които са:

- *запазване структурата на носещия (прикриващия) файл;*
- *скриване факта на присъствието на друга информация;*
- *устойчивост по отношение опитите за премахване или повреждане на скритата информация;*

Отчитайки споменатите изисквания може да се заключи, че за прикриващи (Cover) източници могат да се използват файлове, в чиято структура липсва служебна информация (header). Такива формати са – RAW (за изображения), WAV (за звук), TXT (за текстов документ). Освен това, съдържанието на носещите файлове трябва да е тясно свързано с несъвършенствата в човешките възприятия, каквито има при възприемането на образи, звуци, сетивност, обоняние. Въпреки, че текстовите

документи имат подходящ файлов формат (TXT), те не могат да се използват за носители на скрита информация. Това е така, защото не е възможно да се удовлетвори второто изискване – скриване факта за наличие на друга информация.

От казаното до тук могат да се направят следните заключения [4]:

- ☞ Най-неподходящи за носители (Cover) са всички цифрови източници, притежаващи header или такива, в които информацията се представя с твърде ограничено множество от стойности. Пример за това са текстовите файлове, при които отделните символи се представят само със стойности от 0 до 255.
- ☞ Всеки цифров източник е подходящ за скриване (Secret), стига да са удовлетворени условията (1) и (2), позоволяващи му да се представи в едноканално RAW изображение.

На базата на предложения подход за скриване на произволни цифрови продукти в изображения, и разработения авторски стеганографски метод описан в [6], бяха реализирани успешно следните експерименти, описани в таблица 1. За всеки от проверените случаи бяха констатирани пълно скриване и 100% възстановяване на скритата информация.

Таблица 1.

Области на приложение	**Описание на експеримента**	
	Източник подлежащ на скриване	**Приемник за скриване**
Фотограметрия	Секретно изображение	Цензурирано изображение
	Стереодвойка	Единична аерофотоснимка
Геодезия	DEM с висока резолюция	DEM с ниска резолюция
	(**digital watermark, fingerprinting**)	DEM

	Разнородна нформация	Цифрови карти
Звукообработка	Звуков файл	Изображение
	Звуков файл	Звуков файл
	Изображение	Звуков файл
	Текстов файл	Звуков файл
	Изпълнима програма	Звуков файл
Растерна обработка	Изображение	Изображение
	Звуков файл	Изображение
	Изпълнима програма	Изображение
	Текстов файл	Изображение

2.2. Приложения в стеганографията

Цифровата стеганография се роди като наука буквално в последните няколко години и като такава се развива в различни направления. В този доклад са разгледани само някои от тях, в които може да се приложи представения в точка 2.1 подход за растерна интерпретация на произволни цифрови продукти. Ето някои от тях:

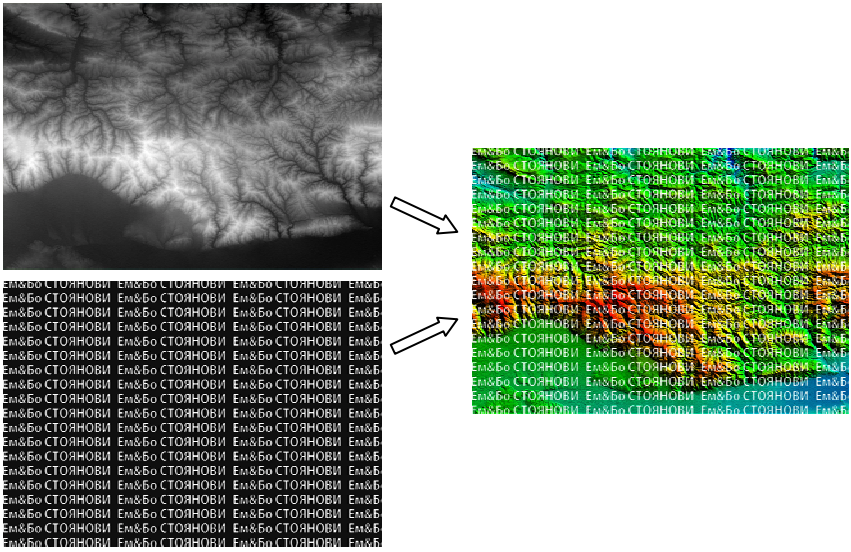
- *защита на авторските права и интелектуалната собственост*
- *скрито предаване на информация (секретни комуникации)*
- *разработване на нови файлови формати и стандарти*

2.2.1. Защита на авторските права и интелектуалната собственост

В съвременните комуникации с бурно развиващи се мултимедийни технологии остро се поставя въпросът за защита на авторските права и интелектуалната собственост върху цифрово представените продукти. Особено актуален става въпросът, когато говорим за цифровата индустрия. Към нея спадат например софтуерната, фотографската, звукозаписната и кино индустрии. Освен това защитата на авторските права е приоритетна област и за много други отрасли, които са само

потребители на цифрови продукти. Такива са автомобило-строенето, самолетостроенето, геодезията, архитектурата и строителството, научно изследователски, военни организации и др.

Предимствата, които дават представянето и предаването на цифрови данни, могат да се окажат засенчени от лекотата, с която е възможно тяхното откradване или модифициране. За това се разработват различни методи за защита, имащи организационно-технически характер. Едно от най-ефективните технически средства за защита на цифрова информация се явява вграждането в защитаемия обект на невидим надпис-етикет (label), който се нарича цифров воден знак (ЦВЗ). Терминът <digital watermark> е бил използван за първи път в работата [7].



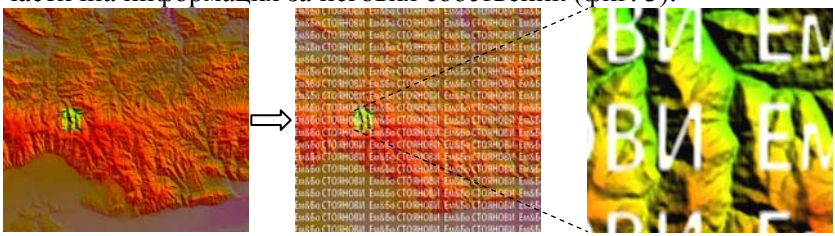
Фиг. 2 Вплитане на watermark-решетка в ЛЕМ

За разлика от обикновените водни знаци ЦВЗ могат да бъдат не само видими, но и (като правило) невидими. Невидимите цифрови водни знаци се анализират от специални декодери, които излизат с решение за тяхната коректност

(автентичност). ЦВЗ може да съдържа в себе си автентичен код, информация за собственика, както и управляваща информация [5]. Най-подходящи обекти за защита с ЦВЗ са неподвижни изображения, файлове с аудио- и видеоданни. В тази връзка, всички цифрови продукти, които могат да се сведат до цифрови изображения, също могат да се защитят с невидим цифров воден знак, указващ техния автор.

На фиг. 2 е показана принципна схема за скриване на <digital watermark> в цифров височинен модел (DEM). **D**igital **E**levation **M**odel представлява цифров модел на част от релефа на земната повърхност, който представя височинната информация в степени на сивото [8]. В него малките височини се представят с по-тъмни нюанси, а големите с по-светли.

В примера watermark представлява черно-бял растер, оформен като ситна (гъста) решетка с повтаряща се информация и насложена върху целия DEM. Това позволява, дори и ако се вземе малка локална област от модела, тя да съдържа пълната или поне частична информация за неговия собственик (фиг. 3).



Фиг. 3 Покритие на *watermark*-решетка върху локална област от

При прилагането на авторския стеганографски метод се наблюдаваха отклонения във височинния модел само от порядъка на 6 мм., което в геодезията се счита за нищожно.

Друга технология, която може да се приложи и има много общо с тази на ЦВЗ, използва вграждане на идентификационен номер от производителя на цифровия продукт. Разликата се заключава в това, че при *<fingerprinting>* всяко защитено копие има вграден уникален идентификационен номер, от където произлиза и названието – буквално *<пръстов отпечатък>*. Тези

номера позволяват на производителите да проследяват бъдещата съдба на своите продукти: не се ли занимава някой от купувачите с незаконно копиране (тиражиране). Ако е така, то <*пръстовият отпечатък*> бързо ще покаже виновника.

Тези методи са приложими във всички отрасли, които се занимават със създаване и комерсиално разпространение на готови цифрови продукти. Прилагането на подхода, описан в точка 2.1, позволява за ЦВЗ и пръстов отпечатък да се използват разнообразни типове източници – текстови, звукови, изображения, кратки видео послания и др.

2.2.2. Приложение в секретните комуникации

Скрити комуникации се използват не само от военни, шпионски и разузнавателни организации, но и от различни държавни институции като Президентство, някои министерства (МВР, МВнР), външна дипломация и др. Не рядко се използват и от бизнесмени, ръководства на държавни и частни фирми с оглед опазване на фирмената тайна, ноу-хау, изобретения и др.

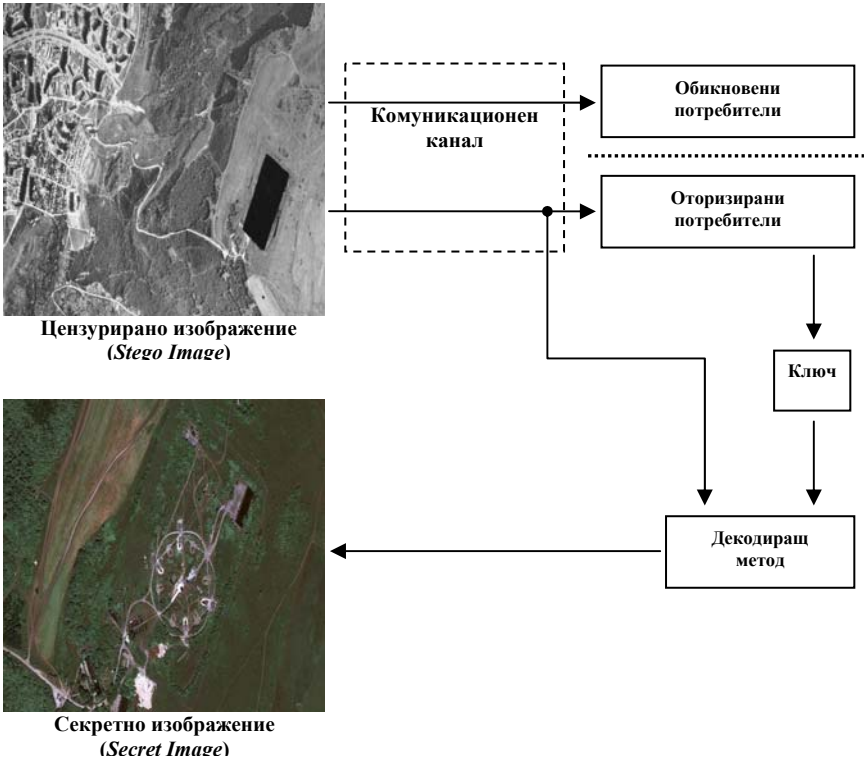
Секретна комуникация може да се осъществява както чрез криптиране на предаваната информация, така и чрез обезпечаване секретността на самия трафик. Перспективен способ за осигуряване секретността на комуникацията е скриването на самия факт, че се осъществява секретна комуникация. Тази идея е залегнала в самата същност на стеганографията – да скрива посланието по начин, който не позволява да бъде видяно [2].

При криптографията е в сила обратният принцип – разбърква се посланието по начин, който не позволява да бъде разбрано. Основен недостатък при използване на криптографията е, че предаването на секретна информация е открито (видимо) за неоторизирани потребители и лесно могат да я прихванат, копират и атакуват.

Отчитайки предимствата и недостатъците на двата метода (криптиране и стеганография), добър подход е съчетаването им за постигане на максимална сигурност и защита.

На фиг. 4 е показано скрито предаване на класифицирана информация чрез достъп до публични данни по общ

комуникационен канал. Например, при заснемане на части от земната повърхност с цел публично предоставяне на тези снимки (напр. Google Earth) в някои от тях могат да попаднат обекти, които са предмет на военна или държавна тайна. В тези случаи се прави цензуриране (маскиране) на онези части от снимките, които разкриват тайната информация.



Фиг. 4 Публичен достъп до цензурирано изображение съдържащо скрита информация

Примерът демонстрира как в цензурирано изображение, което е общодостъпно, може да бъде скрит оригиналният (нецензуриран) вариант на снимката или друга снимка, съдържаща класифицирана информация. По този начин само

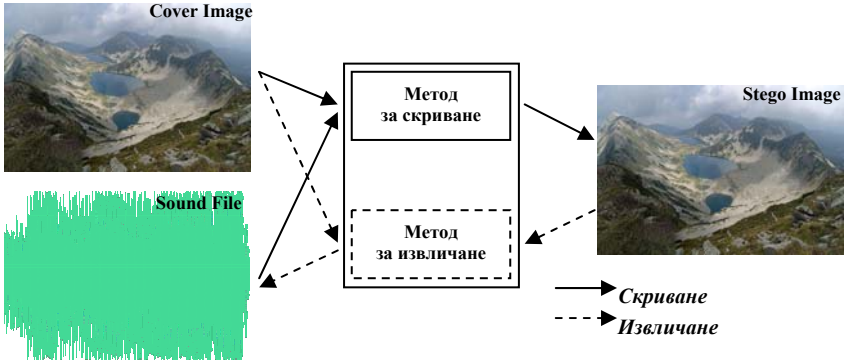
оторизирани потребители ще имат достъп до тази информация, а всички останали – до цензурирания вариант (фиг. 4).

2.2.3. Прилагане на стеганографските методи за разработване на нови файлови формати и стандарти

Описаният в точка 2.1 подход може да се прилага върху всякакъв тип цифрови данни. Тази универсалност може да породи идеи за прилагане на описаната технология и при разработване на нови файлови формати и стандарти. Ето някой от тях.

- ***скриване на звуков файл в изображение***

На фиг. 5 е показана обща схема за вграждане на звуков файл в изображение. Освен скритото пренасяне на звукови данни, друго интересно приложение на тази идея е в бъдеще да се наложи нов графичен формат (контейнер), позволяващ цифровото изображение да бъде придружавано със звуков коментар, музика или информация за неговия автор, вплетени в него.



Фиг. 5 Принципна схема за скриване на звукова информация в изображение

От Таблица 1 се вижда, че методът позволява да се разменят местата на източника и приемника, т.е. да се осъществи обратното скриване – изображение в звуков файл. Единственото

ограничение към носителя е да удовлетворява условията, описани в т. 2.1.

- ***скриване на информация в цифрови карти***

Съвременната цифрова картография представлява процес [8], при който съвкупност от данни се събират и форматират във виртуално изображение. Продукт на цифровата картография са дигиталните карти. Цифрова карта може да се получи или от аналогов първоизточник чрез цифровизация или да е “цифрово родена” (т.е. да няма аналогов дубликат). Независимо от това как са получени, цифровите карти могат да се представят (експортират) като растерни изображения. Обикновено, ако са цветни, се използва RGB системата за представянето на растера. Причината е, че тази система е най-подходяща за мониторна визуализация, тъй като структурно всеки пиксел от повърхността му се състои от три подпиксела – за червен, зелен и син цвят.

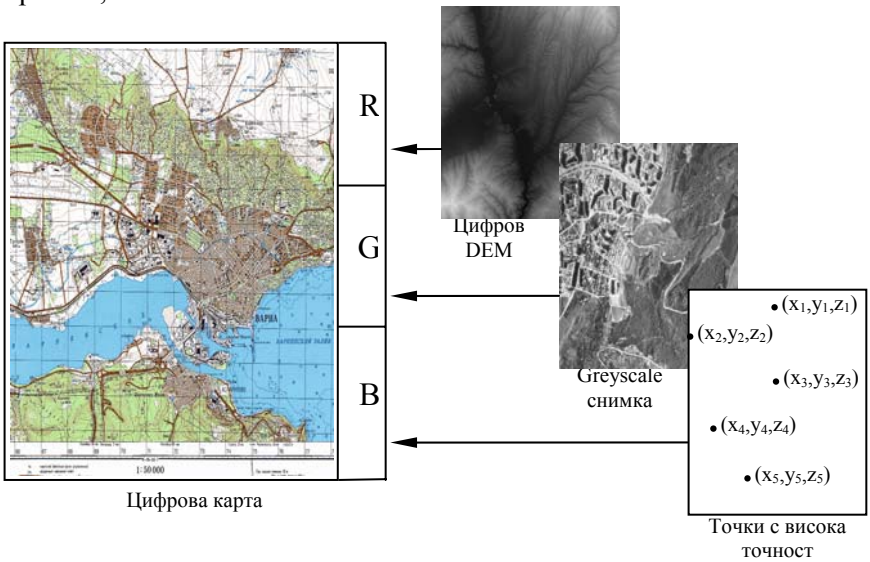
Разглеждането на картите като растерно изображение позволява в тях да бъде скривана и друга информация. Нещо повече, във всеки един от трите цветни канала могат да се скрият различни данни. Такива могат да бъдат цифрови височинни модели (DEM), точки с висока точност (от 1-ви или 2-ри клас), чернобяла снимка на месността, различни слоеве от ГИС и други.

На фиг. 6 е показана схема за вграждане на три различни изображения съответно в R, G и B каналите на цифрова карта. За целта се изисква и трите да са монохромни (т.е. да са представени в Greyscale).

В показания пример цифровата карта може да бъде разглеждана като вид контейнер, в който се съхранява допълнителна информация. Това поражда идеята за разработване на нови файлови формати, които пакетират разнородна, но взаимносвързана информация в един цифров източник.

Въпреки, че описаните по-горе идеи са в противовес с основния принцип в стеганографията – скриване факта на съществуване на друга информация, тази технология може да се използва за контролиране достъпа на потребителите до различни

нива на данни в публично достъпни източници, в зависимост от правата, които имат.



Фиг. 6 Едновременно скриване на разнородна информация в RGB каналите на цифрова карта

3. Заключение

Животът на съвременното информационно общество е немислим без развитието и постиженията на новите цифрови технологии. Големите предизвикателства са най-вече около въпросите за защита на информацията, авторските права и поверителността на комуникацията. Подходът, който бе представен в този доклад, се базира на съвременните стеганографски методи и представлява една стъпка към разрешаването на тези предизвикателства.

ЛИТЕРАТУРА

1. **Neil** F. Johnson, Sushil Jajodia. “Exploring Steganography: Seeing the Unseen”. Computing Practices. //IEEE Press, February 1998, pp.26-34.

2. **T. Aura**, “Invisible Communication”. // EET 1995, technical report, Helsinki Univ. of Technology, Finland, Nov.1995; URL: http://deadlock.hut.fi/ste/ste_html.html.
3. **W. Brown** and B.J. Shepherd, “Graphics File Formats: Reference and Guide”. // Manning Publications, Greenwich, Conn., 1995.
4. **Стоянов** Е., Б. Стоянов, “Един подход за стеганографска защита на цифрови продукти”, Юбилейна научна конференция с международно участие 45 години катедра "Компютърни науки и технологии" и 30 години специалност "Компютърни системи и технологии", ТУ-Варна, 27.09-28.09.2013г., Списание "КОМПЮ-ТЪРНИ НАУКИ И ТЕХНОЛОГИИ", Година XI, Брой 1/2013, с.176-181.
5. **Грибунин** В. Г., Оков И. Н., Туринцев И. В. “Цифровая стеганография” - М., "СОЛОН-Пресс", 2002.
6. **Стоянов** Б., Е. Стоянов, “Обратими растерни трансформации и тяхното приложение в стеганографията”. // Международна научна конференция РУ "Ангел Кънчев" и Съюз на учените в Русе, 31.10.2008-01.11.2008 - гр. Русе., том 47, серия 3.2, с. 84-91.
7. **Osborne** C., van Schyndel R., Tirkel A., “A Digital Watermark”. // IEEE In-tern. Conf. on Image Processing, 1994. P. 86-90.
8. **Стоянов** Е., Б. Стоянов, “Приложение на стеганографията за нуждите на геодезията и цифровата фотограметрия”, MATTEX 2012, 22.11-24.11.2012, ШУ "Еп. К. Преславски".