НОВИ СТЕГАНОГРАФСКИ ПРОГРАМИ В ИНТЕРНЕТ*

СУНАЙ А. АЛИЕВ, ДРАГАН С. ТОНЧЕВ

NEW STEGANOGRAPHIC SOFTWARE IN INTERNET

SUNAY A. ALIEV, DRAGAN S. TONCHEV

ABSTRACT: *The report examines the new software for steganography and steganalysis. There are listed different type of software for steganography and steganalysis. There are presented data from experiments made in the computer lab with specific softwares and technologies. Specifications for different applications are shown in tables with their methods and containers.*

KEYWORDS: *steganography, steganalysis, software, computer steganography, security, steganography tools.*

През втората половина на XX век стеганографията окончателно се превърна от област на специални технически умения, в научно-приложна област и придоби статус на самостоятелна приложна наука, изучаваща способите и методите за скриване на секретни съобщения. Днес лавинообразно се развива нейният клон, наречен компютърна стеганография. Заедно със скриването на информацията винаги остро е стоял и проблема за откриване на скритите канали за предаване на данни и предотвратяване на изтичане на информация (например търговски тайни или лични данни на хората). Поради това заедно с развитието на стеганографията солидна научна основа получи и постоянно съпътстващия я стеганализ, изучаващ методите за разкриване на наличието на скрити съобщения и използването на стеганографски методи [1].

Силният интерес към компютърната стеганография позволи да се реализират много програмни решения в тази област. Днес в Интернет има огромно количество свободно разпространявани и платени софтуерни продукти, използващи стегометоди с графични контейнери. Съществуват много източници за обзор на достъпните стеганографски програми (steganography tools), например [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]. Внедрени са 7 поколения стегопрограми, но подробни описания и анализи има само на тези от първите поколения, които едва ли сега вече някой ще рискува да използва. Тяхното използване е целесъобразно единствено за учебни цели.

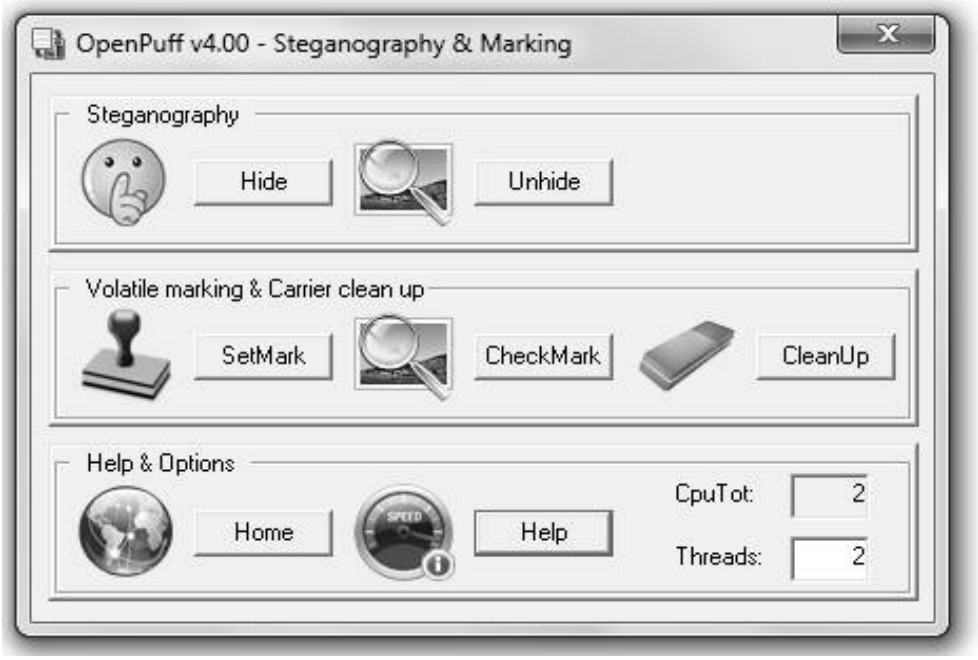
Целта на това изследване е да се разгледат нови достъпни от мрежата софтуерни продукти за стеганография и стеганализ, които не са разгледани подробно в [1]. В продуктите с отворен код графичните формати JPEG и BMP са предпочитани за контейнери. В повечето от програмите се използват методи за вграждане в пространствената област (SD – spatial domain), а други използват трансформационни методи (TD-Transformation domain) – по-конкретно ДКП (DCT). В публикациите относно достъпния софтуер не се използват количествени критерии за сравняване на техните качества [10]. В [3] са разгледани общо 111 стеганографски програми, които се анализират само по типа на стегофайловете, в които скриват съобщения, и по достъпността им (сред тях 30 са open source, 27 са със статут на freeware, 22 – shareware, 8 са комерсиални). В много малко източници се дава архитектурата на стегопрограмите. Интересно е да се отбележи, че в Интернет има публикувани малко

* Разработката е частично финансирана от фонд „Научни изследвания” на Шуменския Университет „Епископ К.Преславски” по проект РД 08-238 / 2014.

оригинални руски стегопрограми [1].

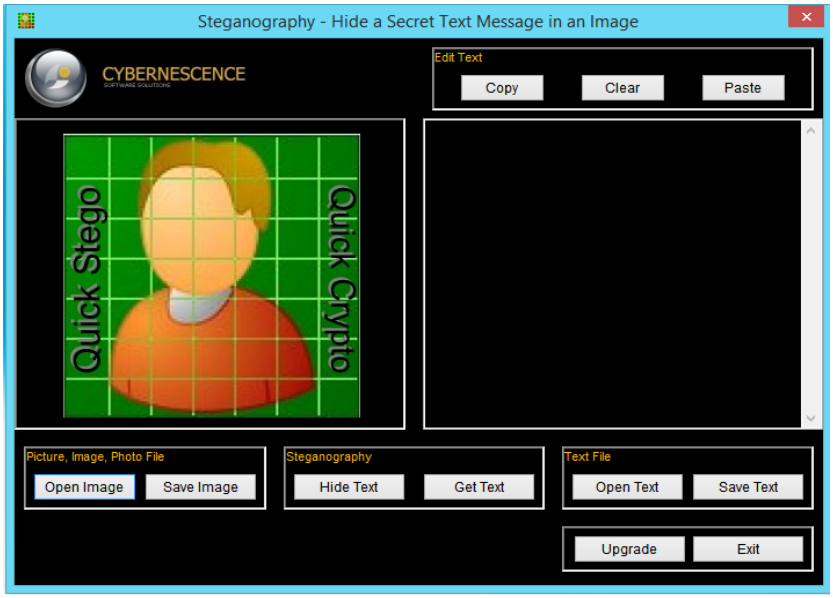
В табл. 1 са дадени данни за използваните контейнери и за лицензния режим на резюмираните програми – търговски (C – Commercial), S – Shareware и свободен F – Freeware.

Една лесна за използване стегопрограма с Shareware лиценз, е Hiderman на A.Raggo. Според мнението на специалистите, полезни за практиката съвременни софтуерни средства, достъпни от Интернет сега, са OpenPuff (фиг. 1) и Our secrets [11]. Open Puff има в състава си модули за криптиране на три нива и т.н. „Контейнер – машина" (carrier engine) за вграждане на съобщения в няколко контейнера [10].



Фиг. 1. Стартов екран на програмата OpenPuff 4.0

QuickStego (фиг. 2) е безплатен софтуерен продукт, позволяващ скриване на текстови съобщения в снмки от различен формат. Снимката със скритата информация е готова да се използва от потребителя – тя ще се зареди като нормално цифрово изображение и единствено друг потребител със тази програма би открил скрито текстово съобщение. Принципът на работа е следния – QuickStego незабележимо променя пикселите (отделните елементи от снимката) на изображението, кодиращи техния текст чрез добавяне на малки вариации в цвета на изображението. На практика, за човешкото око, тези малки разлики не изглеждат че променят изображението, но чрез употребата на продукт като QuickStego тези разлики се откриват и се разбира има ли скрито съобщение или не.



Фиг. 2. Стартов екран на програмата QuickStego

Таблица 1

Програма	Контейнер				Лиценз	Бележки
	BMP	JPG	GIF	Други		
Hiderman					S	A.Raggo
Open Puff	*	*		PNG, TGA, PCK	F	Cosimo Olibomi
Quick Stego					F	
Secret Layer		*			F, C	
Steganography Studio						
StegoVideo						
SilentEye	*	*		WAVE	F	
Xiao Steganography	*	*	*		F	Nakasoft
Our Secretc v.2.5.5 (2013)		*	*		F	

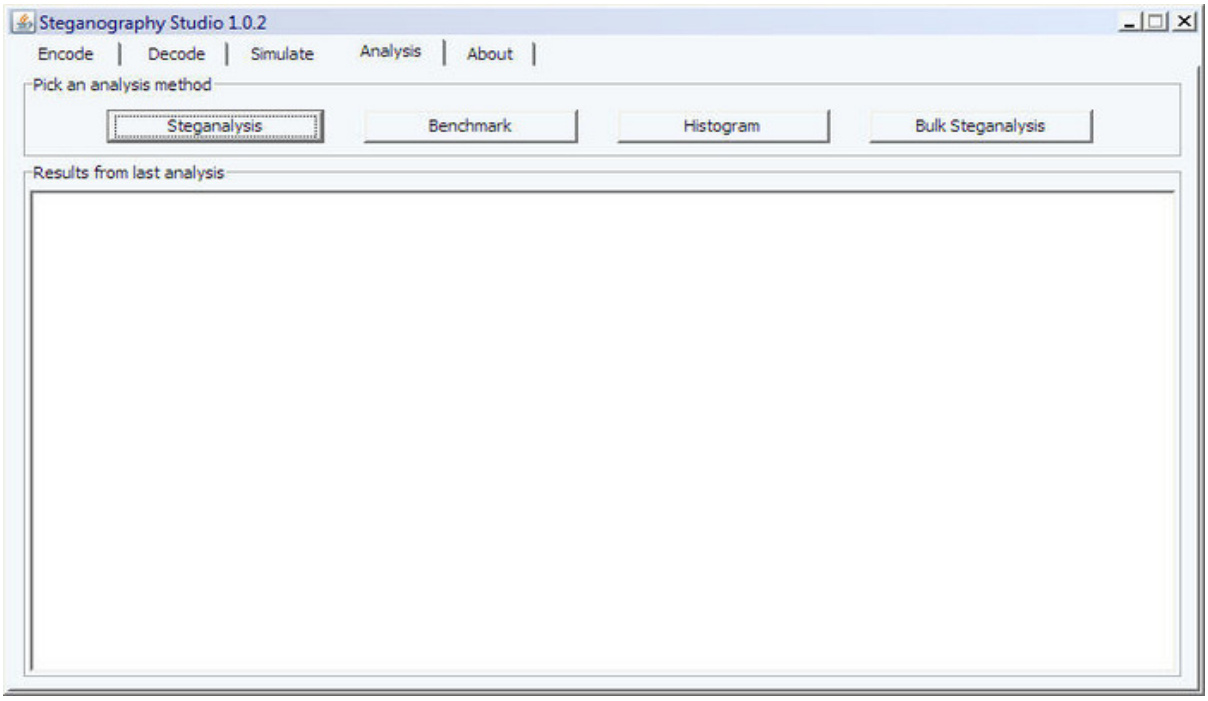
При търсене на ефективна програма се прие условието стеганографска програма, с която се променя размера на стего файла след вграждане на съобщението, да се смята за неподходяща за скриване на съобщения поради вероятността за лесно откриване на присъствието на

SecretLayer Pro на EasySector Software Development Team (фиг. 3). Този продукт позволява на своите потребители да скриват информация в изображения. Програмата работи чрез обработката на пикселите на желаното изображение, в което ще се скрива информация, а именно на много малки сектори от групи пиксели се прилага леко осветяване на техния цвят. Снимката не се променя и дори специалист криминалист не би открил разлика. Нужен ще им е продукт като SecretLayer Pro, за да открият скритата информация. Софтуерът се предлага в две версии – безплатна версия и платена версия. Като разбира, се платената версия поддържа по-голям набор от начини за скриване и кодиране на информация:

- Encryption type: AES, Key length: 128, 196, 256 (bits)
- Encryption type: Blowfish, Key length: 128, 196, 256, 384, 448 (bits)
- Encryption type: Cast-128, Key length: 40, 64, 128 (bits)
- Encryption type: Cast-256, Key length: 128, 160, 192, 224, 256 (bits)
- Encryption type: DES, Key length: 64 (bits)
- Encryption type: IDEA, Key length: 128 (bits)
- Encryption type: RC5, Key length: 64, 128, 192, 256, 384, 448, 512, 1024, 1536, 2040 (bits)
- Encryption type: Twofish, Key length: 128, 192, 256 (bits)

Фиг. 3. Стартов екран на програмата SecretLayer

Steganography Studio (фиг. 4) е мощен инструмент с голям набор от възможности за скриване и анализиране на информация. Подходящ е за потребители, които за първи път се сблъскват със стеганографията и стеганализа, продукт който ще им помогне да научат принципите по които тази наука работи – какви алгоритми използва, как ги реализира на практика. Разполага с едни от най-добрите алгоритми за скриване и откриване на информация. Разработен изцяло на JAVA – може да бъде инсталиран на всяка една операционна система, което го прави лидер в групата на този тип инструменти (http://steganography_studio.en.softonic.com).



Фиг. 4. Стартов екран на програмата Steganography Studio

Xiao Steganography (фиг. 5) е още един водещ софуер за скриване на информация. Работи на принципа на най-младшия бит – LSB, като го сменя или презаписва. Бърз, удобен и лесен за използване от страна на потребителите (http://xiao-steganography.en.softonic.com).

Фиг. 5. Стартов екран на програмата Xiao Steganography

StegoVideo – MSU StegoVideo позволява скриването на всякакъв файл във видео поток. Когато програмата е създадена, бяха анализирани различни известни кодеци и беше избран алгоритъм, който осигурява малка загуба на информация след компресиране на видеото. Може да използвате MSU StegoVideo като VirtualDub филтър или като самостоятелна .exe програма, независимо от VirtualDub (http://compression.ru/video/stego_video/index_en.html).

Съременните тенденции в стаганографията и стеганализа търпят развитие и еволюция на използваните алгоритми и методи за скриване и откриване на информация, етапите на формиране на този тип софтуерни продукти придобива нова концепция за реализиране, тяхното бързодействие, функционалност, защита и приложение – намират своята ниша в отделни работни сфери. В бъдеще повишения интерес към този вид апликации ще доведе до обновяване на вече съществуващите такива продукти и тяхното подобряване. Разгледаните програми може да се използват за сравнение с други програми и при обучението на студенти и специалисти в областта на защитата на данните.

ЛИТЕРАТУРА

1. Станев, С. Стеганологична защита на информацията. Университетско издателство „Епископ Константин Преславски". Шумен, 2013. ISBN 978-954-577-825-4.
2. Cheddad, A. Steganoflage: A New Image Steganography Algorithm.PhD thesis. School of Computing & Intelligent Systems. Faculty of Computing & Engineering.University of Ulster,2009.
3.Hayati, P.,V.Potdar and E. Chang.A Survey of Steganographic and Steganalytic Tools for the Digital Forensic Investigator.[онлайн]. [прегледан 20.05.2013]. http://www.pedramhayati.com/images/docs/ survey _of_steganography_and_steganalytic_tools.pdf.
4. Johnson,N. Steganography software, JJT. [онлайн].[прегледан 22.04.2013]. http://www.jjtc.com/Steganography/tools.html.
5**.** Kessler,G. An Overview of Steganography for the Computer Forensics Examiner .[онлайн].[прегледан1.05.2012].http://www.garykessler.net/ library/fsc_ stego.html.
6. Кеслер, Г. Стеганография для судебного исследователя. Краткий Обзор. [онлайн].[прегледан 06.06.2013]. http://www.bnti.ru/dbtexts/ipks/ old/analmat/1/fors/si.pdf.
7. Steganography tools. [онлайн].[прегледан1.10.2013].http://en. wikipedia.org/wiki/Steganography_tools.
8. Steganography tools. cotse.net [онлайн].[прегледан1.10.2013]. http://www.cotse.com/tools/stega.htm.
9. Computer Forensics, Cybercrime and Steganography Resources Website, Steganography & Data Hiding - Articles, Links, and Whitepapers page. [онлайн]. [прегледан 22.05.2013]. http://www.forensics.nl/steganography.
10. Open Puff 4.00. [онлайн].[прегледан 1.10.2013].http://www.softpedia. com/get/Authoring-tools/Authoring-Related/Puff.shtml.
11. Best Steganography Tools. [онлайн].[прегледан 1.10.2013]. http://www.hackingarticles.in/best-of-haching/best-of-steganography/
13. Stools.http://stools.soft112.com/
14. www.invisiblesecrets.com/download.html
15**.** http://securengine.apponic.com/download
16. http://www.tomsguide.com/us/download/Free-File-Camouflage,0301-49762.html.