СТЕГАНОГРАФИЯ В ОН-ЛАЙН СОЦИАЛНИ МРЕЖИ*

Дениз А. Еминов, Селиме И. Хасанова, Драган С. Тончев

STEGANOGRAPHY IN ON-LINE SOCIAL NETWORKS (OSN)

Deniz A. Eminov, Selime I. Hasanova, Dragan S. Tonchev

ABSTRACT: *This article contains information about how to share secret information in images and how social networks can spread it easily among people . Also some experiments for it are presented.*

KEYWORDS: *Steganography, hiding information , facebook , google +, badoo.*

Социалната мрежа е социална структура, съставена от индивиди (или организации), наречени "Възли", които са обвързани (свързани) с един или повече специфични видове взаимозависимост като приятелство, родство, общи интереси, финансови борси, нехаресвания, вярвания, знания и др. Този термин е въведен първи през 1954 г. от Дж. А. Барнс. Когато комуникацията в социалните мрежи се извършва чрез Интернет, тогава се говори за он-лайн социални мрежи (Online Social Network – OSN) [1]. В доклада съкращението OSN се приема за уеб-базирана услуга, която позволява на хората изграждане на публичен или полу-публичен профил в рамките на ограничена система, артикулиран списък на други потребители, с които те споделят една връзка ,едно виждане в списъка си на връзки и тези, направени от другите в рамките на система" [1]. От първите OSN, стартирани в Интернет през 1999 г. досега са известни над 1000 такива мрежи [2], като списъка на най-популярните 15, е даден в [3], а списъка на 20 от най- интересните според Socialbakers е даден в [4]. В OSN основното представяне на участниците, е чрез профили. Тези профили могат да съдържат информация, като снимки, възраст, местожителство, месторабота, интереси, приятели, семейно положение и др. Чрез тези профили, участниците комуникират помежду си чрез съобщение, статуси, публикации, снимки, видео и др.

Престъпниците от ново поколение, които интегрират технологиите в своите криминални дейности, могат да използват възможностите, които предоставят социалните мрежи, по същите начини, които използват частните или юридически лица [5]. Благодарение на удобството, достъпността и широк обхват на социални медийни платформи като YouTube, Facebook и Twitter, терористични групи все повече използват социалните медии, за да продължат своите цели и разпространяват своите послания. Правени са опити от различни правителства и агенции да осуетят използването на социалните медии от страна на терористични организации [6].

Въвеждането на OSN- социалните мрежи като Facebook дава възможност за контакти с използване на стеганографски методи [7].

Стеганографията е научно-приложна област, съвкупност от технически умения и изкуство за начините за скриване на факта на предаване (наличие) на информация. Тя заема своя ниша в осигуряване на сигурността на предаването на информацията. През втората

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

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. Компютърните технологии вдъхнаха нови сили на стеганографията и днес лавинообразно се развива нейният клон, наречен компютърна стеганография, който съвместно с компютърната криптография е базата за осигуряване на сигурността на компютърната информация От средата на първото десетилетие на XXI век специалистите използват терминът стеганология, обхващащ два смислово противоположни компонента – стеганография и стеганализ [8]. На разработването на нови стеганометоди, алгоритми и софтуер и усъвършенстване на вече съществуващите са посветени множество както явни, така вероятно и много секретни изследвания. Провеждат се конференции и симпозиуми и голяма част от информацията за тях е публична. Чрез Интернет на свободен режим са достъпни вече хиляди компютърни стеганографски приложения. Докато през 2000 година броят на програмите за стеганография в Интернет е бил 140, сега техния брой надхвърля две хиляди. Може само да се предполага какво ще е тяхното увеличение в близките години. Методите на съвременната компютърна стеганология се прилагат в областта на военните и правителствени комуникации, защитата на авторското право, и при решаването на задачите по осигуряване на информационната сигурност.

Ново предизвикателство за специалистите в областта на стеганологията са и социалните мрежи. През май т.г. Pew Research Center публикува доклад, в който се анализира поведението в социалните медии и защитата на личната информация сред тийнеджърите. Според изследването 58% от тях използват подобни техники, за да скриват позицията си в социалните медии, "споделяйки "фирмени шеги" и други кодирани послания, които само техни приятели ще разберат". Ученият Дана Бойд създаде фразата "социална стеганография" която има предвид употребата на споделени социални практики като вид код: за да бъдат скрити послания пред очите на всички, чрез употребата на отправки, които само определени хора могат да разберат [9]. Коментирайки доклада на Pew, Бойд констатира, че той описва показателен съвременен феномен, където много от т.нар. "обитатели на цифровия свят са" изоставили опитите за контролиране на достъпа до съдържание... Вместо това те започват да се фокусират върху контрола на достъпа до смисъла му." Това е промяна с последици, в огромна степен надминаващи областта на поведението в социалните медии на тийнеджърите. Насред продължаващите скандали за масово тайно подслушване и следене на комуникациите, политиката на смисъла – или това, което може да бъде прочетено между редовете, става все по-наложителна. Онлайн вече съществува фин вид социална стеганография. В Китай, където е най-сложната световна система за наблюдение и цензура на Интернет, любимият евфемизъм на държавата за смазване на несъгласните – "he xie", или "хармония" – се е превърнал в таен призив за общ бунт, благодарение на съзвучна игра на думи. Тъй като мандаринският китайски е тонален език, смисълът на думите може да се променя с интонацията на само една сричка. И така леко променено произношение на "хармония" води до фразата "речен рак", измислено създание, използвано като сатиричен инструмент за осмиване на цензурата. За първи път използвана през 2009-а като начин да се избегнат китайските правителствени филтри срещу нецензурните изрази, изписването й в онлайн форуми се е превърнало в подобие на присъединяване към кибер-култ. Този и други дисидентски изрази – най-прочутите китайски примери на политическа игра на думи едва ли биха могли в наши дни да минат за скрити послания. Вместо това те служат за ранни демонстрации на начина, по който хората поемат властта над смисъла онлайн под упоритото наблюдение на властите – и как цензурата и следенето създават плодовита почва за пародии, кодов и езопов език и неписани кодове на съпротивата. Според Бойд,

"криптографите са вманиачени по стеганографията, донякъде защото е най-трудно да разкодираш едно послание, когато не знаеш къде да гледаш." [10].

Начините за споделяне на снимки във Facebook са три, към тях трябва да се прибави и ключовата опция за споделяне на файлове, с която общо възможностите нарастват до четири. Най-често споделяне се извършва, чрез качване на снимки през функцията „Add Fhotos/Video" или чрез създаване на „Album". И двете функции са достъпни от стените, както на лични профили, така и на стените в групи. Друг начин за изпращане на „контейнер" е чрез опцията за изпращане на снимки, чрез съобщения. Все пак и трите предложени начина подлежат на активна атака, чрез компресия, преоразмеряване, промяна на формата и т.н. Единствения способ, който не подлежи на такива атаки е способа за споделяне на файлове в група. Тези файлове не подлежат на никаква модификация от Facebook.

Споделянето на снимки в Google+, е сравнително по-просто от това във Facebook. В Google+ има базова опция за споделяне на снимки „add photo" (добави снимка), но също така има и опцията "+Share" функция. Тук става въпрос за един и същи способ за споделяне, достъпен от различни бутони. Потребителите могат да качат снимка моментално в определения от тях „кръг" или избран албум. Нововъведение е възможността за изпращане на снимки, чрез съобщения. За разлика от Facebook, Google+ не подлага на предварителна компресия качваните снимки. Ако снимката е в съгласие с политиката за качване, то тя е публикувана без допълнителна намеса. Потребителите могат да ограничат достъпа до снимките си или да ги направят видими за всички, или пък само за определени кръгове. „Кръг" в Google+ е подобен на списък с приятели във Facebook, като потребител може да създава неограничен брой кръгове, в зависимост от нуждите си. Кръговете могат да се обособят като приятелски, познати, семейство и т.н. Например ако Алис би искала да сподели изображение, което е „контейнер" със скрита информация, с Боб, тя би добавила Боб, в свой кръг и би му разрешила видимост на своя профил.

Предимството, при използването на Google+ за транспортирането на стеганографски изображения, генерирани от JP Hide and Seek, S-Tools, StegHide, HIP, GIF-it-Up, F5, SteganPEG, SilentEye и т.н. са качени директно, стига те да са във формат JPEG, BMP, PNG или GIF, и да не надвишават 2048 пиксела в широчина или височина. Снимките, са транспортирани, без никаква намеса от страна на платформата. Важно е да се отбележи, че „контейнери" създадени, чрез SilentEye са видимо изменени, което непременно ще събуди подозрителност на даден етап, за това се препоръчва използването на различен софтуер. Също така е препоръчително използването на „контейнери" във формат JPEG, защото той е най-използваният формат в Интернет.

Показаните в [1] резултати от изследвания за възможността за използване на албумите на социални мрежи за стеганографска комуникация, не дават еднозначен отговор. При тестовете с 5 стегопрограми са били използвани графични изображения с различен формат и са качвани в сайтовете на социалните мрежи Facebook и Google+, и след това отново са сваляни оттам, за да се разбере кои методи могат да се използват и кои не могат за скрито предаване в тези мрежи. Резултатите показват че стеганографията трудно може да се използва при качване на фотографии в албуми във Facebook. Скритото съобщение не може да бъде извлечено от снимка, свалена от Facebook, но може да успешно представено чрез прикачени към писмо файлове и фукция групово споделяне на разнообразни графични формати като JPEG, PNG, BMP и GIF. От друга страна, при споделяне на снимки чрез Google+ е бил реализиран успешно целият цикъл на стеганографска комуникация от вграждане до извличане на скрити съобщения със формати JPEG, PNG, BMP и GIF [1].

Свободните стегопрограми, достъпни на пазара, са способни да извършат скриване на информация във файлове JPEG, BMP и GIF и даже PNG. Политиката на OSN обикновено е

да въздейства на размера и формата на изображенията. Ако „качваните" изображения не отговарят на изискванията на мрежата, те или се отхвърлят или автоматично се компресират, изрязват се, реформатират се, променя се размера им от мрежата. Тази модификация е много сериозна за изображенията, в които има вградени съобщения, тъй като всяка от тях може да разруши скритото в нея съобщение, тъй като достъпните стегопрограми на пазара са недостатъчно устойчиви срещу активни атаки.

През 2011 год. са били направени изследвания в три социални мрежи – Facebook, Badoo и Google+. И трите са променяли пикселната резолюция и метаданните на постъпващи в тях изображения, до фиксирани стойности. Facebook и Badoo са приемали само JPEG изображения, докато Google+ JPEG, PNG, BMP и GIF. Обработката на изображенията от мрежите преди тяхното публикуване в албум, е показана в табл. 1 [1].

Таблица 1

Обработка	**Facebook**	**Badoo**	**Google+**
Компресиране	ДА	ДА	НЕ
Промяна на размера	ДА	ДА	Само когато надхвърля изисквания размер
Преобразуване на формата	НЕ на JPEG Останалите формати се преобразуват в JPEG	НЕ на JPEG Останалите формати се преобразуват в JPEG	НЕ
Приемани формати	JPEG	JPEG	JPEG, PNG, BMP , GIF

Може да се направи извода, че от трите социални мрежи, социалната мрежа Facebook е сравнително най-добре защитена срещу използването ѝ за стегокомуникации. Но през 2013 год. студентът Campbell-Moore разработи ново приложение за браузъра Chrome под названието Secretbook. Дотогава използването на изображения в албумите на социалната мрежа Facebook за скриване на съобщения не бе възможно, защото всички изображения се компресират на входа на тази он-лайн социална мрежа (OSN) преди качването им там [7]. Това приложение работи само с браузър Chrome, и засега скриваните текстови съобщения в JPEG изображения не са по-дълги от 140 символа. Secretbook използва декомпресиращ алгоритъм, публикуван от автора му. Когато съобщението трябва да се изпрати, приложението компресира изображението – контейнер по същия начин, по който би го направила мрежата Facebook, след това добавя малко излишни битове към него, и шифрира текста с парола. По този начин се гарантира, че когато Facebook автоматично наново компресира съобщението, промените, които ще бъдат нанесени в него ще бъдат незначителни и съобщението вероятно няма да се повреди много [7].

Отразените в доклада експерименти потвърждават публикуваните в [7] и табл.1 резултати. Те се състоят в скриването на информация във един и същи графичен файл с две програми, качването му във 2 социални мрежи и установяване на промените, които настъпват след смъкването на изображението.

Скриването на информация с програмата Quick Stego версия: 1.2.1 е изключително лесно. Софтуерът единствено дава възможност за скриване на текст в изображение. Когато се вгражда съобщението "Hello world" в снимка IMG_20140909_190448.jpg с програмата

Quick Stego, значително се увеличава размера на стего файла. Началният размер на контейнера - изображение е 910 KB (932 773 bytes), а размера след обработката е 14,0 MB (14 749 696 bytes). Вече обработената снимка е променила типа си в от jpg във Bitmap image (BMP). Повечето социални мрежи не позволяват качването с толкова голям размер. При качването и смъкването на стегофайла в социалната мрежа Фейсбук снимката значително се е променила, като размера след смъкването е 318 KB (326 355bytes).

Откриването на скритата информация се проваля. При опит да се открие скритата информация с друго приложение, не са постигнати никакви резултати.

При качването на стегофайлове в социалната мрежа Facebook, размерът им се променя (смалява). По този начин се губи част от информацията, която съдържат и в този случай извличането на скритото съобщение в изображието е невъзможно.

Все още не съществуват или не са познати добри методи и програми, които да позволят разчитането на скритата информация въпреки промяната във размерите на изображенията.

Подобен експеримент бе направен в OSN Google+. Във файл-контейнер IMG_20140909_190448.jpg с програмата OpenPuff и крипто ключ 123456789, бе вграден файл Hello.txt с размер 12 bytes (съдържание "Hello world"). Началният размер на изображението е 910 KB (932 773 bytes), размера след обработката е 910 KB (932 766 bytes). Тук са настъпили минимални промени на файла относно размера му. Качва се обработеното изображение във соц. мрежа Google+, чрез браузъра Опера, версия 25.0.1614.68. При опит за свалянето му има два варианта на избора – може да се свали оригиналното изображение или подобреното. След сваляне на оригиналното изображение, то има размер 910 KB (932 766 bytes). Изображението не е претърпяло промяна в размера си. Използвайки същата програма и ключ 123456789, се извлича скрития файл Hello.txt, и се прочита същото съдържание. При обработката на снимка с този софтуер няма драстични промени в размера на изображенията. Софтуерът позволява скриването на най-различни типове (doc, txt, jpg,mp3,mp4 и т.н.) във какъвто и да е друг тип (doc, txt, jpg,mp3,mp4и т.н.).

Друг експеримент е направен за проверка дали създателите на софтуерни продукти за електронна поща не са взели мерки за предварителна обработка на прикачените файлове-изображения. Резултатът показва,че при изпращането на стегофайл с пощенското приложение Gmail, размера му не се се губи. Информацията във файла се извлича без проблем със същия софтуер и ключ.

Според публикации в мрежата, най- големите секретни служби сериозно разглеждат проблема за откриване на тайни послания в OSN мрежите. Например на сайта http://www.canyoucrackit.co.uk бе публикуван пъзел – правоъгълник от 160 думи и числа, групирани по двойки в синьо на черен фон, съпроводени от въпроса "Можеш ли да го разбиеш?". Под криптограмата дигитален часовник отброява секундите до края на състезанието. Ако се съди по трафика в "Туитър", "Фейсбук" и ред други социални мрежи и уебсайтове, поне 50 души са успели да решат загадката, откакто тя бе публикувана онлайн. За всеки, който не е обигран криптограф, тя изглежда доста сложна. Агенцията, публикувала пъзела, е една от най-старите и според експерти, най-успешната световна подслушвателна агенция – Правителствената комуникационна централа или GCHQ, разположена в огромна сграда, оградена от огромни сателитни чинии в парк край Челтнъм, на 190 км южно от Лондон. Тя работи с подкрепата на американския си партньор – Агенцията за национална сигурност – NSA, която осигурява достъп до данните от всепроникващата мрежа американски шпионски сателити. GCHQ може да хаква имейли и компютри на практика навсякъде по света. В централата работят експерти, които владеят над 70 езика и наречия, тя играе ключова роля в разкриването на някои от най-мащабните терористични заговори

срещу Запада през последните години. При успешно решаване на онлайн загадката на агенцията, чрез процес, наричан от експертите стеганография, от нея се достига до скрито послание под формата на ключова дума. Този, който въведе ключовата дума, стига до уебадрес, където го очаква поздравление. То е подписано от група, нарекла се Специалисти по киберсигурност – новосформиран отдел в британската агенция, който отговаря за борбата с кибершпионажа [11].

Освен Онлайн социални мрежи (OSN), има много сайтове, които предлагат места за съхранение и споделяне на изображения (снимки, рисунки, cliparts, и т.н.). това са и онлайн фото услуги (OPS). Потребителите могат да публикуват свои собствени изображения, както и да добавят описания и етикети. Чрез регулиране на настройките за защита на личната информация, изображенията стават видими само за оторизирани потребители, след това е възможно да се добави коментар. Като цяло, OSN/OPS мрежите манипулират публикуваните изображения чрез преоразмеряване и обновяване на метаданни, компресиране, вграждане на водни знаци, което прави трудно използването на добре известни стегометоди в тях. В [12] се разглеждат два нови стегометода, които вече се използват за обработка на стегофайлове-изображения преди публикуването им, за да оцелеят след обработката на OSN/OPS. Там е предложена и система от тагове за управление на изпратената и получена информация по секретните канали, която позволява както изтриване на получената информация, така и увеличаване на пропускната способност на тези канали.

Целта на стеганализа е събирането на достатъчно факти за наличието на скрито съобщение и да разбие секретността му. По този начин се унищожава целта на стеганографията – секретната комуникация. Съвременният стеганализ се използва при компютърните съдебни разследвания, в кибервойната, при проследяване на криминални дейности в Интернет и при събиране на доказателства за разследвания [8]. Бяха приложени две стегоаналитични техники, които имат за цел да открият съмнения за използване на стеганография в изображенията. Двете техники, които бяха използвани са: стеганализ основан на принципа на LSB и стеганализ основан на принципа на Pixel Value.Софтуерът, който е използван е Simple Steganalysis Suite. Резултатите могат да изведат след себе си няколко извода. Не винаги,безплатният и популярен стегоаналитичен софтуер може да прихване скрито съобщения. Избраният софтуер не предполага автоматично сканиране на изображения или системата. Безплатният софтуер Simple Steganalysis Suite, който е използван в експеримента, не би могъл да гарантира с голяма точност, дали едно изображение съдържа или не съдържа, скрито съобщение.

Експериментите показаха, че рутинността, която са добили OSN - социалните мрежи в своето използване, се явява проблем, пред защитата от използване на стеганографски способи. Факт, който подкрепя нуждата от изследване на възможностите за стеганография в социалните мрежи е, че тези методи могат да бъдат използвани от хора без специализирано техническо образование.

Бъдещите изследванията могат да се насочат върху това по какъв начин компютърната стеганография може да се приложи в неизследвана социална мрежа. Ще е изключително интересно да се изследват възможностите за комбинация между различните стеганографски техники. Една обещаваща такава техника е разпределението по време и пространство в социалната мрежа или комбинация от социални мрежи.

ЛИТЕРАТУРА

1. Chee, A. Steganographic Techniques on Social Media: Investigation Guideline. [онлайн]. [прегледан 20.10.2013] .http://aut.researchgateway. ac.nz/bitstream/handle/10292/5577/.pdf?sequence=3.
2. List of social networking websites. [онлайн]. [прегледан 15.08.2014] . http://en.wikipedia.org/wiki/List_of _ social_networking_websites .

3. Top 15 Most Popular Social Networking Sites.[онлайн]. [прегледан 5.08.2014]. http://www.ebizmba.com/ articles/social-networking-websites.
4. The 20 Most Interesting Social Networks. [онлайн]. [прегледан 5.08.2014]. http://www.socialbakers.com/resource-center/808-article-the-20-most-interesting-social-networks.
5. Литвинов, Д. и А. Крикунов. Проблема терроризма в сети интернет и методы её решения. [прегледан 8.08.2014]. http://www.sibsiu.ru/antiterror/?p=111.
6. Kohlmann, E. The Antisocial Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations. [онлайн]. [прегледан 5.10.2014]. http://homeland.house.gov/sites/homeland.house.gov/files/ Testimony%20Kohlmann%5B1%5D.pdf.
7. Steganography Now On Facebook. [онлайн]. [прегледан 20.06.2014]. http://www.pentagonpost. com/ steganography-now-on-facebook/8346042.
8. Станев, С. Стеганологична защита на информацията. Университетско издателство „Епископ Константин Преславски". Шумен, 2013. ISBN 978-954-577-825-4.
9. Новите тайни социални кодове на Интернет. [онлайн]. [прегледан 20.08.2014]. http://www.webcafe.bg/id_939656193_Novite_tayni_sotsialni_kodove_na_Internet.
10. Boyd, D. Social Steganography: Learning to Hide in Plain Sight. [онлайн]. [прегледан 20.08.2014]. http://www. zephoria.org/thoughts/archives/2010/08/23/social-steganography-learning-to-hide-in-plain-sight.html.
11. [онлайн]. [прегледан 20.06.2014]. http://www.segabg.com/article.php?sid=20111209000400013 01.
12. Castiglione, A. Steganography and Secure Communication on Online Social Networks and Online Photo Sharing. [онлайн]. [прегледан 20.06.2014]. http://www.informatik.uni-trier.de/~ley/pers/hd/c/Castiglione:Aniello

ДРОНОВЕТЕ, БЪДЕЩЕТО, КОЕТО ТЕ ОБЕЩАВАТ НА ОБЩЕСТВОТО*

ДЕНИЗ А. ЕМИНОВ, СЕЛИМЕ И. ХАСАНОВА, ГЮНЕР И. ЗЕКЕРИЕ

DRONES, THE FUTURE WHICH THEY PROMISE TO SOCIETY

DENIZ A. EMINOV, SELIME I. HASANOVA, GYUNER I. ZEKERIE

ABSTRACT: *The article presents the use of drones as a major technique in guarding and use of capacity in our modern time. The use of drones would save time, human resources, even human life. Their distribution is just beginning and development they first occur.*

KEYWORDS: *drones,future,buildings,security,wi-fi,solar panels,nature disasters,movements.*

Дроновете слагат начало на нов бранш, който се развива с бързо темпо в световен мащаб. Дори в някои области на света се бележи бум на използването на такъв вид летателна апаратура. Тя е съставена от няколко на брой перки (множество), които поддържат платформата във въздуха без тя да пада. Те са с малки размери и дистанционно управление чрез станции, чрез интернет връзка, WI-FI или просто застопорени в една точка, откъдето да наблюдават и работят спрямо обекти. Някои от въздухоплавателните средства са много издръжливи, предназначени за множество излитания и кацания. Те са в състояние да летят при силни насрещни ветрове, турболенция и дори при лоши метеорологични условия.

* Тази статия е разработена по проект от фонд Научни изследвания на ШУ "Епископ Константин Преславски" РД-08-235/13.03.2014 г.