Volodymyr Mosorov

STEGANOGRAFIA CYFROWA

SZTUKA UKRYWANIA INFORMACJI

WYDAWNICTWO UNIWERSYTETU ŁÓDZKIEGO

STEGANOGRAFIA CYFROWA

WYDAWNICTWA
UNIWERSYTETU
ŁÓDZKIEGO

Volodymyr Mosorov

STEGANOGRAFIA CYFROWA

SZTUKA UKRYWANIA INFORMACJI

WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

ŁÓDŹ 2013

Volodymyr Mosorov – Uniwersytet Łódzki, Wydział Ekonomiczno-Socjologiczny
Katedra Informatyki Ekonomicznej, 90-255 Łódź, ul. P.O.W. 3/5
wmosorow@uni.lodz.pl

RECENZENT

Ewa Ziemba

REDAKTOR WYDAWNICTWA UŁ

Katarzyna Gorzkowska

SKŁAD I ŁAMANIE

AGENT PR

OKŁADKĘ PROJEKTOWAŁA

Barbara Grzejszczak

Wydane przez Wydawnictwo Uniwersytetu Łódzkiego
Wydanie I. W.06384.13.0.M

ISBN (wersja drukowana) 978-83-7969-082-4
ISBN (ebook) 978-83-7969-273-6

Wydawnictwo Uniwersytetu Łódzkiego
90-131 Łódź, ul. Lindleya 8
www.wydawnictwo.uni.lodz.pl
e-mail: ksiegarnia@uni.lodz.pl
tel. (42) 665 58 63, faks (42) 665 58 62

SPIS TREŚCI

WSTĘP

Steganografia jest sztuką ukrywania informacji w sposób, który uniemożliwia wykrycie schowanego przekazu. Głównym celem steganografii jest niewzbudzanie podejrzenia co do istnienia przesyłanej ukrytej wiadomości. Steganografia i kryptografia należą do tej samej rodziny metod bezpiecznego przekazywania informacji. Kryptografia zmienia treść wiadomości w taki sposób, że staje się ona nieczytelna dla postronnego obserwatora. Jednakże zawsze jesteśmy w stanie odszyfrować każdą wiadomość zaszyfrowaną za pomocą znanych technik kryptograficznych. W przeciwieństwie do kryptografii, steganografia ukrywa fakt istnienia wiadomości. Zaszyfrowany tekst może wzbudzać podejrzenia, w przeciwieństwie do „niewidzialnej" wiadomości, stworzonej przy użyciu steganografii.

Techniki steganograficzne doskonaliły się przez wieki, jednak największy przełom nastąpił wraz z intensywnym rozwojem systemów i technik informatycznych. Powszechną cechą współczesnej steganografii jest wykorzystanie publicznych, ogólnodostępnych mediów do przesłania wiadomości. Dzisiejsi szpiedzy czy terroryści nie przenoszą już wiadomości na mikrofilmach, rzadko drukują ogłoszenia w gazetach. Zwykle przekazują informacje za pomocą ogólnie dostępnych mediów – takich jak np. radio, telewizja czy Internet. Miliony anonimowych internautów, niezliczona ilość informacji, strony WWW, które pojawiają się i za chwilę znikają – wszystko to tworzy chaos, w którym nikt nigdy nie będzie w stanie znaleźć ukrytej wiadomości.

Według ekspertów członkowie ekstremistycznych organizacji są w rzeczywistości ludźmi dobrze wyszkolonymi w technikach informatycznych. Niektórzy specjaliści uważają, że atak terrorystyczny we wrześniu 2001 r. na budynki World Trade Center był możliwy m.in. dzięki zastosowaniu przez terrorystów nowoczesnych technologii, do których należy steganografia.

Niniejsza publikacja jest próbą przybliżenia Czytelnikowi metod oraz oprogramowania steganograficznego, przeżywających w ostatnich latach burzliwy rozwój. Celem autora jest wykazanie, że steganografia to skuteczne narzędzie, pozwalające chronić przekazywane w sieciach komputerowych poufne informacje nadawane przez instytucje zarówno państwowe, jak i komercyjne oraz chronić

życie prywatne od ingerencji i monitorowania jakichkolwiek osób trzecich.

Opracowanie składa się z siedmiu rozdziałów, wstępu i zakończenia. W rozdziale pierwszym opisano podstawowe pojęcia dotyczące omawianego zagadnienia. Przestawiono w skrócie historię powstania steganografii, wskazano wady i zalety tej techniki w porównaniu z technikami kryptograficznymi.

Rozdział drugi przedstawia obszerny przegląd istniejących metod steganograficznych. Wyjaśniono zasady jej działania dla poszczególnych rodzajów nośników, takich jak pliki multimedialne i pliki tekstowe.

W rozdziale trzecim Czytelnik znajdzie obszerną analizę istniejącego oprogramowania steganograficznego. Podział oprogramowania został wykonany według rodzajów plików, które będą wykorzystane do ukrywania poufnych treści.

Czwarty rozdział przedstawia osobny rodzaj steganografii, mianowicie steganografię sieciową. W odróżnieniu od poprzednio omawianych rodzajów steganografii, tu wykorzystuje się ukrywanie danych w informacji dodawanej do pakietów wysyłanych poprzez sieci komputerowe. Przy takim rozwiązaniu nie jest wymagany nośnik (plik).

W rozdziale piątym opisano historię i zastosowania cyfrowych znaków wodnych, które mogą posłużyć do udowodnienia praw autorskich w zakresie grafik multimedialnych. Omówiono współczesne sposoby oznaczenia takiego rodzaju plików znakiem wodnym.

Rozdział szósty przybliża steganoanalizę – proces odwrotny do steganografii, polegający na wykrywaniu, czy dany obiekt zawiera ukrytą informację. Czytelnik ma możliwość zapoznania się z metodami i narzędziami służącymi do odnajdywania i odczytywania utajnionych informacji.

Ostatni rozdział zawiera praktyczne przykłady zastosowania metod steganograficznych w handlu elektronicznym. Opisuje, w jakich dziedzinach i dlaczego powinno się wykorzystywać techniki ukrywania danych.

Volodymyr Mosorov

1. PODSTAWY STEGANOGRAFII

1.1. Istota i definicje steganografii

Pojęcie *steganografia* wywodzi się ze słów w języku greckim: *steganos* ('potajemny' lub 'ukryty') i *grapho* ('piszę' bądź 'rysuję') [27]. W najszerszym rozumieniu pojęcie to oznacza ukryte pismo, bez względu na to, czy chodzi o niewidzialny atrament na papierze, czy też informacje poufne ukryte w pliku multimedialnym. Pojęcie „ukrywania informacji" po raz pierwszy zostało sformułowane w 1972 r. przez D. Parnasa w pracy *On the criteria to be used in decomposing systems into modules* [43].

W niniejszej publikacji pod pojęciem **steganografii** będziemy rozumieć dział wiedzy zajmujący się utajnianiem informacji poprzez ich ukrycie w innych informacjach. Niektórzy autorzy podają podobne definicje steganografii, traktując ją jako technikę ukrywania informacji w innych informacjach [26, 42]. Lecz taka definicja steganografii – jako techniki – znacząco zawęża jej istotę, sprowadzając steganografię do elementu składowego nauk kryptograficznych. Niniejsza publikacja traktuje steganografię jako osobno rozwijającą się dziedzinę naukową, zajmującą się zarówno teoretycznymi, jak i praktycznymi aspektami ukrywania pewnych informacji w innych informacjach.

Obecnie steganografia jest zwykle kojarzona z jej zaawansowaną technicznie odmianą – *steganografią cyfrową*, która polega na ukrywaniu danych w pliku elektronicznym. Jeśli kryptografia przekształca informację w zaszyfrowany kod, żeby ukryć jej znaczenie, to steganografia całkowicie kamufluje sam fakt ukrywania danych. I tak np. w celu ukrycia informacji można nieznacznie modyfikować pliki graficzne i dźwiękowe, nie zmniejszając ich ogólnej użyteczności dla widza bądź słuchacza. W przypadku dźwięku można wykorzystać te części pliku, które mieszczą w sobie dźwięki niesłyszalne dla ludzkiego ucha. W przypadku grafiki można usunąć nadmiarowe informacje o kolorze, żeby otrzymać obraz, który wygląda na nienaruszony i który niełatwo jest odróżnić od oryginału. Im lepsza jakość obrazu bądź dźwięku, tym więcej zawiera on nadmiarowych danych, toteż największą popularnością cieszą się 16-bitowe pliki

dźwiękowe i 24-bitowe pliki graficzne. Jeśli osoba, która próbuje przechwycić ukrytą wiadomość, nie dysponuje oryginalnym plikiem graficznym bądź dźwiękowym, to na ogół nie będzie mogła stwierdzić, czy dany plik zawiera tylko obraz lub dźwięk, czy też ukryte są w nim pewne dane.

Rys. 1.1. Ogólny schemat działania programu steganograficznego

Źródło: opracowanie własne

Ważniejsze terminy występujące w steganografii to [16]:

• wiadomość do ukrycia lub stegotekst – tajna informacja do ukrycia,

• nośnik lub przykrywka (ang. *cover*) – plik, w którym prawdziwa informacja jest ukrywana,

• osadzanie (ang. *embedding*) – proces ukrywania stegotekstu w nośniku,

• wyodrębnianie (ang. *extracting*) – proces odzyskiwania ukrytej informacji,

• stegosystem – system steganograficzny,

• steganoklucz (ang. *steganokey*) – klucz do odszyfrowania tekstu ukrytego przy pomocy steganografii.

Reasumując – wiadomością do ukrycia może być nie tylko tekst czy steganotekst, lecz także plik graficzny, dźwiękowy lub wideo. Objętość ukrywanego pliku medialnego jest ściśle powiązana z wielkością pliku nośnika, toteż niemożliwe jest ukrycie pliku wideo w pliku tekstowym. Zmiany, jakie niesie za sobą umieszczenie wiadomości w pliku nośnika są nieuchwytne dla ludzkich zmysłów. Ogólny schemat działania programu steganograficznego jest pokazany na rys. 1.1.

Jeden z pierwszych przykładów wykorzystania steganografii, opisany przez Herodota, przypisuje się niejakiemu Histiajosowi. Potrzebował on sposobu na przesłanie tajnej wiadomości do swojej armii drogami kontrolowanymi przez nieprzyjaciela. W tym celu ogolił głowę niewolnikowi i wytatuował informację na gołej skórze. Gdy odrosły włosy, niewolnik dostarczył wiadomość [9].

Metody ukrywania wiadomości, takie jak pisanie między wierszami dokumentu niewidzialnym atramentem sporządzonym z mleka lub soku, który uwidacznia się dopiero po podgrzaniu, były stosowane już w starożytnym Rzymie. W 1499 r. Trithemius ogłosił dzieło zatytułowane *Steganographia* [20]. Jest to jedna z pierwszych książek poświęconych tej dziedzinie. W czasie II wojny światowej Niemcy używali mikrokropek, by ukrywać dane w znakach interpunkcyjnych w papierowych dokumentach.

Przy pewnych założeniach za odmianę pisemnej steganografii możemy uznać stenografię (gr. *stenós* 'ciasny', *gráphein* 'pisać') – jest to skrócona, symboliczna metoda zapisu, zwiększająca jego szybkość i zwięzłość w porównaniu z tradycyjnymi dla danego języka metodami. Stenografia cieszyła się znacznie większą popularnością w przeszłości, przed wynalezieniem przenośnych urządzeń do nagrywania głosu. Metody stenograficzne były wykorzystywane albo do zapisu bieżącej mowy, albo do usprawnienia pracy biurowej i dziennikarskiej. Zapisywanie informacji poufnych w postaci stenogramu pozwalało ukryć treść przez osobami trzecimi w miejscach publicznych.

W dzisiejszych czasach steganografia zdobywa coraz większą popularność w Internecie. Wykorzystywana jest do ukrywania informacji poufnych oraz do ukrywania znaków towarowych w obrazach i muzyce, co definiuje się mianem elektronicznych znaków wodnych (więcej na temat znaków wodnych w rozdziale piątym). Kiedy stosując komercyjne rozwiązania możemy przypuścić, że odpowiednie służby są w stanie odczytać zaszyfrowane informacje, steganografia elektroniczna może realnie okazać się jednym z ostatnich bastionów prywatności we współczesnym świecie Internetu.

Programy do ukrywania informacji można bezpłatnie pobrać z Internetu. Istnieje duża liczba aplikacji dla różnych systemów operacyjnych. Te aplikacje wyposażone są w interfejsy graficzne i umożliwiają proste ukrywanie danych w różnorodnych formatach plików. Opracowano też kilka komercyjnych pakietów steganograficznych. Rosnąca liczba rozwiązań komercyjnych świadczy o tym, że rynek dojrzewa do stosowania tej technologii, a firmy są gotowe za nią płacić.

W zależności od prowadzonej działalności, firmy i przedsiębiorstwa nie zawsze potrzebują steganografii. Gdy jednak zachodzi potrzeba ukrycia poufnych danych, które są tajemnicą firmy i mogą być znane tylko wąskiej grupie pracowników, steganografia okazuje się bardzo przydatna.

Steganografia używana jest podczas działań wojennych przez służby wywiadowcze. Należy jednak podkreślić, że wiele technologii, które przynoszą korzyści społeczeństwu, ma również negatywne lub kryminalne zastosowania. Mogą jej także używać dilerzy narkotyków i inni kryminaliści, więc czasem bywa postrzegana negatywnie.

Wskutek debaty dotyczącej kontroli nad eksportem technologii szyfrowania, steganografia jest dobrą metodą na ukrywanie typu przesyłanych danych. Jeżeli nikomu nie wiadomo, jakiego rodzaju dane są przesyłane, nie ma znaczenia, iloma kluczami zostały zaszyfrowane.

1.2. Zalety steganografii

Steganografia jest wyjątkowo przydatnym narzędziem wówczas, gdy zainteresowani dysponują ścieżką komunikacji. Na przykład, jeżeli ktoś pracuje w wywiadzie wojskowym i szpieguje np. na rzecz Rosji, sam fakt regularnego porozumiewania się z ambasadą tego państwa byłby niezwykle podejrzany, bez względu na rodzaj przekazywanych danych. Skoro w takim przypadku bezpośrednia komunikacja jest niemożliwa, szpieg może przesyłać informacje do jednej z licznych grup dyskusyjnych, serwerów FTP w Internecie albo tablic ogłoszeniowych. Ukrywa dane w pozornie nieistotnym pliku i wysyła ją w ustalone miejsce. Jego partner odwiedza odpowiednią witrynę, pobiera plik, wyodrębnia ukrytą informację i odczytuje ją. Rozwiązanie tego typu określa się mianem cyfrowej skrzynki kontaktowej.