Volodymyr Mosorov, Marian Niedźwiedziński

Zastosowanie metod cyfrowej steganografii w handlu elektronicznym

Ekonomiczne Problemy Usług nr 87, 722-730

2012

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 702 EKONOMICZNE PROBLEMY USŁUG NR 87 2012

VOLODYMYR MOSOROV, MARIAN NIEDŹWIEDZIŃSKI
Uniwersytet Łódzki

ZASTOSOWANIE METOD CYFROWEJ STEGANOGRAFII W HANDLU ELEKTRONICZNYM

Wprowadzenie

Rozwój informatyki i sprzętu komputerowego w drugiej połowie XX wieku spowodował, że sposób przekazywania informacji stał się prostszy, niezależny oraz wygodniejszy. Przykładem tego postępu jest handel elektroniczny (*e-commerce*), który dzięki rozwojowi sieci komputerowych, a zwłaszcza Internetu, stał się bardzo popularnym sposobem przeprowadzania różnych transakcji. Obecnie, nie wychodząc z domu, można kupić prawie każdy produkt, opłacić rachunki i sprawdzić swoje konto bankowe za pomocą formularzy elektronicznych zamieszczonych na stronach WWW. Ta łatwość przekazywania informacji handlowych spowodowała, że informacje te stały się dostępniejsze dla osób nieupoważnionych, co z kolei sprawiło, że pojawiło się pytanie, jak zabezpieczyć ważne dane handlowe przesyłane drogą elektroniczną.

Jednym z rozwiązań alternatywnych dla dobrze znanych metod kryptograficznych jest cyfrowa steganografia[1]. Steganografią nazywamy komunikację w taki sposób, by nie mogła być wykryta obecność przesyłanego komunikatu. W kryptografii obecność komunikatu nie jest negowana, natomiast steganografia ukrywa fakty prowadzenia komunikacji. Możliwości ukrywania informacji handlowych w postaci danych elektronicznych jest bardzo dużo. Informacja może być ukrywana

[1] I. Cox, M. Miller, J. Bloom, J. Fredric, T. Kalker, *Digital Watermarking and Steganography*, 2nd Ed. electronic free book, http://www.freeebookdownload.co.in/ebooks/free-ebook-Digital-Watermarking-and-Steganography-2nd-Ed-The-Morgan-Kaufmann-Series-in-Multimedia-Information-and-Systems--download 2009

prawie we wszystkich typach danych, nie tylko w tekście, ale np. w obrazie JPG, mapie bitowej BMP, pliku audio WAV albo plikach wideo. Informacja ta niekoniecznie musi być tekstem, ukryć w ten sposób można także zdjęcie.

W pewnym stopniu przykładem steganografii są techniki cyfrowych znaków wodnych. Cyfrowym znakiem wodnym nazywamy zintegrowane z plikami graficznymi, wideo lub audio dodatkowe informacje. Informacje te mogą być niewidoczne dla użytkownika, a mogą być odczytane tylko przez dedykowane programy. Podczas sprzedaży produktów multimedialnych przez Internet wykorzystywane są one w celu ochrony praw autorskich[2].

1. Metody steganograficzne w handlu elektronicznym

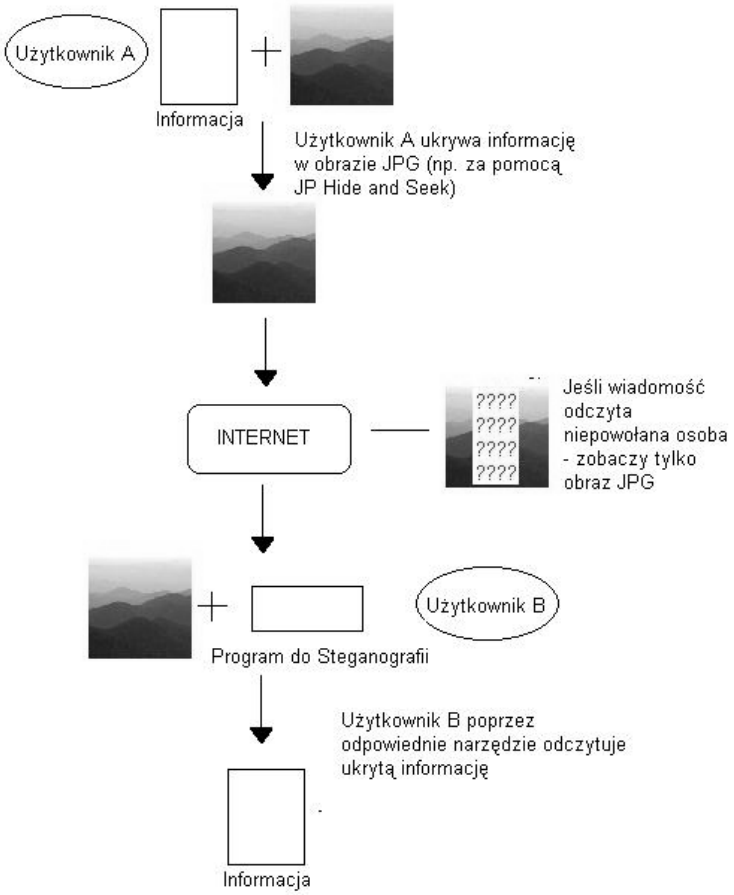
Steganografia ma ogromne znaczenie w procesie zabezpieczania transmisji danych, szczególnie danych gospodarczych pomiędzy stronami handlującymi ze sobą. Schemat procesu ukrywania informacji jest pokazany na rysunku 1. Przykładową aplikacją wykorzystującą steganografię dla bezpiecznej komunikacji jest program *StegComm*^{TM}. Aplikacja wykorzystuje technikę steganografii, czyli ukrywanie informacji w różnych plikach danych (obrazach, plikach dźwiękowych itp.). Umożliwia również łączenie kryptografii z steganografią w celu zabezpieczenia informacji. *StegComm*^{TM} nie zmienia rozmiaru pliku z ukrytą informacją podczas szyfrowania oraz zapewnia integralność danych po rozszyfrowaniu, co zapobiega skasowaniu informacji ukrytych w najmniej znaczących bitach pliku. Dzięki takiemu rozwiązaniu, nawet jeśli plik z ukrytą informacją (np. bardzo ważną informacją biznesową) zostanie rozszyfrowany przez hakera, to bez wiedzy, jak została ukryta informacja (tzw. stegoklucz), plik będzie dla niego bezużyteczny.

Steganografia jest również skuteczna w uwierzytelnianiu klientów w sieci[3]. Przykładową aplikacją łączącą steganografię z uwierzytelnianiem cyfrowym (podpisem elektronicznym) jest *StegSign*^{TM}. Aplikacja ta potrafi w różnych plikach (m.in. w mailach, dokumentach tekstowych itp.) ukryć dane firmy albo inne poufne dokumenty. Dzięki temu, jeśli ktoś niepowołany będzie ingerował w przesyłane pliki z tak ukrytymi danymi, wysyłający i odbierający te pliki zostaną o tym poinformowani (np. podczas przesyłania informacji handlowych w fazie rokowań).

---

[2] P. Wayner, *Disappearing cryptography 3rd Edition, information hiding, steganography & watermarking*, Amsterdam, MK/Morgan Kaufmann Publishers 2009.

[3] www.datamark.com.sg/pdf/steganography.pdf

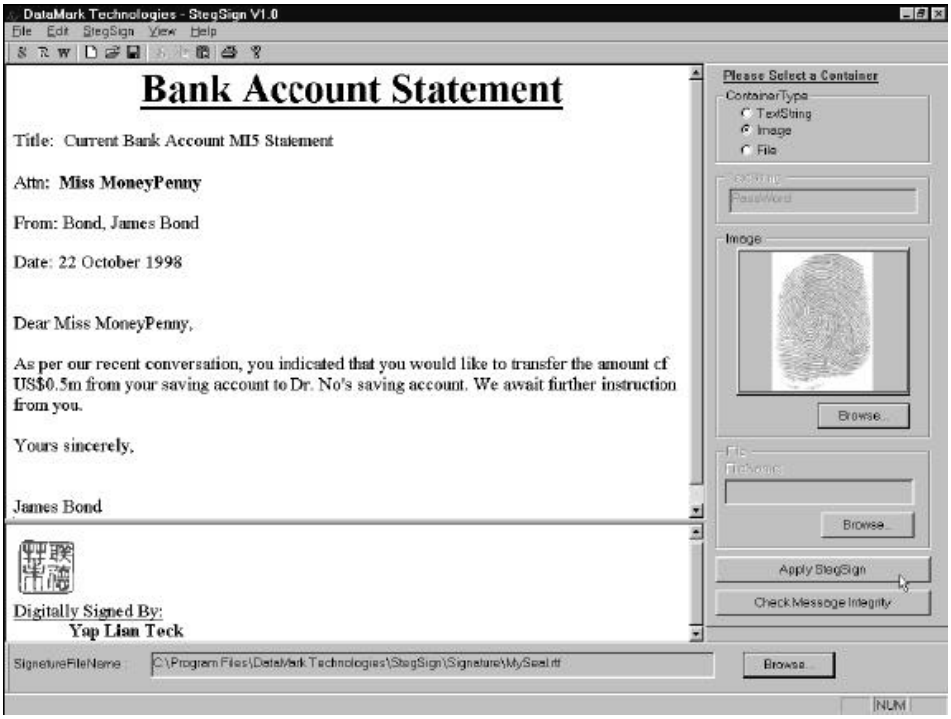


Rys. 1. Schemat procesu ukrywania informacji w zdjęciu JPG

Źródło: opracowanie własne.

Aplikację *StegSign*^{TM} można stosować również w celu zabezpieczenia przed nieupoważnionym dostępem do danych. Przykładem tego typu zastosowania aplikacji może być e-banking, gdzie podpis elektroniczny uwierzytelnia zarówno bank, jak i klienta.

Przykładowe okno aplikacji *StegSign*^{TM} pokazano na rysunku 2.



Rys. 2. Przykładowe okno aplikacji *StegSign*^{TM} stosowanej w bankowości elektronicznej

Źródło: opracowanie własne.

Inną aplikacją mającą za zadanie ochronę praw autorskich jest system *DRM* (*Digital Rights Management* – Zarządzanie prawami cyfrowymi). System ten daje możliwość:

- zabezpieczenia różnych treści multimedialnych przed użytkownikami, którzy korzystają z nich w sposób niezgodny z założeniami dostawcy,
- kontrolowania dostępów do cyfrowych danych.

Prawa, które są nadawane przez autorów różnych treści multimedialnych, dotyczą między innymi:

- zamian formatów plików,
- możliwości ponownego odtwarzania,
- kopiowania.

Przed przekazaniem danego pliku multimedialnego do odbiorcy jest on w systemie DRM wcześniej zabezpieczany przed odczytem. Jedynie posiadanie licencji daje możliwość jego odtworzenia. Aby uzyskać licencję i wygenerować klucz deszyfrujący, należy użyć programu, który służy do odtworzenia plików multimedialnych. Aby uniemożliwić odtworzenie procesu oraz zachowanie tajności jego szczegółów, należy zastosować szereg zabezpieczeń, które utrudnią poznanie

zasady działania programu. Nie do końca zostaje zapewnione bezpieczeństwo, czego świadectwem są programy, które w łatwy sposób pozwalają na ominięcie zabezpieczeń stosowanych w systemach DRM. Aby dany użytkownik mógł zdobyć licencję, musi spełnić wiele warunków, które są z góry ustalone. Najczęściej stosowanym warunkiem jest uiszczenie należności finansowej za dany plik.

Na rynku jest dostępnych wiele aplikacji, które pozwalają realizować zadnia systemu DRM. Przykładem takiej aplikacji jest produkt firmy Microsoft o nazwie *Windows Media DRM*. Platforma ta pozwala na zabezpieczenie i ochronę treści multimedialnych, które są przesyłane do odbiorców. Daje możliwość również odtworzenia treści multimedialnych na urządzeniach sieciowych i przenośnych, a także na zwykłych komputerach typu PC.

Do najczęściej stosowanych usług pobierania chronionych zawartości stosuje się:

- sposób pośredniego pobierania licencji – polega na możliwości przesyłania plików multimedialnych wraz z licencją na te materiały na urządzenia mobilne, np. telefony komórkowe, tablety,
- sposób bezpośredniego pobierania licencji – pobieranie plików multimedialnych oraz programów wraz z licencjami bezpośrednio z Internetu na urządzenia mobilne (tablety, telefony komórkowe). Przykładem takiego rozwiązania może być portal Android Market, który umożliwia kupno i pobranie ponad 300 tys. aplikacji na urządzenia z systemem Android.

Najczęściej stosowanymi usługami w sektorze biznesowym e-commerce są usługi licencji – segment handlu elektronicznego, który umożliwia dostarczanie licencji na oprogramowanie. Usługi te mogą działać w schemacie B2B lub B2C. Przykładem rozwiązania dostarczającego takich usług jest Microsoft Open License Program, który umożliwia kupno licencji na oprogramowanie firmy Microsoft, pobranie licencji oraz oprogramowania z dedykowanego portalu usługi MOLP (*Microsoft Open License Pack*[4]).

Inny pomysł na zaspokojenie potrzeb rynkowych przewiduje kupno oraz pobieranie plików multimedialnych wraz z licencją. Przykładem takiej działalności jest sklep internetowy muzodajnia.pl, który w swojej ofercie ma 110 tys. płyt muzycznych.

Metody steganografii mają wielkie znaczenie w procesie zapewniania bezpieczeństwa usług typu *pay per view* (wideo na żądanie). Wykorzystuje się tutaj widoczne oraz niewidoczne cyfrowe znaki wodne.

Steganografia umożliwia przechowywanie (zaszycie) w jednym pliku multimedialnym wielu różnych licencji, w zależności od sposobu wykorzystania pliku przez klienta aktywuje się odpowiednia licencja.

[4] http://www.microsoft.com/poland/msp/dobierz-licencje.aspx

Możliwa jest też ochrona poufnych materiałów firmowych. Niewidoczne mechanizmy steganografii weryfikują komputer, na którym uruchamiane są pliki firmowe, jeżeli komputer ma poprawną weryfikację w licencji, możliwe jest uruchomienie pliku.

Budowanie stron internetowych zawierających treści objęte licencjonowaniem na platformie Windows Media DRM odbywa się przy użyciu programu *Windows Media Rights Manager*[5] (WMRM). Cała procedura na serwerze WMRM polega na przygotowaniu plików i wystawieniu dla nich licencji. Wyróżniamy następujące etapy w procesie działania platformy Windows Media DRM:

- Przygotowanie pakietu. Plik multimedialny jest szyfrowany i blokowany przez klucz, który zawarty jest w oddzielnie dostarczanej licencji. Do pliku dodawane są również inne informacje, np. adres serwera, na którym przechowywana jest licencja.
- Rozpowszechnianie pakietu. Wcześniej przygotowany plik zostaje udostępniony w sieci, dystrybuowany na nośnikach pamięci lub przesyłany pocztą elektroniczną.
- Konfiguracja serwera licencji. Dostawca treści multimedialnych zobowiązany jest do udostępniania w sieci serwera, który będzie grał rolę magazynu przechowującego prawa i zasady licencyjne. Do tego celu wykorzystuje się oprogramowanie *Windows Media Rights Manager*.

Aby móc odtworzyć plik, użytkownik musi pobrać klucz licencyjny, który pozwoli na jego odblokowanie. Licencja pobierana jest automatycznie w momencie, kiedy użytkownik zaczyna ściągać plik lub próbuje odtworzyć plik po raz pierwszy, np. z płyty DVD. W przypadku kiedy użytkownik jest zobowiązany do zapłaty za licencję, najczęściej jest przekierowywany na stronę internetową, gdzie właśnie może zarejestrować swoją płatność.

Odtwarzanie pliku. Aby odtworzyć pobrane multimedia, trzeba skorzystać z odtwarzacza obsługującego platformę *Windows Media DRM* (np. Windows Media Player). Oczywiście, przeglądanie treści jest możliwe tylko w zakresie wcześniej uzyskanej licencji.

Sklepy internetowe często stosują system Microsoftu, ponieważ łatwo go wdrożyć. Legalni użytkownicy jednak mogą natrafić na pewne problemy. Tego typu rozwiązanie nie pozwala wykonywać kopii na własny użytek zasobów wcześniej zakupionych. Kolejnym problem jest ograniczenie co do formatu pliku. W przypadku, kiedy nasze urządzenie nie poradzi sobie z formatem pliku, nie będzie można go przekonwertować na inny.

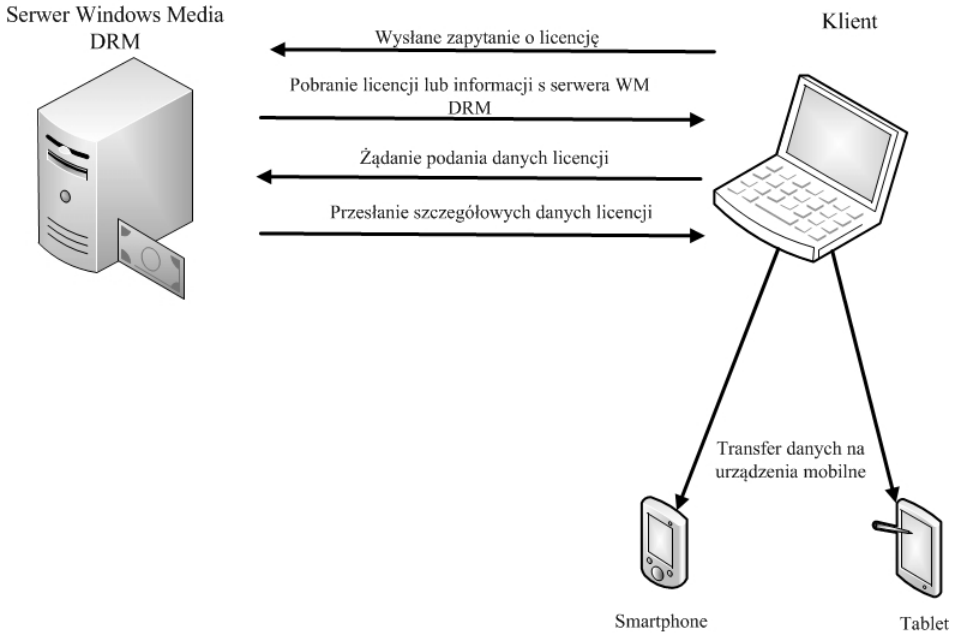
---

[5] http://www.pcmag.com/encyclopedia_term/0,2542,t=Windows+Media+Rights+Manager&i=54664,00.asp

Proces przesyłania i sprawdzania licencji występuje przy próbie odtworzenia pliku multimedialnego w aplikacji Windows Media Player, który jest też częścią wspomnianego wcześniej systemu Windows Media DRM.

Windows Media Player w pierwszej kolejności sprawdza, czy w swojej bibliotece posiada dla danego pliku keyID. W przypadku gdy keyID znajduje się już w bibliotece, plik multimedialny jest uruchamiany. W przeciwnym wypadku klient łączy się z Windows Media DRM w celu pozyskania licencji dla uruchamianego pliku multimedialnego. Jeżeli użytkownik poprawnie przejdzie proces uwierzytelniania i autoryzację, przesyłana jest licencja dla pliku multimedialnego. Klient po otrzymaniu licencji generuje keyID i zapisuje go w bibliotece Windows Media Player.

Jeśli klient nie przejdzie pozytywnie procesu autoryzacji, to serwer Windows Media DRM przekierowuje go do systemu płatności w celu wygenerowania licencji. Na rysunku 3 przedstawiono proces pobierania i sprawdzania licencji w systemie Windows Media DRM.

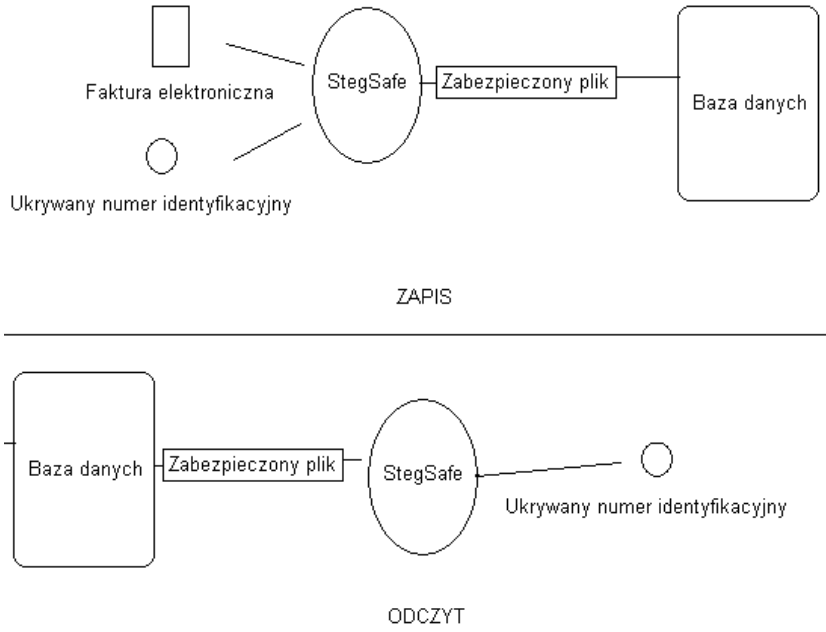


Rys. 3. Schemat procesu pobierania i sprawdzania licencji w systemie Windows Media DRM

Źródło: opracowanie własne.

Steganografia może być skuteczna do ochrony danych komercyjnych przechowywanych w archiwach elektronicznych. Przykładową aplikacją w tej dziedzi-

nie jest *StegSafe*^{TM}. Aplikacja ta ukrywa pewne informacje (np. numer identyfikacyjny, dane partnerów handlowych) w różnych plikach (np. obrazach jpg[6]), które następnie są magazynowane np. w bazach danych. Dzięki ukrytym informacjom można zabezpieczyć przechowywane dane w bazie przed atakiem hakerów, którzy te dane chcą zmienić (np. zmienić kwoty faktur). Zasadę działania *StegSafe*^{TM} przedstawia rysunku 4.



Rys. 4. Koncepcja działania aplikacji *StegSafe*^{TM}

Źródło: opracowanie własne.

Podsumowanie

Steganografia ma do odegrania znaczącą rolę w handlu elektronicznym. Pozwala zabezpieczać dane, które mogą być ogólnie dostępne (np. promocyjna mp3 zachęcająca do kupna całej płyty audio). Ukrywanie informacji umożliwia również zastosowanie nowych, skutecznych metod zapisywania i egzekwowania praw autorskich oraz licencji. Ukryte informacje mogą być wykorzystywane do potwier-

[6] http:\\users.finemedia.pl/dloogie/bezpieczenstwo/stegangrafia.pdf

dzania ważnych transakcji handlowych oraz uwierzytelniania użytkowników. Dzięki zastosowaniu steganografii dane mogą być zabezpieczone bez wzbudzania podejrzeń u potencjalnego hakera. W kryptografii natomiast, w przeciwieństwie do steganografii, jeśli coś jest zaszyfrowane, to jest wyraźnie widoczne.

Literatura

1. Cox I., Miller M., Bloom J., Fredric J., Kalker T., *Digital Watermarking and Steganography*, 2nd Ed. electronic free book, http://www.freeebook download.co.in/ebooks/free-ebook-Digital-Watermarking-and-Steganography-2nd-Ed-The-Morgan-Kaufmann-Series-in-Multimedia-Information-and-Systems--download 2009.
2. Wayner P., *Disappearing cryptography*, 3rd Edition*, information hiding, steganography & watermarking*, Amsterdam, MK/Morgan Kaufmann Publishers 2009.
3. www.datamark.com.sg/pdf/steganography.pdf
4. http://www.microsoft.com/poland/msp/dobierz-licencje.aspx
5. http://www.pcmag.com/encyclopedia_term/0,2542,t=Windows+Media+Rights+Manager&i=54664,00.asp
6. http:\\users.finemedia.pl/dloogie/bezpieczenstwo/stegangrafia.pdf

APPLICATION OF DIGITAL STAGANOGRAPHY METHODS IN E-COMMERCE

Summary

The rapid growth of e-commerce applications via the Internet in the past decades is the reason that both small office and corporations have a need to protect their on-line transactions. These transactions include sensitive documents' transfer, digital signature authentication and digital data storage. The use of digital steganography for information security in various ecommerce applications through the Internet is discussed in details in this article. The security methods, based on digital steganography, include digital signature authentication and validation of electronic documents, digital data storage, as well as secure transfer of multimedia data through the open channels.

Translated by Volodymyr Mosorov