STUDIA INFORMATICA 2003
Volume 24 Number 2B (54)

Arkadiusz LIBER
Politechnika Wrocławska, Wydział Informatyki i Zarządzania

NIEWIDOCZNE WARSTWY ZAWIERAJĄCE UKRYTE WIADOMOŚCI W ZABEZPIECZANIU MULTIMEDIALNYCH SYSTEMÓW INFORMACYJNYCH

Streszczenie. Rosnące znaczenie informacji elektronicznej powoduje konieczność prowadzenia intensywnych prac badawczych z zakresu zapewnienia jej autentyczności. Bardzo łatwe jest tworzenie elektronicznych systemów zawierających sfałszowane i niepełne informacje. Takie systemy zwane systemami dezinformacyjnymi najskuteczniej pełnią swoją rolę, gdy stanowią część składową powszechnie dostępnych bibliotek elektronicznych lub połączone są z powszechnie dostępnymi systemami informacyjnymi. W pracy przedstawiono wyniki badań z zakresu konstrukcji multimedialnych systemów informacyjnych zawierających niewidoczne warstwy informacyjne. Pokazano możliwość zastosowania dodatkowych warstw informacyjnych do rejestracji zmian w zawartości serwisów elektronicznych oraz zabezpieczenia zawartości dokumentów elektronicznych przed atakami dezinformacyjnymi.

Słowa kluczowe: niewidoczne warstwy informacyjne, systemy informacyjne.

INVISIBLE LAYERS WITH HIDDEN INFORMATION IN MULTIMEDIA INFORMATION SYSTEMS PROTECTION

Summary. In this paper, the results of research on the construction of electronic information systems containing invisible information layers are presented. We describe possibilities of using hidden information layers for protecting multimedia information systems against attacks.

Keywords: invisible information layers, information systems.

1. Wprowadzenie

Rozwój urządzeń technicznych oraz postęp w dziedzinie technologii materiałów umożliwiają coraz powszechniejsze i bardziej wysublimowane sygnowanie nie tylko dokumentów, lecz również innych wytwarzanych przez człowieka wyrobów. Znane wcześniej metody niewidocznego sygnowania, takie jak techniki mikrodruku i techniki druku za pomocą niewidocznych tuszów i farb, stosowane są do dzisiaj. Gwałtownie rosnący obrót informacją elektroniczną doprowadził do burzliwego rozwoju kryptografii, a następnie do rozwoju metod niedostrzegalnego przekazywania i podpisywania informacji [1].

Niewidoczne sygnowanie informacji. Najbardziej rozpowszechnionym sposobem udostępniania informacji w systemach informacyjnych jest przedstawienie jej w postaci tekstu. Metody umieszczania dodatkowych informacji w tekście można podzielić na metody językowe i graficzne. Metody językowe oparte są na stosowaniu słów bliskoznacznych, przestawień wyrazów oraz zdań bez zmiany znaczenia tekstu. Metody graficzne związane są z układem tekstu na stronie. Do najciekawszych metod należą tu metody mikroprzesunięć linii tekstu i słów zaproponowane w latach 1994-1995 przez Lowa i Maxemchuka [2], [3], [4]. Najważniejszym problemem, który należy rozwiązać przy dokonywaniu graficznych przesunięć tekstów, jest wybór miejsc w dokumencie, gdzie deformacje nie zostaną zauważone [5], [6]. Metody ukrywania dodatkowej informacji w dźwiękach opierają się na kodowaniu najmniej znaczącego bitu, kodowaniu fazy, kodowaniu widmowym oraz kodowaniu informacji w echu [1], [7].

Najprostszą klasą metod wprowadzania niewidocznej informacji do obrazów jest klasa metod permutacyjnych. Metody permutacyjne oparte są na przestawianiu bitów w binarnym dokumencie wejściowym. Przykładem może być metoda zamiany kolorów o podobnych częstościach występowania w obrazie, stosowana przez Handela i Sanforda oraz metoda adiabatyczna (w sensie niezmienności entropii obrazu) stosowana przez Tinsleya [1].

Znakowanie informacji cyfrowej stosowane jest głównie do zapewnienia ochrony praw autorskich do obrazu cyfrowego lub utworu muzycznego. Prowadzone współcześnie badania mają na celu opracowanie algorytmów znakowania odpornych na: konwersje formatów, kompresję, przetwarzanie analogowo-cyfrowe i cyfrowo-analogowe, skalowanie, obroty, przesyłanie kanałem transmisyjnym o własnościach szumowych [1], [8], [9]. W przypadku uniwersalnych systemów informatycznych interesujące jest poszukiwanie algorytmów sygnowania odpornych na procesy skanowania i drukowania. Opracowanie algorytmów odpornych na te procesy umożliwiłoby nie tylko płynne przenoszenie informacji o prawach autorskich pomiędzy dokumentami elektronicznymi i drukowanymi, lecz również przenoszenie coraz istotniejszych informacji o autentyczności dokumentów. Większość

dotychczasowych metod zapewnienia skutecznej odporności obrazów na transformacje graficzne opartych jest na transformacjach spektralnych, np. Fouriera-Mellina.

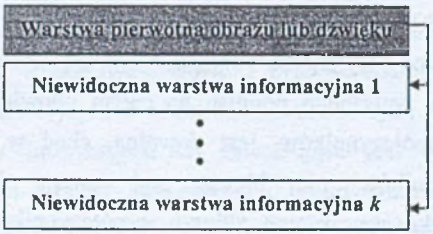
Współczesne metody niewidocznego sygnowania. Podpisy lub inne informacje wpisane w obraz uważa się za perceptualnie niezauważalne, jeżeli przeciętny człowiek mając przed sobą obraz podpisany i nie podpisany nie jest w stanie wskazać na podpisanym obrazie rozmieszczenia podpisu. Istotnymi cechami obrazów z niewidocznymi sygnaturami oraz procesów sygnowania są: wierność podpisanego obrazu, siła podpisu, kruchość podpisu, pojemność informacyjna sygnatury, złożoność obliczeniowa algorytmu sygnowania i odczytu sygnatury, małe prawdopodobieństwo błędnej detekcji sygnatury w obrazie nie podpisanym, możliwość modyfikacji sygnatury umieszczonej w obrazie, możliwość wielokrotnego podpisywania obrazu. Sygnatury obrazowe najczęściej generuje się metodami morfologicznymi lub metodami spektralnymi. Przykładem morfologicznej metody generacji sygnatury jest podpis opisany przez Libera i Lubacza [10]. W metodzie tej wiadomość M wpisywana do obrazu poddawana jest przekształceniu szyfrującemu E_K, w wyniku czego otrzymuje się szyfrogram $C = E_K(M)$. Jako przekształcenie E_K można tu zastosować dowolny schemat szyfrowania. Po rozłożeniu szyfrogramu na bity wyodrębnia się z obrazu k wzorców W_i. Zbiór wzorców wybierany jest na podstawie analizy morfologicznej z zastosowaniem kryterium minimalnej deformacji zawartości obrazu. Ostateczne rozmieszczenie wzorców określane jest z kryterium minimalnego postrzegania fizjologicznego z nałożoną charakterystyką pseudolosową. Sygnatury spektralne wstawia się w przestrzeni częstotliwości. Obraz traktowany jest jako sygnał, a sygnatura umieszczana jest w określonych pasmach częstotliwości. Najbardziej znanym podpisem tego typu jest podpis proponowany przez I. Cox [8]. W metodzie tej podpis jest ciągiem liczb rzeczywistych $X=x_1,x_2, \ldots,x_n$ skończonej precyzji wylosowanych niezależnie zgodnie z rozkładem normalnym $N(0,1)$. Pierwszym krokiem algorytmu wstawiania sygnatury jest transformacja obrazu transformatą Fouriera bądź transformatą kosinusową. Podpis umieszczany jest w n najbardziej perceptualnie znaczących współczynnikach transformaty. Ma to trzy zalety. Po pierwsze, zapobiega usunięciu podpisu przez kompresję obrazu. Po drugie, nawet niewielkie zmiany tych współczynników przez atakującego ten podpis w celu jego wymazania mogą odbić się negatywnie na wyglądzie obrazu. Trzecią zaletą tego podejścia jest rozprzestrzenianie się tak wpisanego podpisu na całym obrazie. Należy dodać, iż sama metoda wyboru tych współczynników jest dowolna, choć w praktyce wybiera się n największych współczynników nie biorąc pod uwagę jednakże współczynnika maksymalnego. W tak skonstruowanym zbiorze współczynników podpis umieszcza się zgodnie z zależnością: $v_i' = v_i(1+\alpha \cdot x_i)$, gdzie v_i jest i-tym z wybranych współczynników, α - parametrem skalującym, a v_i'- nowym współczynnikiem z umieszczoną już częścią podpisu.

Do sprawdzenia podpisu generowanego tą metodą niezbędne jest posiadanie obrazu źródłowego oraz zapamiętanej wartości parametru α [8].

2. Niewidoczne pseudolosowe warstwy informacyjne

Prezentowana metoda wstawiania niewidocznych warstw informacyjnych oparta jest na wynikach uzyskanych przez autora opisanych w pracy [10]. Dodatkowe warstwy informacyjne mogą zawierać uzupełnienie wiedzy udostępnianej przez system informacyjny, nową wiedzę niezależną od udostępnianej lub inne informacje ukryte przed standardowym odbiorcą. Istotną modyfikacją, w stosunku do prac poprzednich dotyczących generacji niewidocznych sygnatur, jest polepszenie algorytmu generacji ścieżki postrzegania oraz zastosowanie zmodyfikowanych generatorów sekwencji pseudolosowych opartych na arytmetyce w ciałach Galois $GF(p)$. Każdą macierz obrazu A można podzielić na prostokątne rozłączne obszary. Dodatkowa informacja może być reprezentowana przez ciąg binarny $C=b_{k-1}b_{k-2}b_{k-3}...b_1b_0$, gdzie k - ilość bitów informacji wpisywanej. W sposób opisany w pracy [10] wyodrębnia się k wzorców: $W_0, W_1, ..., W_{k-1}$ oraz odwzorowanie $f: W_i \xrightarrow[b_i]{} W_i'$. Ścieżka wyboru wzorców W_i oparta jest na charakterystyce widmowej oka ludzkiego i mechanizmach postrzegania obrazu [10]. Długość możliwej ścieżki podpisu związana jest z zawartością obrazu. Dla zadanej długości szyfrogramu k oraz zadanego obrazu A możliwy jest wybór m ścieżek podpisu o długości l_m. Opracowana metoda umożliwia pseudolosowy wybór ścieżki podpisu oraz pseudolosowy wybór rozmieszczenia informacji na zadanej ścieżce. Podejście takie gwarantuje możliwość generowania z jednego obrazu A ciągów podpisanych obrazów A'_s o innym rozkładzie zapisywanej informacji. Do generacji sekwencji pseudolosowych wybrano ogólny generator wielomianowy w ciele $GF(p)$.

Na bazie pojedynczej pierwotnej warstwy obrazu lub dźwięku możliwe jest wykonanie wielu niewidocznych warstw informacyjnych.



Rys. 1. Warstwa obrazu lub dźwięku z k warstwami informacyjnymi utworzonymi na bazie warstwy pierwotnej

Fig. 1. Image or audio layer with k invisible information layers

Sposób tworzenia warstw niewidocznych zależy od przyjętej metody niewidocznego sygnowania. Możliwe jest zarówno utworzenie jednej warstwy podzielonej na mniejsze w przypadku metod umożliwiających jednokrotne sygnowanie, wielu warstw w przypadku metod niewidocznego sygnowania wielokrotnego lub wykonanie warstw w sposób mieszany.

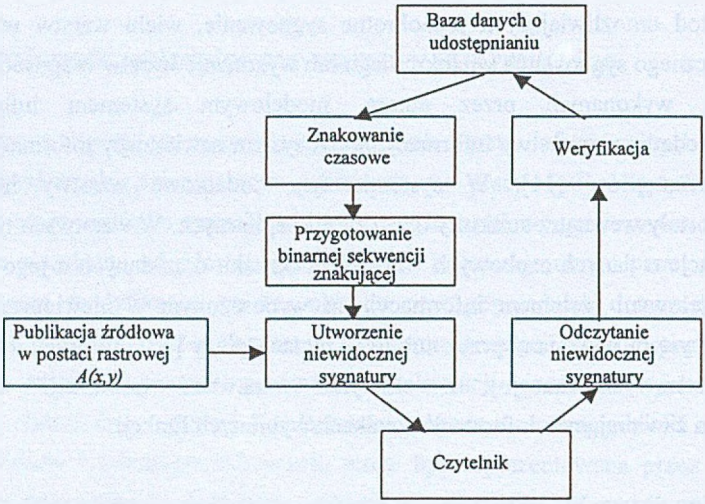
Pierwszym, wykonanym przez autora, modelowym systemem informacyjnym zawierającym dodatkowe warstwy informacyjne był system zawierający informacje o liniach papilarnych przestępców [11]. W systemie tym dodatkowe warstwy informacyjne umieszczone zostały wewnątrz struktury obrazu linii papilarnych. W warstwach tych zawarte zostały informacje o danych osobowych właściciela odcisku oraz danych o jego karalności. Kolejnym modelowym systemem informacyjnym wyposażonym w niewidoczne warstwy informacji jest system wykonany przez autora w ramach pracy [12]. W pracy tej wykonano modelowy system informacyjny z ukrytymi warstwami informacji w serwisie matematycznym zawierającym informacje o całkach wybranych funkcji.

3. Niewidoczne warstwy informacyjne w autentyfikacji serwisów informacyjnych

W ramach pracy przeprowadzono modelowanie systemu biblioteki elektronicznej zawierającej niewidoczne warstwy informacyjne o udostępnianiu oraz dane autentyfikacyjne. Konstrukcja niewidocznych warstw informacyjnych oparta została na wynikach badań opublikowanych w [10], [11], [12], [13]. Informacja przenoszona w publikacji elektronicznej w postaci niewidocznej sygnatury ma postać ciągu binarnego. Ciąg ten zawiera wszelkie dane o czytelniku oraz o procesie udostępniania publikacji. Ze sposobu generacji sygnatury wynika, że publikacja jest jednoznacznie związana z czytelnikiem. W szczególności procesu zwrotu musi dokonać ten sam czytelnik, któremu publikacja została udostępniona.

Ze względu na fakt zawarcia w sygnaturze znaczników czasowych możliwe jest łatwe kontrolowanie obiegu publikacji. W szczególności możliwe jest przeszukiwanie zasobów sieci i lokalizacja publikacji przeterminowanych lub niewłaściwie rozpowszechnionych. Uzupełnienie przedstawionego systemu w specjalizowane urządzenie czytające może uniemożliwić kopiowanie i użytkowanie publikacji po przekroczeniu określonego interwału czasowego. Najskuteczniejszą formą ochrony informacji przed modyfikacją jest zablokowanie dostępu do systemu informatycznego. Jak pokazuje praktyka, systemy operacyjne oraz zainstalowane oprogramowanie ciągle posiadają luki umożliwiające dokonanie włamania do systemu. Skuteczną formą zabezpieczenia informacji przed jej modyfikacją jest zastosowanie podpisów cyfrowych oraz systemów okresowo weryfikujących

podpisy. W opisanym rozwiązaniu do zapewnienia autentyczności publikacji zastosowano niewidoczną warstwę informacyjną zawierającą podpis cyfrowy ECDSA.



Rys. 2. Proces czasowego udostępniania publikacji elektronicznej oparty na niewidocznych sygnaturach obrazowych

Fig. 2. The process of temporary throwing open of the electronic publication leaning on invisible picturesque signatures

4. Wnioski

Zastosowanie niewidocznych warstw informacyjnych w publikacjach elektronicznych oraz w systemach informacyjnych daje nowe możliwości w zakresie niezależnego przesyłania dodatkowych danych oraz w zakresie zapewnienia autentyczności elektronicznych serwisów.

Uzupełnienie publikacji znajdujących się w zbiorach biblioteki elektronicznej o niewidoczne warstwy informacyjne pozwala na wprowadzenie do dokumentów informacji uzupełniających. Uzupełniające informacje mogą być użyte do weryfikacji autentyczności publikacji, a co za tym idzie do ochrony przed atakami dezinformacyjnymi.

Mimo iż większość obecnie stosowanych metod opiera się na analizie w przestrzeni częstotliwości, przedstawiona metoda generacji niewidocznych warstw informacyjnych bazuje na modyfikacji obrazu w przestrzeni odwzorowań morfologicznych. Przedstawiona metoda generacji niewidocznych warstw informacyjnych nie jest odporna na kompresję stratną, tak jak np. metody opisane w [1] i [8], daje ona jednak bardzo dobre rezultaty w cyfrowych kanałach transmisyjnych ze względu na dużą szybkość wprowadzania i odczytu niewidocznej informacji. Jedną z interesujących własności zastosowanej metody jest

możliwość generowania i wykrywania wielu różnych pseudolosowych postaci warstw z tą samą treścią wiadomości dla jednego obrazu. Prowadzone są badania nad wykorzystaniem opisanych metod do umieszczania dodatkowych tekstów w innych systemach informatycznych [12], [13], [14]. Aktualnie prowadzone są badania nad rozszerzeniem opisanej metody na przypadki ogólnych odwzorowań konforemnych oraz nad opracowaniem metody niewidocznych podpisów strukturalnych, jak również nad rozwojem metod falkowych. Prowadzone są dalsze prace nad opracowaniem algorytmów tworzenia i przetwarzania niewidocznych warstw informacyjnych odpornych na procesy skanowania i drukowania.

LITERATURA

1. Petitcolas F. A., Anderson R. J., Kuhn M. G.: Information Hiding – A Survey. Procedings of the IEEE, vol. 87, no. 7, 1999.
2. Brassil J., Low S., Maxemchuk N., O'Garman L.: Electronic Marking and Identification Techniques to Discourage Document Copying, Infocom. Toronto, Canada, IEEE, June 1994.
3. Maxemchuk N.: Electronic Document Distribution. AT & T Technical, vol. 73 no. 5 pp. 73–80, Sept.–Oct. 1994.
4. Low S., Maxemchuk N., Brassil J., O'Gorman L.: Document Marking and Identification using Both Line and Word Shifting. Infocom'95, Apr. 1995.
5. Low S., Maxemchuk N.: Performance Comparison of Two Text Marking Methods. IEEE Journal on Special Areas in Communications, vol. 16 no. 4 pp. 561–572, May 1998.
6. Podilchuk C., Zeng W.: Image-AdaptiveWatermarking Using Visual Models. IEEE Journal on Special Areas in Communications, vol. 16 no. 4 pp. 525–539, May 1998.
7. Chang L., Moskowitz I.: Critical Analysis of Security in Voice Hiding Techniques. Information and Communications Security – First International Conference, Beijing, China, 11–14 Nov. 1997, vol. 1334 of Lecture Notes in Computer Science, pp. 203–216, Springer Verlag.
8. Lin Ch., Wu M., Bloom J. A., Cox I. J., Miller M. L., Lui Y. M.: Rotation, Scale and Translation Resilient Public Watermarking for Images. Proceedings of SPIE, vol. 3971, 2000.
9. O Ruanaidh J. K., Pun T.: Rotation, Scale and Translation Invarant Spread Spectrum Digital Image Watermarking. Signal Processing, 66, pp. 303-317, 1998.
10. Liber A., Lubacz T.: Niewidoczne Sygnatury w Zabezpieczaniu Dokumentacji Technicznej i Obrazów w Postaci Rastrowej. I Krajowa Konferencja Metody i Systemy

Komputerowe w Badaniach Naukowych i Projektowaniu Inżynierskim, Kraków 25-26 listopada 1997.

11. Liber A.: Niewidoczne sygnatury obrazowe w rozproszonych systemach identyfikacji biometrycznej. III Krajowa Konferencja Metody i systemy komputerowe w badaniach naukowych i projektowaniu inżynierskim, Kraków 19-21.11.2002.
12. Liber A.: Systemy informacyjne z wiedzą ukrytą w obrazach i dźwiękach. Multimedialne i Sieciowe Systemy Informacyjne, MISSI Kliczków, 19-20 września 2002.
13. Liber A.: Watermark and Invisible Information Layers in Electronic Publications and Information Systems. From Printed Book to Digital, 13-14.10.2002, Tartu University Library.
14. Liber A.: Metody zapewnienia poufności i autentyczności w obrocie wydawnictwami w postaci elektronicznej ze szczególnym uwzględnieniem procesu czasowego ich udostępniania. Problemy Ochrony Zbiorów i Systemów Komputerowych w Bibliotekach. Białystok-Wigry, 6-8 czerwca 2001.

Recenzent: Dr inż. Roman Starosolski

Wpłynęło do Redakcji 5 kwietnia 2003 r.

Abstract

Because of the growing importance of electronic information it is necessary to intensify research aimed at ensuring its authenticity. It is very easy to create electronic systems containing falsified and incomplete information. In this paper, the results of research on the construction of electronic information systems containing invisible information layers are presented. In chapter 3 possibilities of using hidden information layers for recording the lending of electronic documents and changes in their contents and protecting the latter against disinformation attacks are demonstrated.

Adres

Arkadiusz LIBER: Politechnika Wrocławska, Wydział Informatyki i Zarządzania, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Polska, liber@ci.pwr.wroc.pl