Jerzy KOROSTIL, Łukasz NOZDRZYKOWSKI
POLITECHNIKA SZCZECIŃSKA, WYDZIAŁ INFORMATYKI

Metoda formowania struktury sprzętowej realizacji rozproszonego klucza steganograficznego na bazie FPGA

Prof. dr hab. inż. Jerzy KOROSTIL

Pracuje na Wydziale Informatyki Politechniki Szczecińskiej od 2000r. Obecnie jest kierownikiem Zakładu Bezpieczeństwa Oprogramowania w Katedrze Technik Programowania. Zainteresowania naukowe dotyczą steganografii, bezpieczeństwa sieci komputerowych oraz oprogramowania.

e-mail: jkorostil@wi.ps.pl

Mgr inż. Łukasz NOZDRZYKOWSKI

Ukończył studia na Wydziale Informatyki Politechniki Szczecińskiej w 2006r. Obecnie jest doktorantem w Katedrze Technik Programowania Wydziału Informatyki. Jego zainteresowania naukowe obejmują kryptografię i steganografię oraz bezpieczeństwo sieci komputerowych.

e-mail: lnozdrzykowski@wi.ps.pl

Streszczenie

W artykule przedstawiono metodę wykorzystania układów programowalnych do sprzętowej realizacji fragmentów systemu steganograficznego dotyczących klucza steganograficznego. Z systemu steganograficznego wydzielono "część klucza", czyli przekształceń, w których wykorzystywany jest klucz. Pozwoliło to na sprzętową jego implementację, co zwiększyło bezpieczeństwo wykorzystywanego klucza.

Słowa kluczowe: Steganografia, klucze steganograficzne, ukrywanie informacji, FPGA.

The method of forming hardware structure of diffuse steganographic key in FPGA device

Abstract

This article presents a method used programmable device to hardware implementation same elements of the steganographic system concerning stego-key. In the steganoraphic system has dealt out a key part, that is transformations key in which be used. This step allowed to hardware implementation the key, which enlarged its safety.

Keywords: steganography, key, information hiding, FPGA.

1. Wprowadzenie

Steganografia jako system ochrony informacji, ukrywa bity wiadomości w informacji nośnej tak, aby fakt ukrycia nie był zauważalny dla atakującego. Ponadto dzięki zastosowaniu klucza steganograficznego ukryta wiadomość zabezpieczona jest przed nieuprawnionym odczytem, modyfikacją lub zniszczeniem ukrytej wiadomości. W artykule przedstawiono ideę formowania rozproszonego klucza steganograficznego w strukturze sprzętowej FPGA.

2. Stosowanie kluczy steganograficznych

Klucze steganograficzne wykorzystywane są głównie do wyznaczania miejsc ukrycia wiadomości lub do rozrzucenia ukrywanej wiadomości [1]. Służą one do bezpiecznego ukrycia wiadomości w informacji nośnej.

W pierwszym przypadku bity klucza steganograficznego bezpośrednio lub pośrednio wskazują miejsca ukrycia wiadomości w informacji nośnej. Może on bezpośrednio wskazywać bity informacji nośnej podlegające modyfikacjom lub współczynniki wybranej transformaty (DCT, DFT itp.) [2]. Miejsca ukrycia wiadomości można także wskazać pośrednio z wykorzystaniem funkcji wskazującej takie miejsca, wykorzystując przykładowo generator LFSR inicjowany kluczem steganograficznym [3].

W drugim przypadku klucz steganograficzny stosowany jest podczas rozrzucania ukrywanej wiadomości w informacji nośnej. Najczęściej stosowane tu metody oparte są o rozpraszanie widma, a klucz może zostać wykorzystany do wygenerowania odpowiedniego szumu, z którym ukrywana wiadomość zostanie połączona [4].

Klucz steganograficzny może także służyć do wyznaczania miejsc ukrycia wiadomości w informacji nośnej poprzez analizowanie własności informacji nośnej tak, aby ukryta w niej wiadomość spowodowała jak najmniej zniekształceń [5].

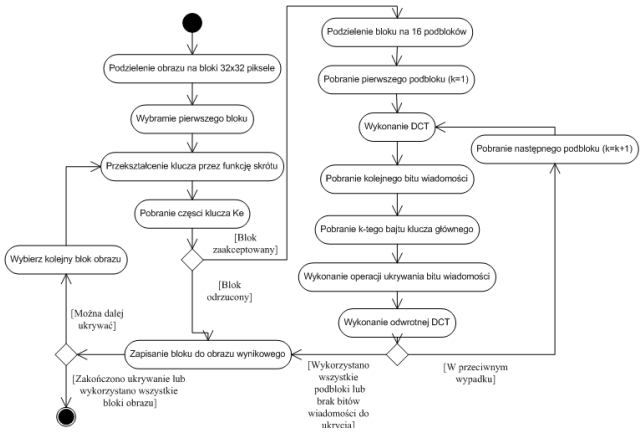
3. Algorytm steganograficzny

W pracy [6] przedstawiono algorytm steganograficznego ukrywania informacji w cyfrowych obrazach TrueColor. Wiadomość ukrywana jest w współczynnikach DCT obrazu. Początkowo obraz dzielony jest na bloki 32x32 piksele. Każdy z bloków jest kolejno klasyfikowany pod kątem możliwości ukrycia w nim bitów wiadomości. Służą do tego odpowiednie progi oraz klucz steganograficzny. Spełnienie zależności określonej przez dany próg (wybierany przez ukrywającego) pozwala na ukrywanie w danym bloku bity wiadomości. Progi te wykorzystują w obliczeniach filtry wyznaczające liczbę punktów tworzących krawędzie oraz miary statystyczne (średnią arytmetyczną, modę lub odchylenia standardowe i przeciętne) histogramów kolorów, kontrastów lub korelacji. Poprawnie sklasyfikowany blok jest następnie dzielony na podbloki 8x8 pikseli. Następnie na każdym podbloku wykonuje się transformatę DCT. Wiadomość ukrywana jest we współczynnikach tej transformaty. W celu poprawnego ukrycia wiadomości należy wyznaczyć dwa współczynniki transformaty danego podbloku. Współczynniki te wyznacza się z wykorzystaniem bitów klucza steganograficznego. Ukrywanie bitów wiadomości w współczynnikach t1 i t2 wykonywane jest zgodnie z następującą regułą:
a) dla bitu 1: t1+c>=t2-c (t1 jest większym ze współczynników);
b) dla bitu 0: t1-c<t2+c (t1 jest mniejszym ze współczynników).
gdzie c jest siłą wstawiania wiadomości.

Przedstawiony algorytm został zaprezentowany w postaci diagramu aktywności na rys. 1. Wykorzystano w nim jeden klucz steganograficzny składający się z trzech części. Schemat klucza zostanie przedstawiony w dalszej części niniejszej pracy.

Aby odczytać wiadomość należy wykorzystać następującą regułę podczas przetwarzania bloków obrazu:
- ukryto bit 1, gdy: $t_1>=t_2$;
- ukryto bit 0, gdy: $t_1<t_2$.

Do odczytania wiadomości należy użyć tych samych reguł jakie zostały wykorzystane do ukrycia tj. barwa, w której ukrywano wiadomość, rodzaj progu oraz klucz.



Rys. 1. Przedstawiony algorytm steganograficzny
Fig. 1. Steganographic algorithm

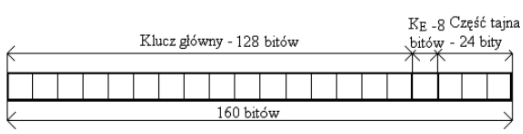
3.1. Schemat rozproszonego klucza steganograficznego

Przedstawiany klucz steganograficzny (rysunek 2) pozwala na wykorzystywanie go w dwojakiej roli. Po pierwsze można dokonywać selekcji bloków obrazu pod kątem przydatności ich do ukrywania w nich bitów wiadomości. Na rysunku 2 oznaczono część tego klucza jako K_E. Tą część klucza stosuje się w progach pozwalających na klasyfikację bloków informacji nośnej. Progi te przedstawiono w pracach [6, 7]. Zostały one zrealizowane w oparciu o:

a) zliczanie punktów tworzących krawędzie i filtry krawędziowe,
b) miary statystyczne (średnią arytmetyczną, modę, odchylenie standardowe i przeciętne) dla histogramów (kolorów, kontrastów oraz korelacji).

Zastosowanie selekcji bloków obrazu pozwala na ukrywanie wiadomości w miejscach, gdzie nie powodowałoby to znaczących zniekształceń w informacji nośnej. Dzięki takiemu rozwiązaniu wybierane są głównie obszary o zróżnicowanej teksturze w informacji nośnej.

Druga część klucza wykorzystywana jest do właściwego ukrywania bitów wiadomości. Na rysunku 1 przedstawiono go jako klucz główny. Składa się on z 16 części służących do wyznaczania współczynników DCT 16 podbloków obrazu (sposób wyznaczania współczynników przedstawiono w pracy [6]).



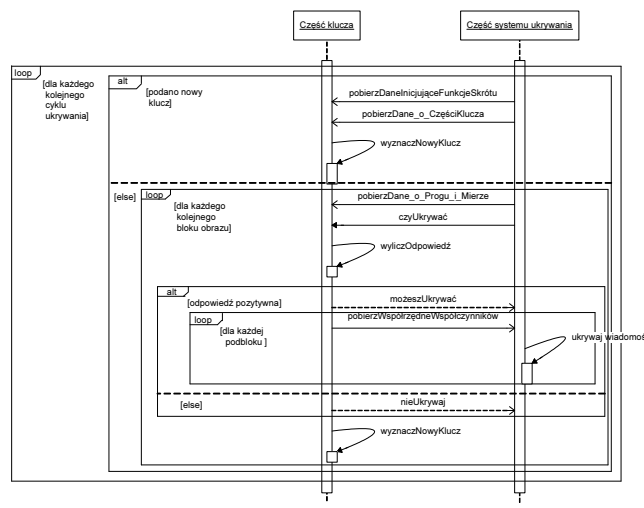
Rys. 2. Klucz steganograficzny
Fig. 2. Stego-key

Ostatnią częścią klucza jest część tajna. Nie jest ona wykorzystywana w algorytmie steganograficznym. Stanowi ona ziarno dla funkcji skrótu, która przekształca klucz dla każdego kolejnego bloku obrazu. Funkcja skrótu przetwarza także klucz przed pierwszym użyciem klucza. Stosowanie takiego rozwiązania ma za zadanie, przy założeniu zastosowania bezpiecznej funkcji skrótu i bezpiecznego algorytmowi steganograficznemu, uniemożliwić atakującemu odtworzenie klucza. Bezpieczna funkcja skrótu oraz część tajna uniemożliwia odtworzenie klucza dla bloku *n-1* (w którym ukrywana była wiadomość) na podstawie przetwarzanego aktualnie bloku *n*, a także na wyznaczenie klucza użytego do ukrywania wiadomości w następnym bloku informacji nośnej użytego do ukrywania.

Przedstawiony na rysunku 2 klucz został przystosowany dla algorytmu zaprezentowanego na rysunku 1. Klucz taki może zostać w łatwy sposób przystosowany do innych algorytmów steganograficznych operujących na obrazach cyfrowych, poprzez dobranie odpowiedniej jego długości i dostosowanej do niej funkcji skrótu. Dla danego algorytmu zastosowano jako funkcję skrótu przekształcenie SHA-1. Format tego klucza pozwala także na zastosowanie go dla algorytmów steganograficznych, które nie wykorzystują selekcji bloków obrazu, gdyż stosowane progi są niezależne od algorytmu i można je stosować dla innych metod steganograficznych.

Na rysunku 3 przedstawiono podział całego systemu na część klucza i część systemu ukrywania wiadomości oraz wymianę pomiędzy nimi komunikatów w postaci UML-owego diagramu sekwencji.

Idea podziału systemu na dwie części tj. klucza i systemu ukrywania, jest taka, aby klucz nigdy nie opuszczał swojej części (po stronie systemu nie ma na jego temat żadnych informacji). Po stronie klucza wykonuje się przekształcenie wstępne klucza przez funkcję skrótu, a następnie jego podział na podczęści klucza. Po stronie systemu dokonuje się przekształceń na informacji nośnej. Obraz dzielony jest na bloki 32x32 piksele. Następnie wyliczana jest miara dla odpowiedniego progu, która zostanie przekazana do części klucza. Tam dokonywana jest selekcja bloku. Jeżeli odpowiedź jest negatywna, blok przepisywany jest do obrazu wynikowego. W przeciwnym wypadku blok dzielony jest na 16 części, na których wykonywana jest osobno transformata kosinusowa. Następnie system pobiera dane na temat lokalizacji współczynników dla każdego podbloku, w których ukrywane będą bity wiadomości. Po ukryciu wiadomości wyliczane są odwrotności transformaty, a wynik zapisywany jest do obrazu wynikowego i wybierany jest kolejny blok obrazu (chyba, że zakończono ukrywanie bitów wiadomości lub skończyły się wolne bloki informacji nośnej). Natomiast po stronie klucza wykonuje się ponowne przekształcenie klucza przez funkcję skrótu.



Rys. 3. Klucz i system steganograficzny
Fig. 3. Steganographic system and key

4. Metoda realizacji sprzętowej części systemu steganograficznego

Klucz przedstawionego systemu steganograficznego można w łatwy sposób zrealizować sprzętowo. Wiadomo jest, że realizacja sprzętowa może znacznie przyspieszyć obliczenia. Realizacja programowa daje natomiast możliwość łatwej modyfikacji systemu. Ponieważ prezentowane formowanie klucza steganograficznego może być przystosowane do różnych algorytmów steganograficznych to lepszym rozwiązaniem może być realizowanie go w postaci sprzętowej. Realizacja taka ma jeszcze jedną ważną zaletę, gdyż klucz nigdy nie opuści układu sprzętowego, a wszystkie obliczenia, w których potrzebne są dane z klucza, mogą być w tym sprzęcie zrealizowane. Sprzętowo realizowana jest prezentowana na rysunku 3 część klucza, a programowo systemu.

W układzie takim znajdzie się więc część realizująca funkcję skrótu. Zalecane jest stosowanie funkcji opartych o algorytm szyfrowania symetrycznego (np. AES), która dzięki temu staje się odporna na atak metodą dnia urodzin. Ponadto implementacja powinna przewidywać możliwość generowania dowolnej długości ciągi wyjściowe. Do implementacji wykorzystano funkcję SHA-1.

Ponadto w układzie tym znajdą się wszystkie postacie progów (zaprezentowanych w pracy [7]), potrzebne do selekcji bloków obrazu. Progi te muszą zostać zaimplementowane po stronie części klucza, aby klucz nigdy nie musiałby opuszczać sprzętu. Z tej samej przyczyny po części klucza, wyznaczane są wszystkie lokalizacje współczynników dla transformaty DCT.

Można uzależnić od klucza wybór odpowiedniego progu tak, aby stosowany próg nie byłby stały dla selekcji wszystkich bloków obrazu. Ponadto od klucza może zależeć barwa, w której ukrywana jest wiadomość.

4.1. Instalacja klucza w sprzęcie

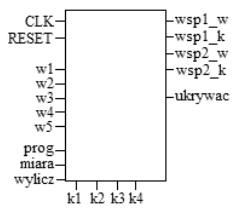
Do prawidłowego przetwarzania klucza potrzebne są informacje na temat wartości inicjalizujących funkcje skrótu. Przykładowo funkcja SHA-1 inicjuje się 5 stałymi (A-E), które na stałe umieszczone w układzie. Kolejną rzeczą konieczną do umieszczenia w układzie są struktury wszystkich możliwych do realizacji progów.

Do układu są wprowadzana następujące wartości:
- wartości inicjujące funkcję skrótu;
- cały klucz – na początku w 5 cyklach zegara (po 4 bajty klucza);
- odpowiednia miara lub miary, jeżeli próg wybierany jest w zależności od klucza;
- jeżeli stosowany próg wybiera ukrywający, to powinna być wprowadzony identyfikator danego progu.

Wartościami wyjściowymi są informacje dotyczące poprawnej lub negatywnej klasyfikacji bloku obrazu oraz lokalizacje współczynników. Dla prezentowanego algorytmu steganograficznego, sposób wyznaczania lokalizacji współczynników został przedstawiony w pracy [6].

4.2. Opis implementacji

Realizowany układ posiada 14 portów wejściowych oraz 5 wyjściowych. Zostały one pokazane na rysunku 4.



Rys. 4. Porty I/O układu
Fig. 4. I/O ports

Wejściami układu są:
- CLK - port zegara;
- RESET;
- w1…w5 - dane inicjujące funkcje skrótu;
- prog - określa stosowany aktualnie numer identyfikacyjny progu;
- miara - wyliczona przez system miara statystyczna;
- k1…k4 - służy do wprowadzania klucza;
- wylicz – określa, czy układ powinien wyznaczać nowe lokalizacje współczynników.

Wyjście układu stanowi 5 portów:
- wsp1_w i wsp1_k (określają wiersz i kolumnę pierwszego współczynnika), wsp2_w i wsp2_k (wiersz I kolumna drugiego współczynnika);
- ukrywac – określa czy system ma rozpocząć ukrywanie bitów informacji.

Podanie sygnału RESET=’1’ powoduje, że układ rozpoczyna pobieranie nowego klucza (do momentu RESET=’0’). W pierwszym cyklu zegara pobierane są wartości inicjujące funkcje skrótu. Służą do tego porty w1...w5. W następnych cyklach pobierany jest klucz poprzez porty k1...k4 (po cztery bajty jednocześnie). Z godnie z diagramem przedstawionym na rysunku 3 klucz musi zostać na wstępie przekształcony przez funkcję skrótu. Jeżeli na wejściu *wylicz* zostanie podany sygnał ‘1’, układ rozpoczyna wyliczanie miejsc ukrycia kolejnych bitów wiadomości. Dla kolejnych bloków obrazu pobierany jest numer progu (określa rodzaj miary statystycznej i czego ona dotyczy, np. jakiego rodzaju histogramu) oraz wyliczona przez system miara. Pozwala to na zmianę stosowanego progu dla każdego kolejnego bloku obrazu. Jeżeli zależność określona progiem dla klucza i miary zostanie spełniona to na wyjściu *ukrywać* podawana jest wartość ‘1’, a system rozpoczyna pobieranie kolejnych lokalizacji współczynników z układu.

Układ ten został opisany w języku VHDL. Jego symulacja i synteza została wykonana dla układu firmy Altera z rodziny Cyclone III EP3C120F78017 z użyciem narzędzia Quartus II. W implementacji tej wykorzystano 1909 bloków logicznych, co stanowi niecałe 2% wszystkich bloków tego układu. Liczba wykorzystanych pin-ów wynosi 484 z 532, czyli 91% ze wszystkich dostępnych.

5. Wnioski

Sprzętowa implementacja, oddzielonej od systemu steganograficznego części klucza, pozwala zwiększyć bezpieczeństwo używanego klucza (przy założeniu stosowania bezpiecznego algorytmu ukrywania). Klucz taki może zostać na stałe osadzony w układzie i zmieniany rzadziej w stosunku do realizacji programowej całego systemu steganograficznego. W realizacji systemowej, klucz może w dość łatwy sposób wyciągnięty z systemu, a realizacja sprzętowa może przed tym atakiem zabezpieczyć. Dodatkowo wybór progu oraz wartości inicjujących funkcje skrótu można uzależnić od przekształceń losowych realizowanych sprzętowo na podstawie wprowadzonego klucza np. opisywanej części tajnej. Ponadto realizacja sprzętowa wydzielonej części klucza jest stosunkowo łatwa do implementacji i ma małe wymagania sprzętowe, a szybkość ukrywania bitów wiadomości jest znacznie większa niż w pełnej realizacji programowej całego systemu.

6. Literatura

[1] Abdelkader H., Ouda and Mahmoud R., El-Sakka:. A Step Towards Practical Steganography Systems. Springer, Berlin 2005. http://www.springerlink.com/content/a6f8a8m7ebkpljyx.

[2] Areepongsa S., Syed Y.F., Kaewkammed N., Rao K.: Steganography For Low Bit-Rate Based Image Coder. www-ee.uta.edu/dip/paper/icip_2000.pdf.

[3] Sharp T.: An Implementation of Key-Based Digital Signal Steganography. http://citeseer.ist.psu.edu/742986.html.

[4] Lisa M. Marvel, Charles G. Boncelet, Jr., Charles T. Retter: Spread Spectrum Image Steganography. IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 8, NO. 8, AUGUST 1999.

[5] Peter H. W. Wong, Oscar C. Au, Justy W. C. Wong: A Data Hiding Technique in JPEG Compressed Domain. http://citeseer.ist.psu.edu/609998.html.

[6] Korostil J., Nozdrzykowski Ł.: Sposób budowania klucza steganograficznego w oparciu o progowe metody wyboru bloków obrazu. Metody Informatyki Stosowanej. Roczniki Informatyki Stosowanej Wydziału Informatyki PS nr 10, Szczecin 2006.

[7] Nozdrzykowski Ł.: Wbudowywanie wiadomości metodami steganograficznymi w środowisku graficznym na podstawie wykorzystania specjalnych parametrów obrazu. Praca magisterska, Szczecin 2006.

Artykuł recenzowany