Biuletyn WAT
Vol. LV, Numer specjalny, 2006

Koncepcja systemu autoryzacji korespondenta radiowego

ZBIGNIEW PIOTROWSKI, JERZY ŁOPATKA, PIOTR GAJEWSKI

Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Telekomunikacji,
00-908 Warszawa, ul. S. Kaliskiego 2

Streszczenie. Opracowana koncepcja systemu autoryzacji oparta jest na technologii OFDM oraz watermarkingu. W systemie wykorzystana została Indywidualna Sygnatura Identyfikująca Korespondenta (ang. *Correspondent Personal Identification Signature* — CPIS), w szczególności CPIS może reprezentować sobą dane biometryczne abonenta radiowego. Główną ideą tej koncepcji jest autoryzacja użytkownika końcowego (abonenta), który skrycie w tle sygnału akustycznego przesyła sygnaturę przez takie łącza, jak: Internet, KF/UKF itp. W sprawozdaniu opisano koncepcję nadajnika i odbiornika takiego systemu. Podano również wstępne wyniki badań.
Słowa kluczowe: telekomunikacja, akustyka, znak wodny, testy subiektywne
Symbole UKD: 621.39

1. Technologia znakowania obiektów cyfrowych

Obecnie obserwuje się lawinowy wzrost zainteresowania technologią watermarkingu, czyli oznaczania obiektów cyfrowych specjalnie zaprojektowaną w tym celu sygnaturą. Proces taki zachodzi już od dziesięciu lat, a to głównie ze względu na możliwość realizacji nawet bardzo obliczeniochłonnych algorytmów operujących na sygnale cyfrowym. Głównym celem technologii watermarkingu jest ukrywanie sygnału dodatkowego pod drugim sygnałem, zwanym sygnałem oryginalnym. Dodatkowy sygnał „wtrącany" do sygnału oryginalnego może zostać ponadto poddany szyfrowaniu kryptograficznemu w celu zabezpieczenia informacji poufnej.

Do głównych metod znakujących sygnał akustyczny można zaliczyć:

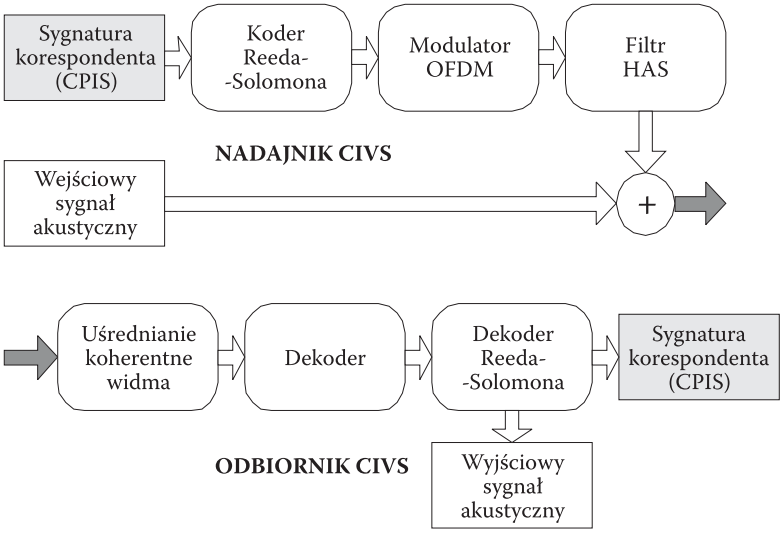
- modulację fazy [1],
- rozpraszanie widma [2],

- kwantyzowany Indeks Modulacji [3],
- kluczowanie Częstotliwości i Amplitudy [4],
- modelowanie Echa [5],
- kodowanie najmniej znaczących bitów [3].

Wysiłki podejmowane w wielu laboratoriach na świecie koncentrują się na znalezieniu kompromisu pomiędzy odpornością, przepływnością binarną a transparentnością znaku wodnego. Idealny system watermarkingowy wytwarza znak wodny w ten sposób, że w obecności sygnału oryginalnego, np. muzyki, jest on niedostrzegalny dla Systemu Słuchowego Człowieka i jednocześnie jest odporny na ataki celowe oraz na przekłamania podczas detekcji sygnału z kanału. Jedną z potencjalnych aplikacji wykorzystujących model słuchowy człowieka (ang. HAS — *Human Auditory System*) oraz znakowanie cyfrowe może być System CIVS służący do weryfikacji tożsamości korespondenta (CIVS — ang. *Correspondent Identity Verification System*). Główną funkcją systemu CIVS jest autoryzacja przesyłanej depeszy w łańcuchu telekomunikacyjnym. System CIVS został zaprojektowany i zaimplementowany w środowisku Matlab 7.0 i został przetestowany w różnych warunkach akustycznych.

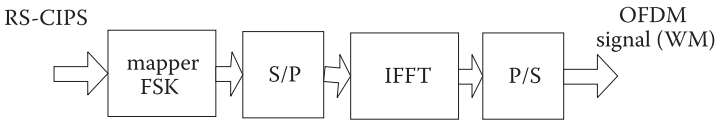
2. Schemat blokowy SYSTEMU

Na rysunku 1 przedstawiono schemat nadajnika i odbiornika systemu znakującego:



Rys. 1. Schemat blokowy nadajnika i odbiornika CIVS

Sygnatura cyfrowa CPIS[1] jest niepowtarzalną sekwencją binarną, dedykowaną tylko na potrzeby jednej sesji. CIPS podlega kodowaniu zabezpieczającemu kodem Reeda-Solomona (oznaczenie: RS-CIPS) w celu uczynienia sygnatury znaku wodnego odporną na błędy pojawiające się podczas transmisji. Modulator OFDM (ang. *Orthogonal Frequency Division Multiplexing*) generuje sygnał modulowany sekwencją binarną RS-CIPS. Podstawowy schemat modulatora OFDM przedstawiono na rysunku 2.



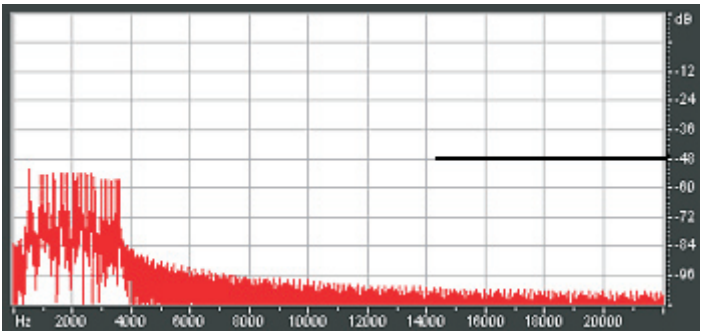
Rys. 2. Podstawowy schemat modulatora OFDM

Strumień binarny RS-CIPS jest podawany na mapper FSK, który wypełnia przedziały FFT (generuje sinusoidy o ustalonej częstotliwości w danym przedziale widmowym) w zależności od wartości logicznej bitu. Konwersja z formy szeregowej na równoległą jest konieczna do przekształcenia widma sygnału z dziedziny częstotliwości na dziedzinę czasu. Sygnał znaku wodnego (ang. WM — *Watermark*) jest rozmieszczony w paśmie 4 kHz. Widmowa gęstość mocy (ang. PSD — *Power Spectum Density*) sygnału oryginalnego jest skoncentrowana w tym regionie, zatem kodowanie znaku wodnego będzie najbardziej efektywne w przypadku skoncentrowania sygnatury znaku wodnego właśnie w tym paśmie. Filtr HAS posiada wbudowaną procedurę MPEG-1[2], która jest odpowiedzialna za wyznaczenie tzw. poziomu JND (ang. *Just Noticeable Difference level*). Filtr HAS jest filtrem dwuetapowej korekcji znaku wodnego: w pierwszym etapie dopasowywany jest kształt widmowy znaku wodnego wygenerowanego metodą OFDM, a w drugim etapie (w oddzielnej procedurze) dopasowany jest poziom znaku wodnego poniżej poziomu sygnału oryginalnego. Dwuetapowa korekcja przedstawiona jest na rysunkach 3 i 4. Pozioma linia na rysunkach oznacza poziom referencyjny –48 dB, pomocny w określeniu różnicy poziomu sygnału przed korekcją i po niej.

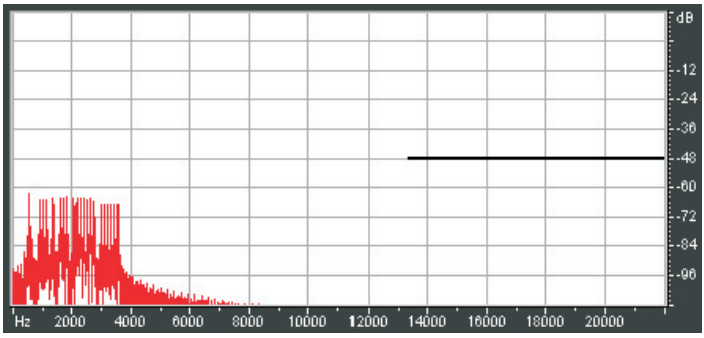
Odbiornik znaku wodnego wykorzystuje blok uśredniania koherentnego. Uśrednianie widma redukuje wariancję szumu dla komponentów nieskorelowanych i nie jest powiązane z algorytmem MPEG-1. W omawianej aplikacji szum jest reprezentowany przez sygnał oryginalny, który nie jest skorelowany, w przeci-

[1] CPIS — ang. *Correspondent Personal Identification Signature*.

[2] MPEG-1 — *Moving Pictures Expert Group* — standard [ISO91] kodowania stratnego dźwięku dla warstwy pierwszej, opublikowany w 1991 r.



Rys. 3. Pierwszy etap korekcji widma znaku wodnego: kształtowanie widma do kształtu widma sygnału oryginalnego



Rys. 4. Drugi etap korekcji widma: korekcja poziomu widma znaku wodnego

wieństwie do sygnału znaku wodnego. Zysk wzmocnienia SNR_{coh} [6], dla metody uśredniania koherentnego jest opisany jako:

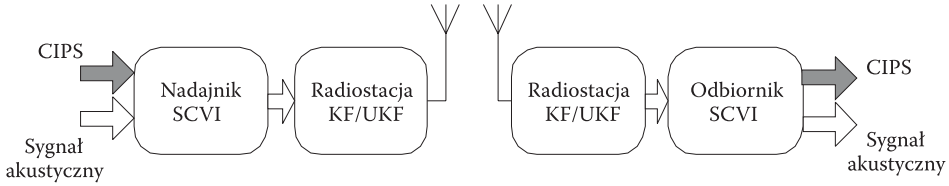
$$SNR_{coh} = \frac{\delta_{org}}{\delta_{org} / \sqrt{M}} = \sqrt{M}, \tag{1}$$

gdzie: δ_{org} — odchylenie standardowe sygnału oryginalnego;
M — liczba iteracji (uśrednień sygnału).

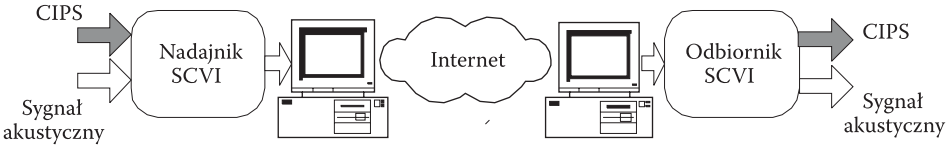
Można zauważyć, że SNR_{coh} jest proporcjonalny do pierwiastka kwadratowego z liczby uśrednień M. Dekoder przedstawiony na rysunku 1 jest odpowiedzialny za poprawne dekodowanie znaku wodnego. Zastosowano tutaj detekcję poziomów prążków znaku wodnego jako regułę decyzyjną. Wyjściowy strumień binarny jest poddawany procedurze korekcji błędów w dekoderze *Reeda-Solomona*, zatem gwarantowany jest poprawny odbiór CIPS z mocą korekcji kodu detekcyjno-korekcyjnego.

3. Stanowisko testowe

Przeprowadzono testy laboratoryjne w celu weryfikacji poprawności kodowania i dekodowania CIPS. Stanowisko badawcze składało się z radiostacji KF/UKF z wykorzystaniem łącza akustycznego po stronie odbiorczej. W drugiej wersji stanowiska wykorzystano łącze internetowe. Konfigurację obu stanowisk przedstawiono na rysunkach 5 i 6.



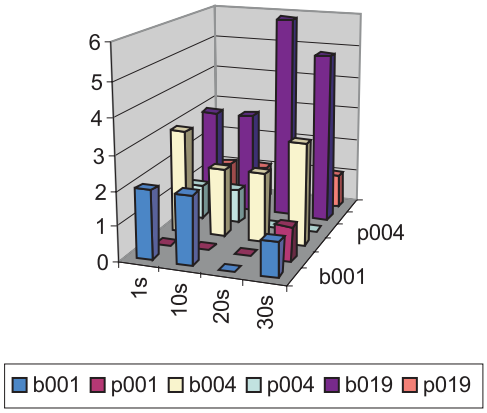
Rys. 5. Stanowisko testowe — łącze KF/UKF



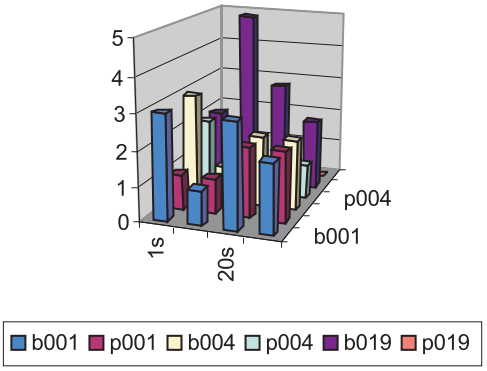
Rys. 6. Stanowisko testowe — łącze internetowe VoIP

4. Wyniki testów: Dekodowanie CIPS w sygnale pozbawionym znaku wodnego

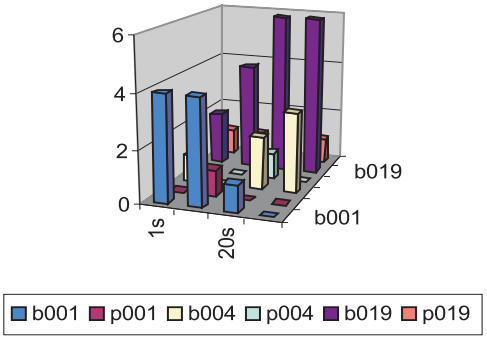
Jednym z krytycznych wymogów narzuconych na system jest spełnienie warunku odporności na błędy typu *false positive*, czyli: detekcja znaku wodnego w przypadku jego braku w sygnale oryginalnym. Poniżej przedstawiono wyniki eksperymentów potwierdzających odporność tego formatu kodowania na błędy *false-positive*. Eksperymentów dokonano dla różnych warunków akustycznych: cisza, biuro, transporter opancerzony oraz różnych czasów uśredniania koherentnego: 1, 10, 20 oraz 30 s. Testy przeprowadzono dla różnych ścieżek muzycznych oznaczonych symbolami: 001, 004 oraz 019.



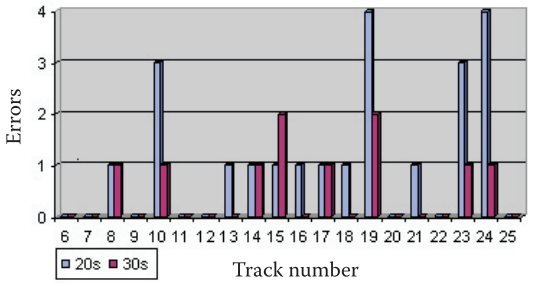
Rys. 7. Dekodowanie CIPS w sygnale pozbawionym CIPS. Sygnał akustyczny nie jest zdegradowany, nie jest zakłócony innymi sygnałami akustycznymi, cisza, SNR = 10 dB



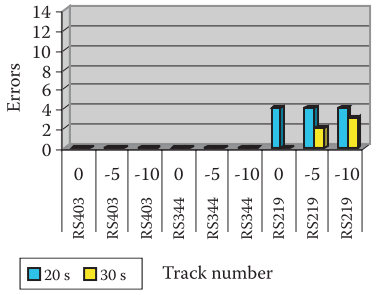
Rys. 8. Dekodowanie CIPS w sygnale pozbawionym CIPS. Sygnał akustyczny zdegradowany (biuro, SNR = –10 dB)



Rys. 9. Dekodowanie CIPS w sygnale pozbawionym CIPS. Sygnał akustyczny zdegradowany (transporter opancerzony, SNR= –10 dB)



Rys. 10. Dekodowanie CIPS w sygnale z CIPS (cisza, SNR = 10 dB)



Rys. 11. Dekodowanie CIPS w sygnale z CIPS (biuro, SNR = 10 dB)

5. Wyniki testów: Dekodowanie CIPS w sygnale oryginalnym z CIPS

Podstawowym testem było sprawdzenie odporności koncepcji systemu na błędy typu: *false-negative* (brak detekcji znaku w przypadku jego obecności w sygnale oryginalnym). Test przeprowadzono na 25 ścieżkach muzycznych dla różnych czasów uśredniania koherentnego: 20 s i 30 s oraz różnych warunków akustycznych. Zdolność korekcyjna zastosowanego kodu to 4 bity, zatem system potwierdził swoją przydatność, ponieważ kod *Reeda-Solomona* poprawnie rozpoznawał miejsca, w których wystąpiły przekłamania do czterech błędnie zdekodowanych bitów (rys. 10 i 11).

6. Wnioski

Zaprezentowane wyniki badań nad eksperymentalnym systemem znakującym dowodzą, że możliwe jest przesyłanie sygnatury CPIS o niewielkiej liczności (kilka bitów) w tle sygnału akustycznego przez łącza radiowe oraz cyfrowe łącza transmisji danych. System wymaga jeszcze wielu badań sprawdzających jego potencjalną

przydatność w wojskowych systemach łączności KF/UKF, m.in. odporności na standardowe czynniki degradujące, np. resampling, rekwantyzację, szum addytywny oraz na ataki celowe i odporność na stegoanalizę, czyli na detekcję opartą na zaawansowanej analizie statystycznej w celu stwierdzenia istnienia znaku wodnego w danym sygnale.

Artykuł wpłynął do redakcji 19.07.2006 r. Zweryfikowaną wersję po recenzji otrzymano 9.10.2006 r.

LITERATURA

[1] I. J. Cox, M. L. Miller, J. A. Bloom, *Digital Watermarking*, Academic Press, 2002.

[2] M. Arnold, *Audio watermarking: features, applications and algorithms*, IEEE Proceedings 2000, Department for Security Technology for Graphics and Communication Systems Fraunhofer--Institute for Computer Graphics.

[3] W. Bender, D. Gruhl, N. Morirrnoto, A. Lu, *Techniques for data hiding*, IBM Systems Journal 35, no. 3&4, 1996, 313-336.

[4] Changsheng Xu, Jiankang Wu, Qibin Sun, *Digital Audio watermarking and its applications in multimedia database*, Signal Processing and its applications ISSPA'99Brisbane, Australia, 22-25 August, 1999.

[5] F. A. Everest, *Master Handbook of Acoustics,* McGraw-Hill Companies Inc., 2001.

[6] R. G. Lyons, *Understanding Digital Signal Processing*, Addison Wesley Longman Inc, 1997.

Z. PIOTROWSKI, J. ŁOPATKA, P. GAJEWSKI

Conception of a system of radio correspondent authorization

Abstract. The proposed conception of the authorization system is based on both OFDM and watermarking technology and using CPIS - *Correspondent Personal Identification Signature*. CPIS can represent, e.g., biometrics data of the radio correspondent. The main idea of the proposed solution is authorization of the end-user in KF/UHF radio channels and Internet. The base scheme of transmitter and receiver is described as well as work principles of the dedicated system. In the paper, the results of the preliminary tests as well as the conclusions are given.

Keywords: telecommunication, acoustic, watermark, subjective tests
Universal Decimal Classification: 621.39