Paper

New model of identity checking in telecommunication digital channels

Piotr Gajewski, Jerzy Łopatka, and Zbigniew Piotrowski

Abstract— We proposed an OFDM and watermarking based technology system for correspondent identity verification (CIVS) in military telecommunication digital channels. Correspondent personal identity signature (CPIS) is represented by digital watermark. The main idea of this system solution is to verify the end user who sends acoustic signal, e.g., speech, music, etc., via Internet, HF/UHF radio, modem, etc. OFDM modulation scheme is used to prepare secret digital signature. This signature is a single-use secret key used for correspondent verification, thus binary sequence of that key is changing for every session. We describe transmitter and receiver block scheme. The results of experiments for both ideal and degraded signals are described in details too. The results are summarized with comments and conclusion.

Keywords—identity checking, watermark, watermark transceiver, watermark receiver, OFDM generator, watermarked host quality, ITU-BS1116-1 test, subjective quality test.

1. Watermarking eruption

At present we are the witnesses of large watermarking application eruption. The efficiency of the personal computers enables realization of even very computational expensive algorithms. The goal of the watermarking technology is to hide additional signal under another, host signal. This additional signal can be a clear or encrypted sequence stream. Main methods for audio watermarking are well documented [1–5]. Following schemes are the most popular:

- phase modulation,
- spread spectrum,
- quantized index modulation o frequency and amplitude keying,
- echo modeling,
- least significant bit (LSB) coding.

Goals of actual investigations conducted in many laboratories concentrate on finding optimal compromise between: robustness, data payload and watermark transparency. The ideal watermarking system can produce signal transparent for human auditory system (HAS) [7], enables hidden message reliability and robustness against intentional attacks. A potential watermarking application for military purposes can be, a system for correspondent identity verification (CIVS). The main CIVS feature is message sender authorization in telecommunication channels. CIVS were designed and implemented as software in Matlab 7.0 environment and was tested in various acoustical environment conditions.

2. System for correspondent identity verification scheme

Figure 1 shows a scheme of CIVS transmitter and receiver. Digital signature (CPIS) is a unique binary sequence, dedicated for only one session. This correspondent personal identity signature (CPIS) is coded with Reed-Solomon-correspondent identity personal signature (RS-CIPS) procedure to make CPIS robust against errors at the receiver side. Six additional bits were entered to the output RS-CIPS to ensure proper detection of false positive errors.

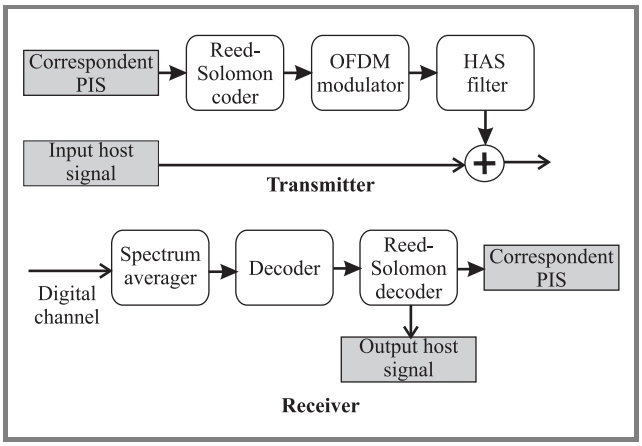

Fig. 1. CIVS transmitter and receiver scheme.

An orthogonal frequency division multiplexing (OFDM) modulator generates a signal according to RS-CIPS. Basic OFDM modulation scheme is illustrated in Fig. 2.

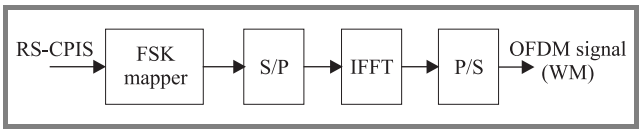

Fig. 2. Basic OFDM modulation scheme.

Binary stream in RS-CIPS form, modulate frequency shift keying (FSK) mapper, that decides which fast Fourier transform (FFT) bin should be filled. Serial to parallel conversion is required to process spectrum by IFFT function. Signal need to be converted into serial form to create an OFDM signal in time domain. Orthogonally formed harmonics are shown in Fig. 3.

Watermark signal (WM) is located in 4 kHz frequency band. Power spectrum density function (PSD) of the host signal is cumulated on this region, and it is more efficient to hide relatively stronger additional signal (WM) under host signal in this region. HAS filter contains build-in MPEG-1 audio analysis procedure to compute just noticeable difference level (JND).

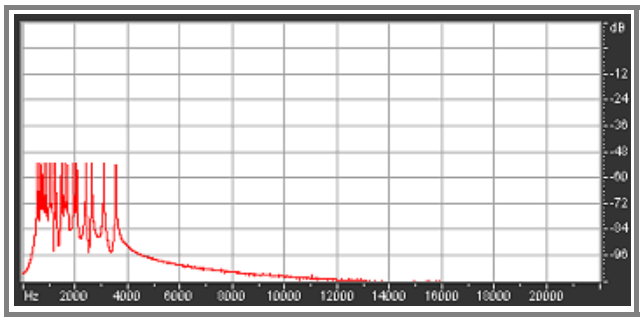

Fig. 3. OFDM generated watermark.

Signal that possesses less PSD then estimated JND is not noticeable by HAS at host signal presence. Input host signal is processed by MPEG-1 algorithm to inform HAS filter about host's JND threshold level. HAS filter is a two-stage, frequency band corrector. First stage of HAS filtering is a watermark spectrum shaping according to the host signal spectrum. The second one is correcting a power level of watermark spectrum below estimated JND threshold. Two-stage of HAS filtering is shown in Figs. 4 and 5.

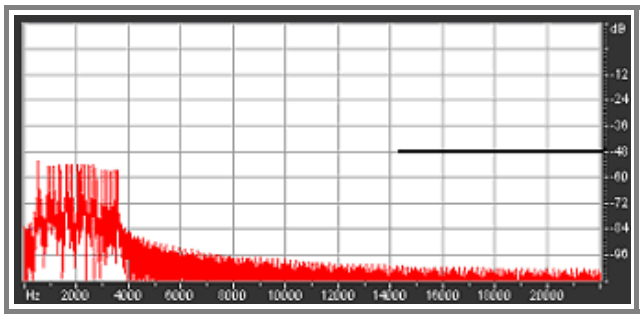

Fig. 4. First stage of HAS filtering: spectrum shaping.

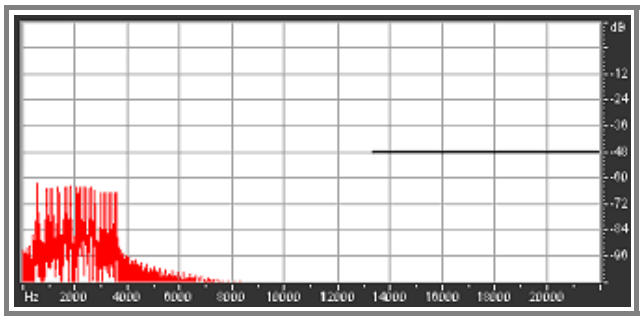

Fig. 5. Second stage of HAS filtering: level correction.

The effect of the HAS filtering can be illustrated by comparing WM before and after two-stage correction process (Figs. 6 and 7).

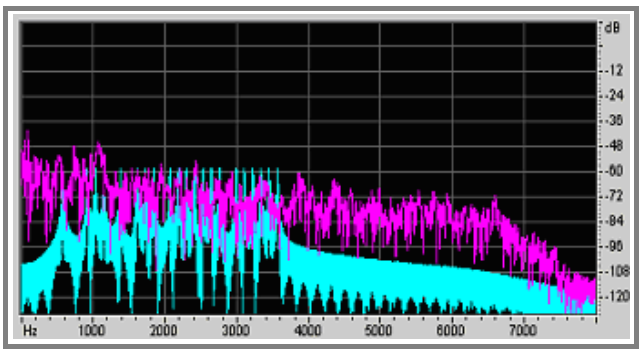

Fig. 6. WM before HAS filter correction.

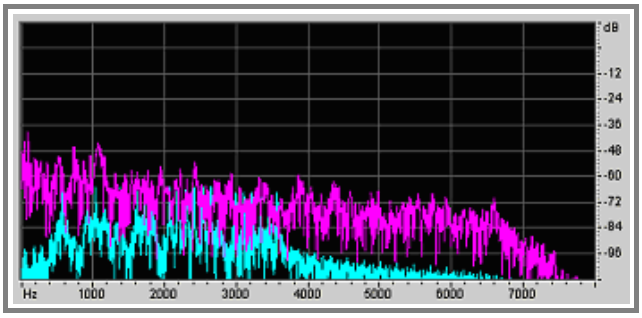

Fig. 7. WM after HAS filter correction.

Watermark receiver bases on main module: coherent spectrum averager. Spectrum averaging can reduce noise by reducing its standard variation for uncorrelated components. In this application the noise is represented by a host signal, which is not correlated contrary to WM, because WM is periodically generated according to the same pattern. Watermark gain SNR_{coh} [6] in this method is given as:

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

where:

δ_{org} – standard deviation of the original signal,

M – number of averaging frames.

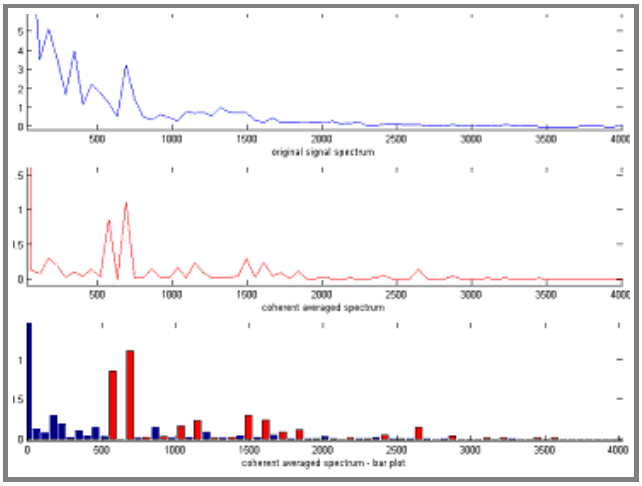

Fig. 8. Spectrum of the watermarked host, before and after coherent averaging.

We can notice, that SNR_{coh} is proportional to the square root of the M number averaging frames. Decoder, presented in Fig. 1, is responsible for correct decision. Decoder rule bases on WM level detection. The binary output stream is error corrected in Reed-Solomon decoder, thus correct CPIS should be received. The result of the coherent averaging process is shown in Fig. 8.

3. Quality of watermarked signal

Coding WM in the audio host signal we agree on degradation of this signal. The standard ITU-BS1116-1 test [8] can estimate quality of watermarked signal and degree of its degradation. In our test set of 22 listeners were asked to assess quality of tracks, watermarked by CIVS. ITU-BS1116-1 describes in details full procedure and environment conditions to be fulfilled to get reliable results. Five points degree scale is used for watermarked signal quality estimation (Table 1).

Table 1
Grading scale for ITU-BS1116-1 test

Impairment	Grade
Imperceptible	5.0
Perceptible, but not annoying	4.0
Slightly annoying	3.0
Annoying	2.0
Very annoying	1.0

One subject at a time is involved and the selection of one of three stimuli ("A","B","C") is at the discretion of this subject. The known reference is always available as stimulus "A". The hidden reference and the object are simultaneously available but are "randomly" assigned to "B" and "C" depending to the trial. Listener assesses which one from two similar signals "B" or "C" is watermarked.
Based on this grading scale, the diff grades scale (SDG) values are computed. Signal is imperceptible if SDG is higher than –1 value. In case the SGD is a positive value, it indicates that listener assessed that watermarked signal had better quality then the host. Results of carried out ITU BS1116-1 test are illustrated in Fig. 9.
We observe in Fig. 9, that group of listeners could not correctly recognize embedded watermark in tracks. None of the tested tracks achieved –1 SDG value.

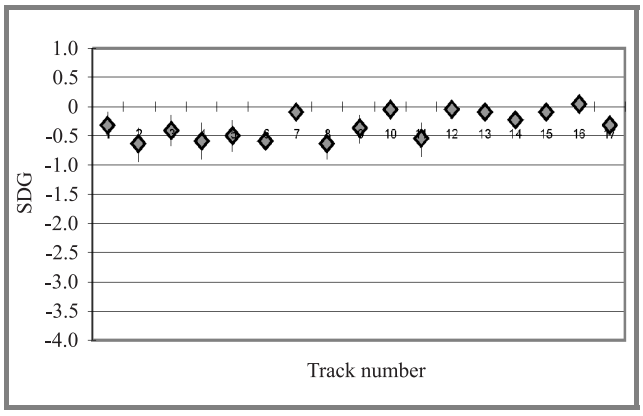

Fig. 9. SDG values for tracks coded by SCVI transmitter.

4. Test beds for CIVS

Laboratory tests were carried out for evaluation of the CPIS coding and decoding effectiveness and were conducted using HF/UHF radio stations with acoustic link on the receiver side. Internet SCVI mode based on standard voice over Internet Protocol (VoIP) is also available and passed, the same procedures carried out in radio link mode. Configurations of test beds are illustrated in Figs. 10 and 11.

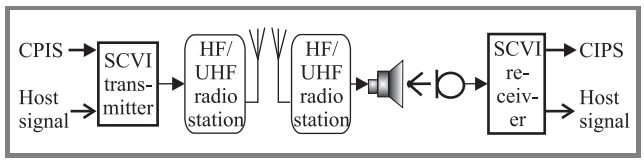

Fig. 10. Test bed CIVS – HF/UHF radio link mode.

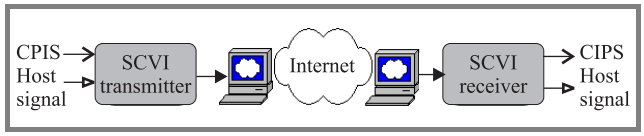

Fig. 11. Test bed CIVS – Internet VoIP mode.

The CIVS works in HF/UHF radio link with acoustic link on the receiver side, or in Internet using voice over Internet Protocol. Radio link mode with acoustic link requires very stable and precise quartz clocks for timing a/d and d/a converters with ±1 ppm short-time stability. This requirement must be fulfilled to ensure coherention in spectrum averager module.

5. Decoding host signal without embedded CPIS

One of the critical imposed requirements is SCVI robustness against wrong decision (false positive errors). When host signal is not watermarked, decoder must detect this fact and inform user that correspondent is not authorized for lack of valid CPIS. We examined decoding process in various acoustic environments (Fig. 10): silent, office, HMMV. Results of CIPS decoding (27 bits length) are illustrated in Figs. 12, 13 and 14. Figures show the performance of the CIVS decoder for various input signal duration time 1 s, 10 s, 20 s and 30 s. Thus we can determine the number of M iterations used in formula 1 and SNR_{coh}. The decision that CIPS is not embedded in a host signal is based

on a number of properly decoded "pilot" bits (p). Transmitter embedded six pilot bits and four or more (up to 6) correct decoded bits are enough to detect a fact that host contains a hidden signature. Overall number of decoded bits is indicated as (b) in Figs. 12, 13, and 14, and symbols of the three decoded tracks were indicated as 001, 004 and 019.

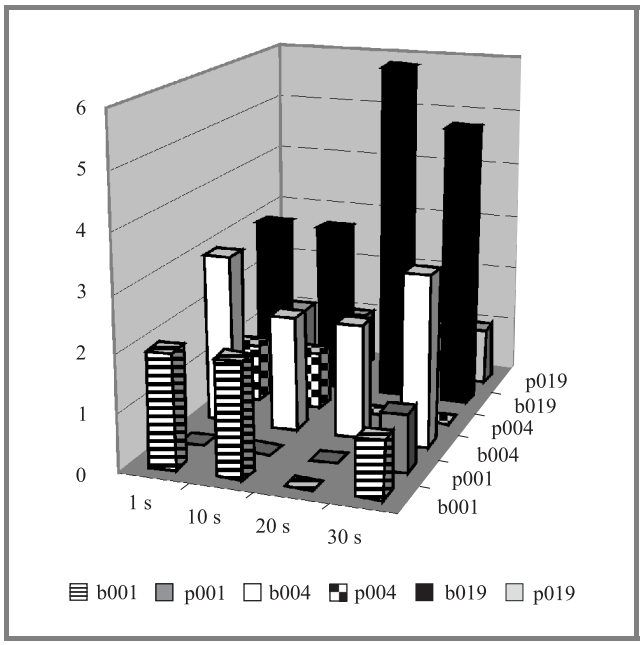

Fig. 12. Decoding host signal without embedded CIPS. Acoustic signal not degraded (silence, $SNR = 10$ dB).

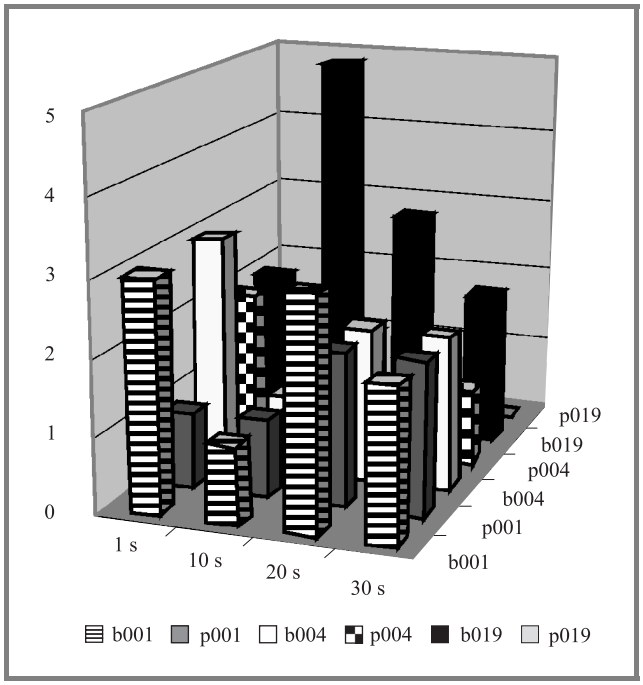

Fig. 13. Decoding host signal without embedded CIPS. Acoustic signal degraded (office, $SNR = -10$ dB).

Summarizing, CIVS will not detect CIPS in host signal until host signal will be coded by this system. Thus host signal itself can not produce false-positive decision ("silent") even if it is degraded by strong (–10 dB) degrading signal ("office", "HMMV").

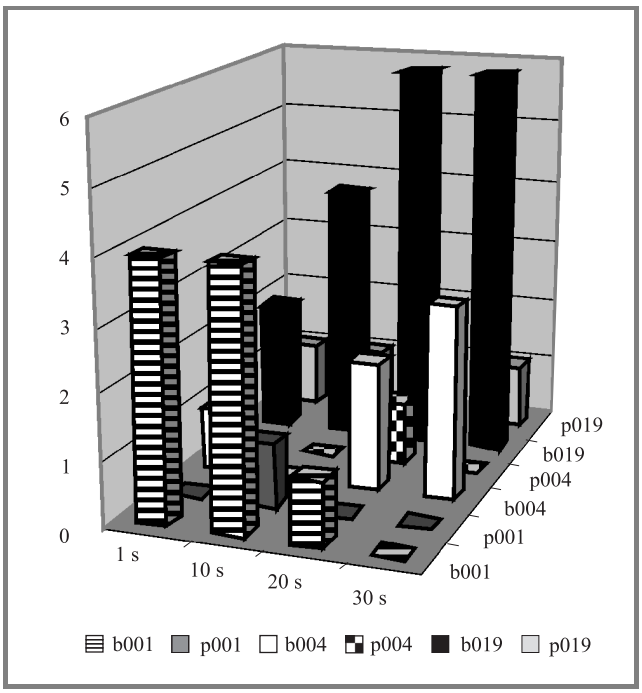

Fig. 14. Decoding host without embedded CIPS. Acoustic signal degraded (HMV, $SNR = -10$ dB).

6. Decoding watermarked host signal

We verified the correctness of CIPS decoding when host signal is watermarked by CIVS. We examined decoding process in various acoustic environments: silent (25 tracks), office (3 tracks), high-mobility multi-purpose vehicle (HMMV) (3 tracks) and for various input signal duration time: 20 s and 30 s. Results of decoding CIPS (27 bits length) are illustrated in Figs. 15, 16 and 17. Decoder gives correct CIPS even for very strong degraded signal (–10 dB). In all cases CIVS detects a fact that sig-

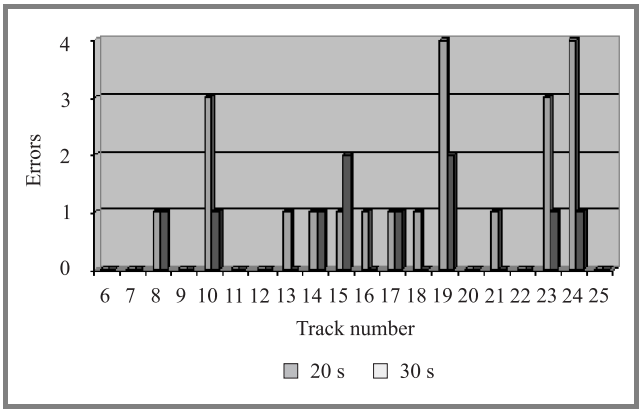

Fig. 15. Decoding host signal with embedded CIPS. Acoustic signal not degraded (silence, $SNR = 10$ dB).

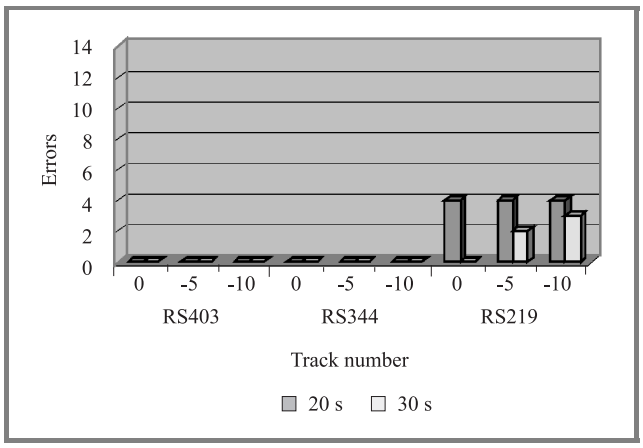

Fig. 16. Decoding host signal with embedded CIPS. Acoustic signal degraded (office).

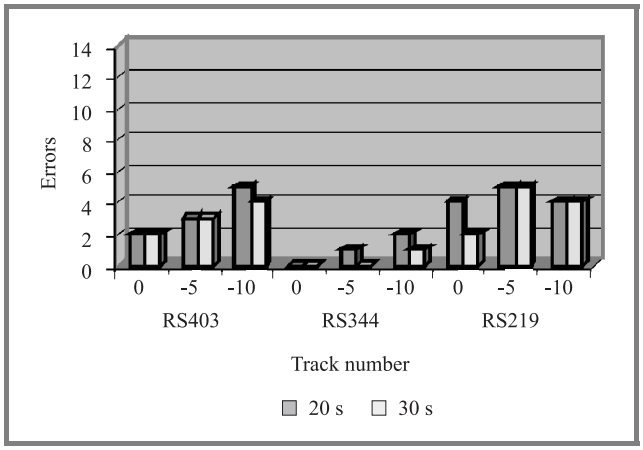

Fig. 17. Decoding host signal with embedded CIPS. Acoustic signal degraded (HMMV).

nal is watermarked. Because proposed Reed-Solomon code scheme has ability to correct only 3 bits, the figures where number of errors is higher than 3, decoded CIPS was not correct.

7. Just noticeable difference level changing

We verified the correctness of CIPS decoding when host signal is watermarked by CIVS using various modifications of JND level. Signal-to-mask ratio (SMR) coefficient describes proportion between power of host signal and WM. Standard MPEG-1 psychoacoustic procedure compute SMR = JND level for audio host signal and this is optimal value from listener point of view, but when SMR level is smaller we can decode MW with greater efficiency (higher WM power) and with higher probability that HAS recognize watermarked signal. In opposite, higher SMR can reduce watermark HAS detection probability to zero but correct WM detection will be impossible because of too small WM power. In this experiment we correct JND level using values: –9 dB –6 dB –3 dB 0 dB 3 dB 6 dB and 9 dB thus 0 dB equals JND level computed for MPEG-1. Duration time 10 s for each from three tested tracks was assumed. Results of this experiment are illustrated in Figs. 18, 19, 20 and 21. We can notice that

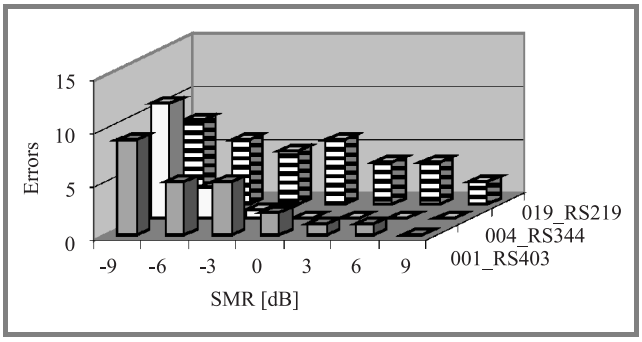

Fig. 18. Errors in SMR function.

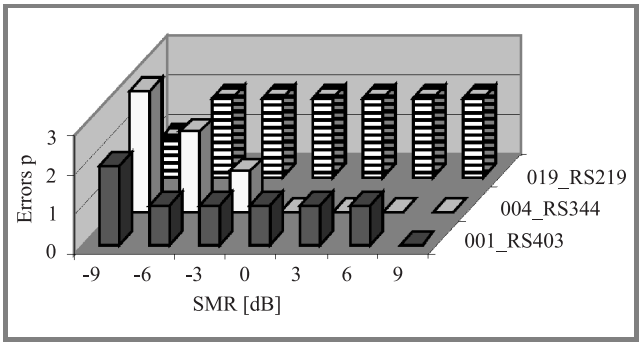

Fig. 19. Pilot errors in SMR function.

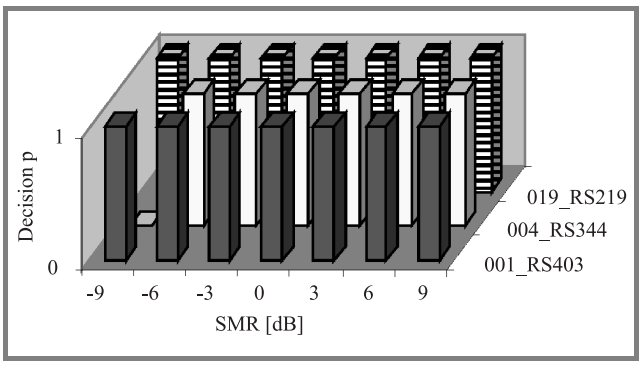

Fig. 20. CIVS decisions for WM presence detection.

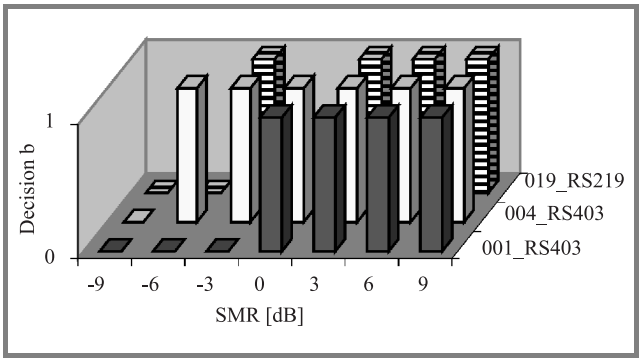

Fig. 21. CIVS decisions for correct CPIS decoding.

CIVS is very robust for false-negative detection. SMR below JND level (0 dB) reduce effectiveness (decoding for 10 s averaging).

8. Conclusion

Presented system proves its usability at the laboratory tests. The correspondent ID signature can be detected with success (watermark transmitted in digital channels, even strongly degraded). Future experiments will concentrate on higher system effectiveness and robustness for loose compression and higher number of embedded bits. CIVS can be used in those military systems where identification has a priority before message interpretation. Implementing hash function for host signal we can get a message authentication system (MAS) and together with CIVS mechanism it enables, high priority message will never be anonymous and always will be integral.

References

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

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

[3] W. Bender, D. Gruhl, N. Morirrnoto, and A. Lu, "Techniques for data hiding", *IBM Syst. J.*, vol. 35, no. 3-4, pp. 313–336, 1996.

[4] C. Xu, J. Wu, and Q. Sun, "Digital audio watermarking and its applications in multimedia database", in *Proc. ISSPA'99*, Brisbane, Australia, 1999.

[5] F. A. Everest, *Master Handbook of Acoustics*. New York: McGraw-Hill, 2001.

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

[7] E. Zwicker, *Psychoacoustics*. New York: Springer-Verlag, 1982.

[8] *Methods for the subjective assessment of small impairments in audio systems including multichannel sound systems*, ITU-R BS.1116-1.

Piotr Z. Gajewski received the M.Sc. and D.Sc. degrees from Military University of Technology (MUT) Warsaw, Poland, in 1970 and 2001, respectively, both in telecommunication engineering. Since 1970 he has been working at Electronic Faculty of Military University of Technology (EF MUT) as a scientist and lecturer in communications systems (radios, cellular, microcellular), signal processing, adaptive techniques in communication and communications and information systems interoperability. He was an Associate Professor at Telecommunication System Institute of EF MUT from 1980 to 1990. From 1990 to 1993 he was Deputy Dean of EF MUT. Currently he is the Director of Telecommunication Institute of EF MUT. He is an author (co-author) of over 80 journal publications and conference papers as well as four monographs. He is a member of the IEEE Vehicular Technology and Communications Societies. He is also a founder member of the Polish Chapter of Armed Forces Communications and Electronics Association.
e-mail: pgajewski@wel.wat.edu.pl
Military University of Technology
S. Kaliskiego st 2
00-908 Warsaw, Poland

Jerzy Łopatka received the M.Sc. and Ph.D. degrees in communications from the Military University of Technology (MUT), Warsaw, Poland. At present he is a Head of Radiocommunication Section in the Telecommunication Institute (MUT). His main research interests include digital signal processing in wireless systems.
e-mail: jlopatka@wel.wat.edu.pl
Military University of Technology
S. Kaliskiego st 2
00-908 Warsaw, Poland

Zbigniew Piotrowski received the M.Sc. and Ph.D. degrees in communications from the Military University of Technology (MUT), Warsaw, Poland, in 1996 and 2005, respectively. At present he is a DSP engineer of Radiocommunication Section in the Telecommunication Institute (MUT). His main areas of interest are speech and audio processing, telecommunication systems engineering and watermarking technology.
e-mail: zpiotrowski@wel.wat.edu.pl
Military University of Technology
S. Kaliskiego st 2
00-908 Warsaw, Poland