(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 085 964 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.08.2009 Bulletin 2009/32

(51) Int Cl.:
G10L 19/00 *(2006.01)*

(21) Application number: **09151967.8**

(22) Date of filing: **03.02.2009**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK TR
Designated Extension States:
AL BA RS

(30) Priority: **04.02.2008 PL 38495008**

(71) Applicant: **Wojskowa Akademia Techniczna im. Jaroslawa Dabrowskiego**
00-908 Warszawa 49 (PL)

(72) Inventors:
- **Piotrowski, Zbigniew**
  05-082, Stare Babice (PL)
- **Gajewski, Piotr**
  03-580, Warszawa (PL)

(74) Representative: **Bury, Lech Marek**
Patpol
ul. Nowoursynowska 162 J
02-776 Warszawa (PL)

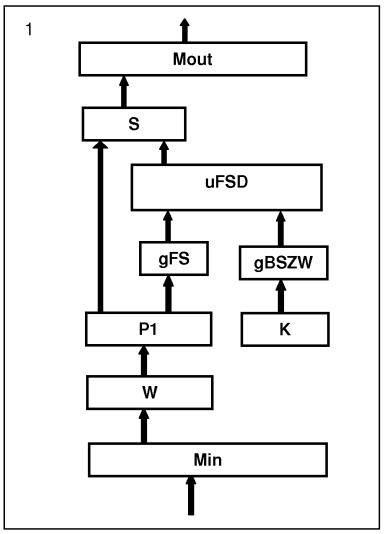
(54) Method and apparatus for subscriber authorization and audio message integrity verification

(57) In the method, to the traffic signal an additional watermark signal is added which is not audible at the presence of the traffic signal, and then the signal is transmitted on a telecommunication link to a subscriber, where it is received and decoded, as a result of which a Watermark Binary Signature and a first Hash Function are received. The Watermark Binary Structure is compared at the receiving side of the link with the declared by the subscriber Watermark Binary Watermark Structure. A second Hash Function is determined from the non-decoded received signal. The two Hash Functions are compared with each other in order to determine whether the audio message has been edited.

To the subscriber's terminal an Electronic Subscriber Module (EMA) is connected which comprises in its structure a transmitting line (1) and a receiving line (2) of an additional signal (SD), in which transmitting line (1) the following main functional blocks are provided: Hash Function generator (gFS) and a Watermark Binary Signature generator (gBSZW), as well as an Additional Signal Generating unit (uFSD), while in the receiving line (2) the following main functional blocks are provided: an Additional Signal decoder (dSD), a Hash Function decoder (dFS), and a Hash Function comparator (kFS).

The advantageous features of the invention are constituted by a function of secret identification of a subscriber and a function of verification of integrity of a traffic signal as a subscriber's audio message, based on the technique of marking traffic channel in telecommunication links. These two functions: subscriber identification and audio message integrity verification, are performed in a secret manner, at the background of the traffic signal, and thus the subscriber with a terminal without the described apparatus connected thereto will not be aware that he is being authorized as a subscriber, and moreover the method and the apparatus are independent from the telecommunication link infrastructure and they do not interfere with its internal components.

fig.1



EP 2 085 964 A2

Description

[0001] The object of the invention is to provide a method and apparatus for secret authorization of a subscriber and verification of integrity of an audio message.

[0002] Watermarking of the speech is know in the art. US Patent Application US 2006/0227968 A1 disclose a time dependant speech watermark system for information integrity identification and tampering detection and damaged area reconstruction for digitally recorded speech that can be used as evidence in the court of law. The known system utilizes the speech characteristics of frame, reconstruction information and time-dependent information to generate watermark for adding to the speech data at the secondary parameters where the impact on the speech quality is minimal. It also provides a detection mechanism of tampering location and tamper way. The analysis scheme, according to the location and the type of the damaged watermark, determines the location and the way of tampering so that the reconstruction can be performed with the reconstruction information established in advance.

[0003] An apparatus is known for authorization of a subscriber, said apparatus being in a form of a subscriber's terminal provided with a function or separate assembly for identification of the caller's number, to which apparatus, in an open manner, signals to identify the telephone number of the calling subscriber are sent by the telephone exchange and on telecommunication links. The identification signals are transmitted between the ring signals in a form of an FSK sequence or a DTMF code, and they are displayed upon decoding in a numeric form in the display of the called subscriber's telephone.

[0004] This service is known as CLIP (Calling Line Identification Presentation) and it has been introduced by numerous telecommunication operators, such as TP SA, Orange, Dialog, Netia, and its purpose is to identify the telephone number of the calling person. However, the CLIP function does not allow to identify the actually calling person, since the telephone number does not identify in an unambiguous manner any specific user. The same telephone may be used by several users. It is neither possible to establish whether the call signal transmitted as an audio message is original or it has been edited; moreover operation of the CLIP Function is based on openly declared signals: FSK sequence or DTMF code, and thus this is not a function that operates secretly, i.e. is invisible for the operator or unauthorized end subscriber.

[0005] The object of the invention is to provide a method and an apparatus to authorize secretly identity of subscribers and to verify integrity of audio messages of the subscribers, in telecommunication systems.

[0006] The method of the invention provides that to a subscriber traffic signal an additional watermark signal is added which is inaudible at the presence of the traffic signal. Lack of audibility of the watermark is ensured by perceptive generation of watermark additional signal to a signal level at which it becomes inaudible at the presence of the traffic signal. The additional watermark signal represents both information on the Watermark Binary Signature (BSZW) assigned to a specific subscriber and on the Hash Function determined basing on the traffic signal. The speech signal with the additional watermark signal added thereto is transmitted on telecommunication links and then it is received and decoded at the subscriber's terminal. As a result of decoding, information on the subscriber's Watermark Binary Signature and on the Hash Function is received which can be subsequently compared with the Hash Function determined basing on the non-decoded received traffic signal. If these two Hash Functions, i.e. the one determined from the decoded received traffic signal and the one determined from the non-decoded received traffic signal, expressed in a binary form, are the same, this means that the traffic signal as an audio message has not been edited.

[0007] The main idea of the apparatus of the invention provides that the Electronic Subscriber Module (EMA) comprises in its structure a transmitting line (1) and a receiving line (2) of the additional watermark signal (SD), in which transmitting line (1) to the socket input (Min) acoustic signal is supplied, and the socket output (Min) is connected to an amplifier block (W), then the output of the amplifier (W) is connected to an analog-to-digital converter block (P1). The output of the first Converter (P1) is connected to the first output of a digital signal adder (S), while the second output of the converter (P1) is connected to a Hash Function generator block (gFS). The output of the (gFS) block is connected to the first input of an Additional Signal Generating unit (uFSD), and the second input (uFDS) is connected to an output of a Watermark Binary Signature generator (gBSZW). The input of the (gBSZW) block is connected to a keyboard unit (K). The output of the Additional Signal Generating unit (uFSD) is connected to the second input of the digital signal adder block (S), and the output of the adder (S) is connected to an output socket of a microphone (Mout). The (Mout) socket is connected to an acoustic input/output interface in the subscriber's terminal. In the receiving line (2) of the Electronic Subscriber Module (EMA), the input of the input socket of the speaker signal (Gin) is connected to an input/output interface of the subscriber terminal, and the first output of the (Gin) block is connected to a speaker signal socket (Gout). The second output of the (Gin) block is connected to an analog-to-digital converter block (P3), the first output of which is connected to an Additional Signal decoder block (dSD), while the second output of the (P3) converter is connected to a Hash Function decoder block (dFS). The first output of the (dSD) block is connected to the first input of a multiplexer block (Mux), while the second output (sDS) is connected to the first output of a Hash Function comparator block (kFS). The output of the (dFS) block is connected to the second input of the (kFS) block, and the output of the Hash Function comparator block (kFS) is connected to the second input of the Multiplexer block

(Mux). The output of the multiplexer block (Mux) is connected to the input of an imaging unit (uZ) which constitutes a display in the subscriber's terminal.

[0008] According to the invention method of marking an audio message by adding an inaudible watermark to voice signal transmitted on a telecommunication channel is characterized in that a watermark comprises a combination of signatures comprising the first signature representing an identification code of the Electronic Subscriber Module, while the second signature representing a result of applying a hash function to physical parameters of the voice signal.

[0009] According to the invention method of reproducing a watermarked audio message transmitted on a telecommunication channel is characterized by deriving from an audio message a combination of the signatures comprising the first signature representing an identification code of the Electronic Subscriber Module while the second signature representing a result of applying a hash function to physical parameters of the voice signal of the audio message; calculating a third signature representing a result of applying a hash function to physical parameters of received watermarked audio message; comparing second signature with third signature.

[0010] Further method according the invention is characterized by presenting the first signature representing an identification code of the Electronic Subscriber Module or presenting a result of comparing second signature with third signature.

[0011] According to the invention apparatus for marking an audio message by adding an inaudible watermark to voice signal transmitted on a telecommunication channel, comprising input stage for receiving a audio message is characterized in that it further comprises means for generating first signature representing an identification code of the Electronic Subscriber Module; means for generating second signature representing a result of applying a hash function to physical parameters of the voice signal of the audio message; means for generating watermark signal being a combination of first signature and second signature; output means for adding a watermark signal to the audio message.

[0012] According to the invention apparatus for reproducing watermarked audio message transmitted on a telecommunication channel , comprising input stage for receiving a watermarked audio message, and is characterized in that it further comprises a means for deriving from an audio message a combination of the signatures comprising the first signature representing an identification code of the Electronic Subscriber Module and the second signature representing a result of applying a hash function to physical parameters of the voice signal of the audio message; means for calculating a third signature representing a result of applying a hash function to physical parameters of received watermarked audio message; means for comparing second signature with third signature.

[0013] According to the invention apparatus for reproducing is further characterized in that further comprises presentation module for presenting the first signature representing an identification code of the Electronic Subscriber Module or the result of comparing the second signature with a third signature.

[0014] The invention is explained further in an exemplary manner with reference to a drawing at which:

fig. 1 presents a block diagram of an apparatus for marking an audio message according to the invention;

Fig. 2 presents a block diagram of an apparatus for reproducing watermarked audio message according to the invention.

[0015] According to the invention, to the acoustic traffic signal, a specially generated additional watermark signal is added, which is inaudible at the presence of the traffic signal. The additional watermark signal includes information on the Hash Function (FS) determined basing on the traffic signal and information on the Watermark Binary Signature (BSZW). The traffic signal with the additional watermark signal added thereto is transmitted on telecommunication links in a hidden manner, and this means that the additional watermark signal is inaudible at the presence of the traffic signal, at the receiving side of the link the signal constituted by a sum of the traffic signal and the additional watermark signal is decoded, as a result of which information on the Hash Function (SF) and on the Watermark Binary Signature (BSZW) is obtained. Two Hash Functions are compared: both the one obtained as a result of decoding the received traffic signal with the included additional watermark signal, and the one determined from the non-decoded received traffic signal with the watermark included. If these two hash functions, expressed in a binary form, are the same, this means that the traffic signal as an audio message has not been edited. Authorization of a subscriber consists here on comparison of the Watermark Binary Signature (BSZW) decoded from the received traffic signal with the included additional watermark signal with the declared at the receiving side of a telecommunication link Watermark Binary Signature (BSZW). If these two BSZW signatures, expressed in a binary form, are the same, this means that the subscriber is the subscriber declared as the user at the receiving side of the link, and it is also important that the additional watermark signal, including information on the binary signature, is inaudible to the subscriber in the traffic signal.

[0016] According to fig. 1 the apparatus for subscriber authorization and for electronic audio message integrity verification, as presented in the drawing, comprises an Electronic Subscriber Module (EMA) which has in its structure a transmitting line (1) and a receiving line (2) of the additional watermark signal (SD), in which transmitting line (1) to the socket input (Min) the acoustic signal is supplied, and the socket output (Min) is connected to an amplifier block (W), then the amplifier output (W) is

connected to an analog-to-digital converter block (P1). The first output of the Converter (P1) is connected to the first input of a digital signal adder block (S), and the second output of the converter (P1) is connected to a Hash Function generator block (gFS). The output of the (gFS) block is connected to the first input of an Additional Signal Generating unit (uFSD), and the second input of the (uFSD) is connected to the output of a Watermark Binary Signature generator (gBSZW). To the input of the (gBSZW) a keyboard unit (K) is connected. The output of the Additional Signal Generating unit (uFSD) is connected to the second input of the digital signal adder block (S), and the output of the adder (S) is connected to the output socket of a microphone signal (Mout). The (Mout) socket is connected to an audio input/output interface of the subscriber's terminal.

[0017] According to fig. 2 the apparatus for reproducing watermarked audio signal comprises

[0018] In the receiving line (2) of the Electronic Subscriber Module (EMA), the input of the input socket for the speaker signal (Gin) is connected to an input/output interface of the subscriber's terminal, and the first output of the (Gin) block is connected to a signal socket of a speaker (Gout). The second output of the (Gin) block is connected to an analog-to digital converter (P3), the first output of which is connected to an Additional Signal decoder block (dSD), while the second output of the converter (P3) is connected to a Hash Function decoder block (dFS). The first output of the (dSD) block is connected to the first input of a multiplexer block (Mux), and the second output of the (dSD) is connected to the first output of a Hash Function comparator block (kFS). The output of the (dFS) block is connected to the second input of the (kFS) block, and the output of the Hash Function comparator block (kFS) is connected to the second input of the multiplexer block (Mux).

[0019] The output of the multiplexer block (Mux) is connected to the input of an imaging unit (uZ) which is constituted by a display in the subscriber's terminal.

Claims

1. A method of marking an audio message by adding an inaudible watermark to voice signal transmitted on a telecommunication channel
   characterized in that
   a watermark comprises a combination of signatures comprising
   first signature representing an identification code of the Electronic Subscriber Module
   second signature representing a result of applying a hash function to physical parameters of the voice signal.

2. Method of reproducing a watermarked audio message transmitted on a telecommunication channel
   characterized by
   deriving from an audio message a combination of the signatures comprising
   first signature representing an identification code of the Electronic Subscriber Module
   second signature representing a result of applying a hash function to physical parameters of the voice signal of the audio message;
   calculating a third signature representing a result of applying a hash function to physical parameters of received watermarked audio message;
   comparing second signature with third signature.

3. Method according to claim 2, **characterized by** presenting the first signature representing an identification code of the Electronic Subscriber Module.

4. Method according to claim 2 or 3, **characterized by** presenting a result of comparing second signature with third signature.

5. Apparatus for marking an audio message by adding an inaudible watermark to voice signal transmitted on a telecommunication channel, comprising
   input stage for receiving a audio message
   characterized in that it further comprises
   means for generating first signature representing an identification code of the Electronic Subscriber Module
   means for generating second signature representing a result of applying a hash function to physical parameters of the voice signal of the audio message,
   means for generating watermark signal being a combination of first signature and second signature,
   output means for adding a watermark signal to the audio message.

6. Apparatus for reproducing watermarked audio message transmitted on a telecommunication channel, comprising
   input stage for receiving a watermarked audio message,
   characterized in that it further comprises
   a means for deriving from an audio message a combination of the signatures comprising
   first signature representing an identification code of the Electronic Subscriber Module
   second signature representing a result of applying a hash function to physical parameters of the voice signal of the audio message;
   means for calculating a third signature representing a result of applying a hash function to physical parameters of received watermarked audio message;
   means for comparing second signature with third signature.

7. Apparatus according to claim 6, **characterized in that** further comprises presentation module for presenting

the first signature representing an identification code of the Electronic Subscriber Module or
the result of comparing the second signature with a third signature.

fig.1

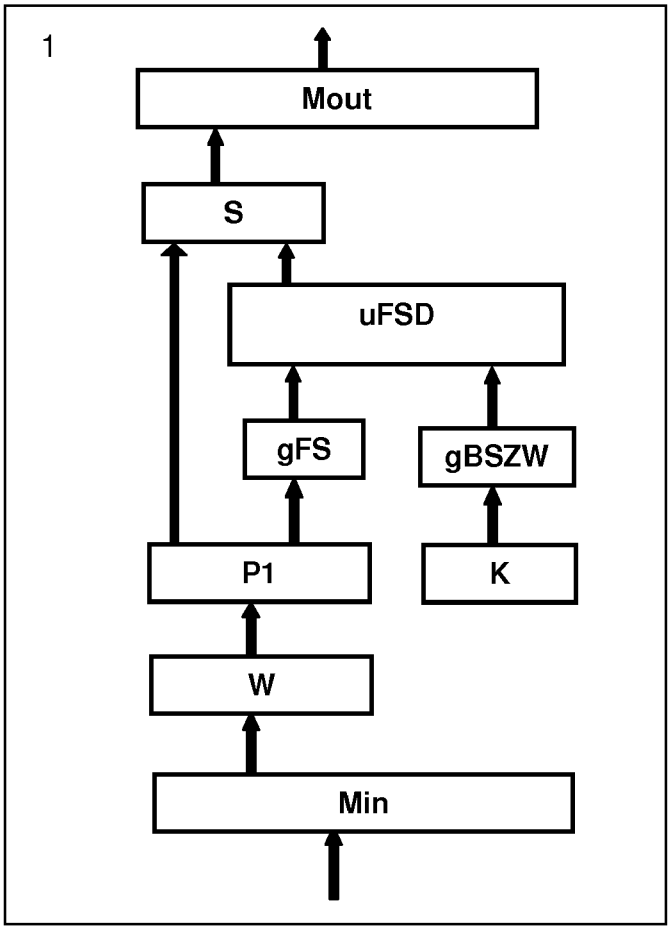
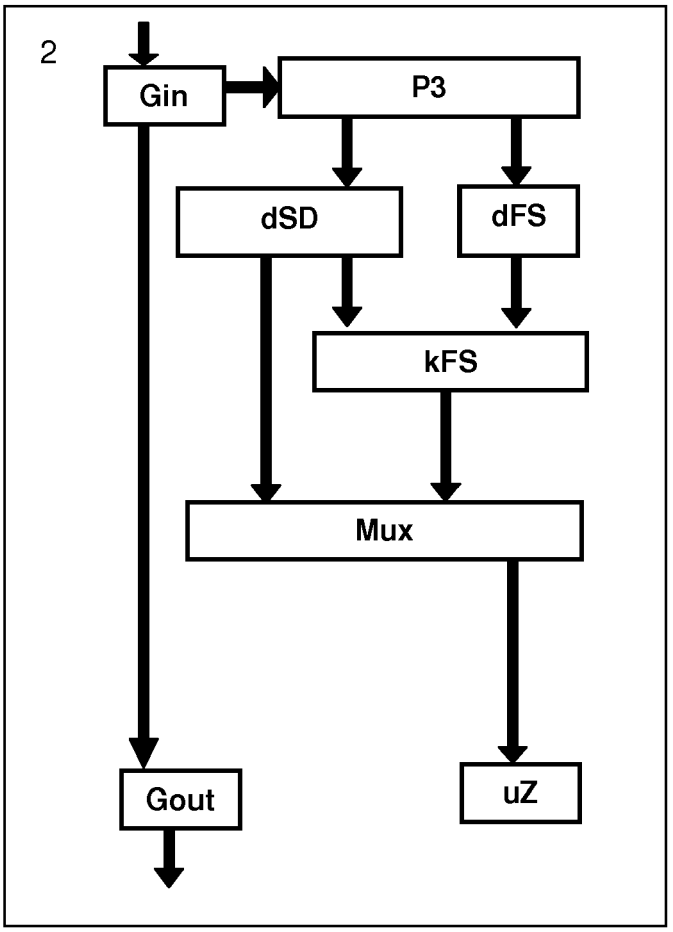


fig. 2



REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 20060227968 A1 **[0002]**