ABSTRACT

Method and device for speech encryption and decryption in voice transmission

In the case of the method according to the invention for speech encryption and decryption in voice transmission as well as the device based on the method, a digitized real voice signal is converted via complex filtering, preferably via Hilbert filtering, into a complex signal which is subjected to sampling rate reduction, the bandwidth of the respective complex filter corresponding to the sampling rate. The complex signal obtained from this is phase-modulated by means of a code signal generated by a random-number generator and is additively combined with a pilot signal, which is likewise phase-modulated in a random distribution, to form an encrypted useful signal to be transmitted. The useful signal is transmitted in a sequential manner together with a preamble which is used for synchronization and useful signal equalization at the receiver end. At the receiver end, on the one hand, clock synchronization for a phase-modulated pilot signal which is produced at the receiver end is forced and, on the other hand, equalizer coefficients for an equalizer (51) at the receiver end are calculated from the digitized received signal, once again after complex filtering and corresponding sampling rate reduction, during a preamble recognition phase, at which point the phase of the useful signal decryption is initialized. The encrypted, transmitted useful signal is separated from its phase-modulated pilot signal, which is superimposed at the transmitter end, by linking to the synchronized pilot signal, which is produced at the receiver end, and the phase-modulated, encrypted digital speech signal thus obtained is subsequently decomposed by means of the code signal which is produced at the receiving end and is clock-controlled by the preamble.

In comparison with known speech encryption methods, the invention has the advantage of very good monitoring security linked with high speech comprehensibility and good voice recognition despite precise conformity with the specified transmission bandwidths available in analog radio networks and in the telephone field.

(Fig. 1)