

A Bone Conduction Communication System and Method Based on Internet of Things ("IoT")

Technical field

[0001] This invention relates to the field of data processing technology, especially a bone conduction communication system and communication method based on Internet of Things.

Background technique

[0002] At present, earphones or bone conduction headsets use manual operation to control the working state of the earphones, which leads to limitations of use. In addition, manual switches also bring inconvenience to the user and put forward new requirements for the industry.

[0003] Regarding the prior art: a voice-controlled bone conduction headset includes a bone conduction headset and a PTT control component connected to the bone conduction headset, as well as a voice control device that is communicatively connected to the PTT control component and controls the on-off of the bone conduction headset. The said PTT control component is a wireless PTT control component, which is wirelessly connected to the bone conduction headset. The PTT control component is a wired PTT control component, which is electrically connected to the bone conduction headset and forms an integral part of the headset. The voice control device is integrated with the bone conduction headset.

[0004] To sum up, the problems with the prior art are that the existing digital voice-controlled bone conduction headset system has a single function and cannot automatically change the desired content according to customers' needs, and that it cannot cooperate with walkie-talkies or other communication equipment to achieve reliable and flexible communication. Furthermore, the existing communication system does not have security and confidentiality control, and is exposed to the potential danger of confidential information leakage.

Summary of the invention

[0005] In order to solve the problems with the prior art, the present invention provides a bone conduction communication system and method based on the Internet of Things.

[0006] The invention is realized by a bone conduction communication system based on the Internet of Things which comprises:

[0007] A headset unit that is used to provide a microphone signal for the voice controller and convert the headset signal provided by the voice controller into corresponding voice;

[0008] A voice controller that is used to control, detect, and communicate the microphone signal transmitted by the headset unit, and converts the signal into a digital signal and compress the signals in real-time into the data in a smaller volume, and send the data to the host computer through the communication system;

[0009] The encryption method of the voice controller specifically includes the following steps:

[0010] Step 1. Define the random function funA, generate several pairs of random integers (x, y) according to the length of the video file, store them in the set $S\{ \}$, and save the set S in the attribute field of the corresponding video file in the database to control the Y value of the size of the generated video encrypted file <10 ;

[0011] Step 2: Read the video file stream by byte, read the stored set $S\{ \}$ from the database according to the information of the video file, and obtain all the random pairs;

[0012] Step 3: According to the data pair (x, y), write a random string of Y length at the X position in the file stream, and write the file stream into the encrypted video file stream;

[0013] Step 4. Repeat step 3 until the file is read and written;

[0014] The signal receiving module is connected to the headset unit and the voice controller for the reception of voice signals;

[0015] The encryption module is connected to the said signal receiving module for the encryption of the voice signals;

[0016] The encryption method of the said encryption module includes:

[0017] 1) CA initialization module, run $\text{Setup_CA}(1^\lambda)$;

[0018] Select the safety parameter 1^λ at the selection stage of a prime number p , generate a group G with and the generator g , and define a bilinear mapping $e: G \times G \rightarrow G_1$ to satisfy bilinearity, non-degeneration, and computability. Choose a hash function $H: \{0,1\}^* \rightarrow G$. Determine the set I of all attributes in the system; initialize the token tree according to the number of attribute authority AA , determine the private key S_K for each attribute authority AA , and map S_K to the random key RK_j of the leaf node of the token tree one by one. Determine the minimum cover key set $MCKS$, let $G(x)$ represent the set of AA containing attribute x . $\varphi(x)$ is the set of leaf nodes in the token tree corresponding to AA in the attribute group $G(x)$. $\varphi^{(x)}$ is the minimum coverage $\varphi(x)$ node-set of the token tree, the minimum coverage key set $MCKS_x$ represents the combination of random keys corresponding to all the nodes of $\varphi^{(x)}$, then $MCKS = \{MCKS_x\}_{x \in I}$. Determine the token chain set TCS , let n_i be a leaf node in the token tree, then TCS_i represents the set of all tokens that n_i passes to the root node

$$GTDM = \{g^{TD_x}\}_{x \in I} \circ \forall \alpha, \beta \in \mathbb{Z}_p,$$

$TCS = \{TCS_i\}_{i \in I}$. For each attribute $x \in I$, determine a trapdoor TD_x . Encrypt the trapdoor with the key in the minimum coverage key set $MCKS_x$, obtain the trapdoor information TDM_x corresponding to the attribute x , and generate the trapdoor public key. Publicly release $PP = \{e(g, g)^\alpha, TCS, g^\beta, g^\alpha, GTDM, H\}$, and retain the master key $MSK = (\alpha, \beta, \{TD_x\}_{x \in I})$;

[0019]

- ① AA_K registers with CA, CA runs AA_Reg_CA(). The details are as follows: CA verifies the identity information of AA_K. Upon a successful verification, the key of the leaf node corresponding to AA_K, the set of managed attributes I_K , the trapdoor information $\{TDM_x\}_{x \in I_K}$ corresponding to the attribute, and the value of

$$SK_{AA_K} = \{S_K, I_K, \{TDM_x\}_{x \in I_K}\} \text{ will be sent to AA}_K.$$

[0020]

- ② The user registers with the CA, and the CA runs User_Reg_CA(ID). After the user's real identity ID is authenticated by the CA, and the start and end time of the user authorization and the user's identity are signed by the CA, the certificate will be obtained and returned to the user (Where Cert=ID||t||te||SKCA(ID||t||te));

[0021] AA initializes the module, runs the AA_Setup() function. The detail is shown as follows: select a group-based broadcast encryption scheme, and determine a group for each attribute x for $\forall x \in I_K$ AA_K. The trapdoor information $\{TDM_x\}_{x \in I_K}$ corresponding to its management attribute is encrypted with the private key of the attribute, AT_x . Obtain $TDM_{x, \text{version } 1}$, which will be sent to the CSP. AA_K calculates each attribute managed by it.

[0022] 3) Key generation module. When a user u_j registers, AA_K will run the Key _ Gen (Cert) function. The details are as follows:

AA_K verifies its certificate. If it is correct, selects $\forall v_{x,j}, z_j, k_j \in \mathbb{Z}_p$ randomly for each attribute x of u_j , calculate

$$\{B_{x,j} = A_x^{v_{x,j} \cdot H(ID)} \cdot AT_{x,K}, D_{x,j} = g^{-v_{x,j} \cdot H(ID)}\}_{x \in I_u}, D_{j1} = g^{\alpha/z_j + \beta k_j}$$

and $D_{j2} = g^{-k_j}$, to get the user's private key $sk_{j,k}$, send $sk_{j,k}$ to the user, where

$$sk_{j,k} = \{S_K, \{B_{x,j}, D_{x,j}\}_{x \in I_u}, t_{end}, I_u = \{att_i\}, D_{j1}, D_{j2}, z_j\};$$

[0023] 4) Encryption module. Input plaintext message m , system public parameter PP , data owner runs $\text{Encrypt}(PP, m)$. The details are shown as follows:

[0024] Choose the symmetric encryption key k , and encrypt the confidential information m symmetrically to obtain $E_K(m)$; construct an access control policy $\Gamma=(M, \rho)$, where M is an $l \times d$ matrix, and encrypt the symmetric encryption key k with attributes. Randomly select $s \in \mathbb{Z}_p$, record the vector $\vec{v} = (s, v_2, v_3, \dots, v_d)$, then $\lambda_i = \vec{v} \cdot M_i$, calculate $C = k \cdot e(g, g)^{as}$ for all attributes involved in the access control strategy, obtain the corresponding attribute public key GTDM, and calculate $\{C_i = g^{\lambda_i \cdot TD_i}, C'_i = g^{\beta \lambda_i}\}_{i \in I_A}$ (I_A represents all attributes involved in the access control policy),

And finally, get the ciphertext CT , and send it to the cloud server CSP .

$$CT = \{E_k(m), C = k \cdot e(g, g)^{as}, \{C_i = g^{\lambda_i \cdot TD_i}, C'_i = g^{\beta \lambda_i}\}_{i \in I_A}, (M, \rho)\};$$

[0025] The wireless transceiver module is connected with the voice controller for digital signal data transmission and reception;

[0026] The data management module is used for storing voice information;

[0027] The mobile terminal is connected with the voice controller to receive the digital signal sent by the voice controller through the communication system and share data with the host computer.

[0028] Furthermore, the said voice controller has a built-in frequency analysis unit, a phase curve calculation unit, an error calculation unit, and a sound signal recognition unit;

[0029] The frequency analysis unit analyzes the frequency signal of sound signals;

[0030] The phase curve calculation unit calculates a phase curve that approximates the time change of the phase of the frequency signal;

[0031] The error calculation unit calculates the error between the phase curve and the phase of the frequency signal;

[0032] The sound signal recognition unit identifies whether the sound signal is a periodic sound signal based on the error.

[0033] Furthermore, the said host computer comprises:

[0034] A first channel terminal, a second channel terminal, and a microphone terminal;

[0035] A data sending module that is electrically connected to the microphone terminal, to send data to the mobile terminal;

[0036] A data receiving module that is electrically connected to the second sound channel terminal to receive data from the mobile terminal;

[0037] A safety authentication module that is electrically connected to the data sending module and the data receiving module;

[0038] A power taking module, the input end of which is electrically connected to the first sound channel terminal, and the output end of the power taking module supplies power to the data sending module, the data receiving module, and the safety authentication module.

[0039] Furthermore, the data scan lines include data lines, scan lines and pixels;

[0040] The pixel is formed at the intersection of the data line and the scan line, and includes a first sub-pixel, a second sub-pixel, a third sub-pixel, and a fourth sub-pixel;

[0041] The first sub-pixel includes a first switch, a first liquid crystal capacitor, and a first storage capacitor. The first terminal of the first switch is connected to the scan line, the second terminal of

the first switch is connected to the data line, and the third terminal of the first switch is connected to the first terminal of the first liquid crystal capacitor and the first terminal of the first storage capacitor;

[0042] The second sub-pixel includes a second switch, a second liquid crystal capacitor, and a second storage capacitor. The first terminal of the second switch is connected to the scan line, the second terminal of the second switch is connected to the data line, and the third terminal of the second switch is connected to the first terminal of the second liquid crystal capacitor and the first terminal of the second storage capacitor, and the second storage capacitor line is electrically connected to the second terminal of the second storage capacitor;

[0043] The third sub-pixel includes a third switch, a third liquid crystal capacitor, and a third storage capacitor. The first terminal of the third switch is connected to the scan line, the second terminal of the third switch is connected to the data line, and the third terminal of the third switch is connected to the first terminal of the third liquid crystal capacitor and the first terminal of the third storage capacitor. The second storage capacitor line is electrically connected to the second terminal of the third storage capacitor;

[0044] The fourth sub-pixel includes a fourth switch, a fourth liquid crystal capacitor, and a fourth storage capacitor. The first terminal of the fourth switch is connected to the scan line, the fourth terminal of the fourth switch is connected to the data line, and the third terminal of the fourth switch is connected to the first terminal of the fourth liquid crystal capacitor and the first terminal of the fourth storage capacitor, and the first storage capacitor line is electrically connected to the second terminal of the fourth storage capacitor;

[0045] When the scan line is enabled, the first switch element, the second switch element, the third switch element, and the fourth switch element are turned on, so that the signal of the data line is transmitted to the first sub-pixel, the second sub-pixel, the third sub-pixel and the fourth sub-pixel. When the scan line is disabled, the electrical levels of the first storage capacitor line, the second storage capacitor line, the third storage capacitor line, and the fourth storage capacitor line will be

changed respectively, so that the pixel voltage of the first sub-pixel will have a first offset voltage from the input voltage, the pixel voltage of the second sub-pixel will have a second offset voltage from the input voltage, and the pixel voltage of the third sub-pixel will have a third offset voltage from the input voltage, and the pixel voltage of the fourth sub-pixel will have a fourth offset voltage from the input voltage. Hence, the pixel voltage of the first sub-pixel, the second sub-pixel, the third sub-pixel, and the fourth sub-pixel will be different from each other. Furthermore, the first offset voltage, the second offset voltage, the third offset voltage, and the fourth offset voltage are different from each other.

[0046] Another objective of this invention is to provide a bone conduction communication method based on the Internet of Things, which constitute the following contents:

[0047] The microphone signal is provided through the headset unit. The headset signal provided by the voice controller is converted into a corresponding voice;

[0048] The microphone signal transmitted by the headset unit is controlled, detected, and communicated through the voice controller;

The said signal is converted into a digital signal and compressed in real-time to become data in smaller volume and sent to the host computer through the communication system;

[0049] The voice signal is received through the signal receiving module;

[0050] Encrypt the voice signal through the encryption module;

[0051] Receive and send digital signal data through the wireless transceiver module;

[0052] Store voice information through the data management module;

[0053] Share the data in the form of digital signals with the host computer, which are sent by the reception voice controller to the mobile terminal through the communication system.

[0054] The bone conduction communication system and method based on the Internet of Things provided by the present invention solved the problem that the communication system cannot be encrypted in the existing radio communication, and that the current digital voice-controlled bone conduction headset system has a single function and cannot automatically change the desired content according to customers' needs or cooperate with walkie-talkies or other communication equipment to achieve reliable and flexible communication.

[0055] The invalid radio signals in the Internet of Things are effectively stopped from intrusion, and the valid radio signals are protected. The position of mobile radio terminals can be monitored in real-time. The joint encryption system places a mark on the position of incoming signals to avoid unnecessary loss. The control system is easy to operate and has good applicability.

Description of the drawings

[0056] FIG. 1 is a schematic diagram of a bone conduction communication system based on the Internet of Things according to an embodiment of the present invention.

[0057] In the figure: 1. Headset unit; 2. Voice controller; 3. Signal receiving module; 4. Encryption module; 5. Wireless transceiver module; 6. Data management module; 7. Mobile terminal.

Detailed description

[0058] In order to make clear the objectives, technical solutions, and advantages of the present invention, further descriptions in detail are made below in conjunction with embodiments. It should be understood that the specific embodiments described here are only used to explain the present invention, but not to limit the present invention.

[0059] The application principle of the present invention will be described in detail below with reference to the attached drawings.

[0060] As shown in FIG. 1, the bone conduction communication system based on the Internet of Things according to an embodiment of the present invention includes:

[0061] The headset unit 1 is used to provide a microphone signal for the voice controller and convert the headset signal provided by the voice controller into corresponding voice;

[0062] A voice controller 2, which is used to control, detect, and communicate the microphone signal transmitted by the headset unit, and converts the signal into a digital signal and compress the signals in real-time into the data in a smaller volume, and send the data to the host computer through the communication system;

[0063] The signal receiving module 3 is connected to the headset unit and the voice controller for the reception of voice signals;

[0064] The encryption module 4 is connected to the said signal receiving module for the encryption of the voice signals;

[0065] The wireless transceiver module 5 is connected with the voice controller for digital signal data transmission and reception;

[0066] The data management module 6 is used for storing voice information;

[0067] The mobile terminal 7 is connected with the voice controller to receive the digital signal sent by the voice controller through the communication system and share data with the host computer.

[0068] The encryption method of the voice controller specifically includes the following steps:

[0069] Step 1. Define the random function funA, generate several pairs of random integers (x, y) according to the length of the video file, store them in the set $S\{ \}$, and save the set S in the attribute

field of the corresponding video file in the database to control the Y value of the size of the generated video encrypted file <10;

[0070] Step 2: Read the video file stream by byte, read the stored set $S\{\}$ from the database according to the information of the video file, and obtain all the random pairs;

[0071] Step 3: According to the data pair (x, y), write a random string of Y length at the X position in the file stream, and write the file stream into the encrypted video file stream;

[0072] Step 4. Repeat step 3 until the file is read and written;

[0073] The encryption method of the said encryption module includes:

[0074] 1) CA initialization module, run $\text{Setup_CA}(1^\lambda)$;

[0075] Select the safety parameter 1^λ at the selection stage of a prime number p, generate a group G with and the generator g, and define a bilinear mapping $e: G \times G \rightarrow G_1$ to satisfy bilinearity, non-degeneration, and computability. Choose a hash function $H: \{0,1\}^* \rightarrow G$. Determine the set I of all attributes in the system; initialize the token tree according to the number of attribute authority AA, determine the private key S_K for each attribute authority AA, and map S_K to the random key RK_j of the leaf node of the token tree one by one. Determine the minimum cover key set MCKS, let $G(x)$ represent the set of AA containing attribute x. $\varphi(x)$ is the set of leaf nodes in the token tree corresponding to AA in the attribute group G (x). $\varphi^{(x)}$ is the minimum coverage $\varphi(x)$ node-set of the token tree, the minimum coverage key set $MCKS_x$ represents the combination of random keys corresponding to all the nodes of $\varphi^{(x)}$, then $MCKS = \{MCKS_x\}_{x \in I}$. Determine the token chain set TCS, let n_i be a leaf node in the token tree, then TCS_i represents the set of all tokens that n_i passes to the root node

$$GTDM = \{g^{TD_x}\}_{x \in I} \circ \forall \alpha, \beta \in Z_P,$$

$TCS=\{TCS_i\}_{i \in I}$. For each attribute $x \in I$, determine a trapdoor TD_x . Encrypt the trapdoor with the key in the minimum coverage key set $MCKS_x$, obtain the trapdoor information TDM_x corresponding to the attribute x , and generate the trapdoor public key. Publicly release $PP=\{e(g,g)^\alpha, TCS, g^\beta, g\alpha, GTDM, H\}$, and retain the master key $MSK=(\alpha, \beta, \{TD_x\}_{x \in I})$;

[0076]

- ① AA_K registers with CA, CA runs $AA_Reg_CA()$. The details are as follows: CA verifies the identity information of AA_K . Upon a successful verification, the key of the leaf node corresponding to AA_K , the set of managed attributes I_K , the trapdoor information $\{TDM_x\}_{x \in I_K}$ corresponding to the attribute, and the value of $SK_{AA_K} = \{S_K, I_K, \{TDM_x\}_{x \in I_K}\}$ will be sent to AA_K .

[0077]

- ② The user registers with the CA, and the CA runs $User_Reg_CA(ID)$. After the user's real identity ID is authenticated by the CA, and the start and end time of the user authorization and the user's identity are signed by the CA, the certificate will be obtained and returned to the user (Where $Cert=ID||tb||te||SKCA(ID||tb||te)$);

[0078] AA initializes the module, runs the $AA_Setup()$ function. The detail is shown as follows: select a group-based broadcast encryption scheme, and determine a group for each attribute x for $\forall x \in I_K$ AA_K . The trapdoor information $\{TDM_x\}_{x \in I_K}$ corresponding to its management attribute is encrypted with the private key of the attribute, AT_x . Obtain TDM_x , version 1, which will be sent to the CSP. AA_K calculates each attribute managed by it.

[0079] Key generation module. When a user u_j registers, AA_K will run the $Key_Gen(Cert)$ function. The details are as follows:

AA_K verifies its certificate. If it is correct, selects $\forall v_{x,j}, z_j, k_j \in \mathbb{Z}_p$ randomly for each attribute x of u_j , calculate

$$\{B_{x,j} = A_x^{v_{x,j} \cdot H(ID)} \cdot AT_{x,K}, D_{x,j} = g^{-v_{x,j} \cdot H(ID)}\}_{x \in I_u}, D_{j1} = g^{\alpha/z_j + \beta k_j}$$

and $D_{j2} = g^{-k_j}$, to get the user's private key $sk_{j,k}$, send $sk_{j,k}$ to the user, where
 $sk_{j,k} = \{S_K, \{B_{x,j}, D_{x,j}\}_{x \in I_u}, t_{end}, I_u = \{att_i\}, D_{j1}, D_{j2}, z_j\}$;

[0080] Encryption module. Input plaintext message m , system public parameter PP , data owner runs Encrypt (PP, m). The details are shown as follows:

[0081] Choose the symmetric encryption key k , and encrypt the confidential information m symmetrically to obtain $E_K(m)$; construct an access control policy $\Gamma=(M,\rho)$, where M is an $l \times d$ matrix, and encrypt the symmetric encryption key k with attributes. Randomly select $s \in \mathbb{Z}_p$, record the vector $\vec{v} = (s, v_2, v_3, \dots, v_d)$, then $\lambda_i = \vec{v} \cdot M_i$, calculate $C=k \cdot e(g,g)^{as}$ for all attributes involved in the access control strategy, obtain the corresponding attribute public key GTDM, and calculate $\{C_i = g^{\lambda_i \cdot TD_i}, C'_i = g^{\beta \lambda_i}\}_{i \in I_A}$ (I_A represents all attributes involved in the access control policy),

And finally, get the ciphertext CT , and send it to the cloud server CSP .

$$CT = \{E_k(m), C = k \cdot e(g, g)^{as}, \{C_i = g^{\lambda_i \cdot TD_i}, C'_i = g^{\beta \lambda_i}\}_{i \in I_A}, (M, \rho)\};$$

[0082] the said voice controller 2 has a built-in frequency analysis unit, a phase curve calculation unit, an error calculation unit, and a sound signal recognition unit;

[0083] The frequency analysis unit analyzes the frequency signal of sound signals;

[0084] The phase curve calculation unit calculates a phase curve that approximates the time change of the phase of the frequency signal;

[0085] The error calculation unit calculates the error between the phase curve and the phase of the frequency signal;

[0086] The sound signal recognition unit identifies whether the sound signal is a periodic sound signal based on the error.

[0087] The said host computer comprises:

[0088] A first channel terminal, a second channel terminal, and a microphone terminal;

[0089] A data sending module that is electrically connected to the microphone terminal, to send data to the mobile terminal;

[0090] A data receiving module that is electrically connected to the second sound channel terminal to receive data from the mobile terminal;

[0091] A safety authentication module that is electrically connected to the data sending module and the data receiving module;

[0092] A power taking module, the input end of which is electrically connected to the first sound channel terminal, and the output end of the power taking module supplies power to the data sending module, the data receiving module, and the safety authentication module.

[0093] The data scan lines of the voice controller include data lines, scan lines and pixels;

[0094] The pixel is formed at the intersection of the data line and the scan line, and includes a first sub-pixel, a second sub-pixel, a third sub-pixel, and a fourth sub-pixel;

[0095] The first sub-pixel includes a first switch, a first liquid crystal capacitor, and a first storage capacitor. The first terminal of the first switch is connected to the scan line, the second terminal of the first switch is connected to the data line, and the third terminal of the first switch is connected to the first terminal of the first liquid crystal capacitor and the first terminal of the first storage capacitor;

[0096] The second sub-pixel includes a second switch, a second liquid crystal capacitor, and a second storage capacitor. The first terminal of the second switch is connected to the scan line, the second terminal of the second switch is connected to the data line, and the third terminal of the second switch is connected to the first terminal of the second liquid crystal capacitor and the first terminal of the second storage capacitor, and the second storage capacitor line is electrically connected to the second terminal of the second storage capacitor;

[0097] The third sub-pixel includes a third switch, a third liquid crystal capacitor, and a third storage capacitor. The first terminal of the third switch is connected to the scan line, the second terminal of the third switch is connected to the data line, and the third terminal of the third switch is connected to the first terminal of the third liquid crystal capacitor and the first terminal of the third storage capacitor. The second storage capacitor line is electrically connected to the second terminal of the third storage capacitor;

[0098] The fourth sub-pixel includes a fourth switch, a fourth liquid crystal capacitor, and a fourth storage capacitor. The first terminal of the fourth switch is connected to the scan line, the fourth terminal of the fourth switch is connected to the data line, and the third terminal of the fourth switch is connected to the first terminal of the fourth liquid crystal capacitor and the first terminal of the fourth storage capacitor, and the first storage capacitor line is electrically connected to the second terminal of the fourth storage capacitor;

[0099] When the scan line is enabled, the first switch element, the second switch element, the third switch element, and the fourth switch element are turned on, so that the signal of the data line is transmitted to the first sub-pixel, the second sub-pixel, the third sub-pixel and the fourth sub-pixel. When the scan line is disabled, the electrical levels of the first storage capacitor line, the second storage capacitor line, the third storage capacitor line, and the fourth storage capacitor line will be changed respectively, so that the pixel voltage of the first sub-pixel will have a first offset voltage from the input voltage, the pixel voltage of the second sub-pixel will have a second offset voltage from the input voltage, and the pixel voltage of the third sub-pixel will have a third offset voltage

from the input voltage, and the pixel voltage of the fourth sub-pixel will have a fourth offset voltage from the input voltage. Hence, the pixel voltage of the first sub-pixel, the second sub-pixel, the third sub-pixel, and the fourth sub-pixel will be different from each other. Furthermore, the first offset voltage, the second offset voltage, the third offset voltage, and the fourth offset voltage are different from each other.

[0100] A bone conduction communication method based on the Internet of Things provided by the invention constitutes the following contents:

[0101] The microphone signal is provided through the headset unit. The headset signal provided by the voice controller is converted into a corresponding voice;

[0102] The microphone signal transmitted by the headset unit is controlled, detected, and communicated through the voice controller;

The said signal is converted into a digital signal and compressed in real-time to become data in smaller volume and sent to the host computer through the communication system;

[0103] The voice signal is received through the signal receiving module;

[0104] Encrypt the voice signal through the encryption module;

[0105] Receive and send digital signal data through the wireless transceiver module;

[0106] Store voice information through the data management module;

[0107] Share the data in the form of digital signals with the host computer, which are sent by the reception voice controller to the mobile terminal through the communication system.

[0108] The bone conduction communication system and method based on the Internet of Things provided by the present invention solved the problem that the communication system cannot be

encrypted in the existing radio communication, and that the current digital voice-controlled bone conduction headset system has a single function and cannot automatically change the desired content according to customers' needs or cooperate with walkie-talkies or other communication equipment to achieve reliable and flexible communication. The invalid radio signals in the Internet of Things are effectively stopped from intrusion, and the valid radio signals are protected. The position of mobile radio terminals can be monitored in real-time. The joint encryption system places a mark on the position of incoming signals to avoid unnecessary loss. The control system is easy to operate and has good applicability.

[0109] The above are only preferred embodiments of the utility model patent and are not intended to limit this invention. Any modification, equivalent replacement, and improvement made within the spirit and principle of the invention shall fall under the protection scope of this invention.

Claims

1. A bone conduction communication system based on the Internet of Things is characterized by its composition of:

A headset unit that is used to provide a microphone signal for the voice controller and convert the headset signal provided by the voice controller into corresponding voice;

A voice controller that is used to control, detect, and communicate the microphone signal transmitted by the headset unit, and converts the signal into a digital signal and compress the signals in real-time into the data in a smaller volume, and send the data to the host computer through the communication system;

The encryption method of the voice controller specifically includes the following steps:

Step 1. Define the random function funA, generate several pairs of random integers (x, y) according to the length of the video file, store them in the set $S\{\}$, and save the set S in the attribute field of the corresponding video file in the database to control the Y value of the size of the generated video encrypted file <10 ;

Step 2: Read the video file stream by byte, read the stored set $S\{\}$ from the database according to the information of the video file, and obtain all the random pairs;

Step 3: According to the data pair (x, y), write a random string of Y length at the X position in the file stream, and write the file stream into the encrypted video file stream;

Step 4. Repeat step 3 until the file is read and written;

The signal receiving module is connected to the headset unit and the voice controller for the reception of voice signals;

The encryption module is connected to the said signal receiving module for the encryption of the voice signals;

The encryption method of the said encryption module includes:

1) CA initialization module, run Setup_CA(1^λ);

Select the safety parameter 1^λ at the selection stage of a prime number p , generate a group G with and the generator g , and define a bilinear mapping $e: G \times G \rightarrow G_1$ to satisfy bilinearity, non-degeneration, and computability. Choose a hash function $H: \{0,1\}^* \rightarrow G$. Determine the set I of all attributes in the system; initialize the token tree according to the number of attribute authority AA , determine the private key S_K for each attribute authority AA , and map S_K to the random key RK_j of the leaf node of the token tree one by one. Determine the minimum cover key set $MCKS$, let $G(x)$ represent the set of AA containing attribute x . $\varphi(x)$ is the set of leaf nodes in the token tree corresponding to AA in the attribute group $G(x)$. $\varphi(x)$ is the minimum coverage $\varphi(x)$ node-set of the token tree, the minimum coverage key set $MCKS_x$ represents the combination of random keys corresponding to all the nodes of $\varphi(x)$, then $MCKS = \{MCKS_x\}_{x \in I}$. Determine the token chain set TCS , let n_i be a leaf node in the token tree, then TCS_i represents the set of all tokens that n_i passes to the root node

$$GTDM = \{g^{TD_x}\}_{x \in I} \circ \forall \alpha, \beta \in \mathbb{Z}_p,$$

$TCS = \{TCS_i\}_{i \in I}$. For each attribute $x \in I$, determine a trapdoor TD_x . Encrypt the trapdoor with the key in the minimum coverage key set $MCKS_x$, obtain the trapdoor information TDM_x corresponding to the attribute x , and generate the trapdoor public key. Publicly release $PP = \{e(g, g)^\alpha, TCS, g^\beta, g^\alpha, GTDM, H\}$, and retain the master key $MSK = (\alpha, \beta, \{TD_x\}_{x \in I})$;

- ① AA_K registers with CA, CA runs AA_Reg_CA(). The details are as follows: CA verifies the identity information of AA_K . Upon a successful verification, the key of the leaf node corresponding to AA_K , the set of managed attributes I_K , the trapdoor information $\{TDM_x\}_{x \in I_K}$ corresponding to the attribute, and the value of

$$SK_{AA_K} = \{S_K, I_K, \{TDM_x\}_{x \in I_K}\}$$

will be sent to AA_K .

- ② The user registers with the CA, and the CA runs User_Reg_CA(ID). After the user's real identity ID is authenticated by the CA, and the start and end time of the user

authorization and the user's identity are signed by the CA, the certificate will be obtained and returned to the user (Where $\text{Cert} = \text{ID} \parallel \text{tb} \parallel \text{te} \parallel \text{SKCA}(\text{ID} \parallel \text{tb} \parallel \text{te})$);

- 2) AA initializes the module, runs the $\text{AA_Setup}()$ function. The detail is shown as follows: select a group-based broadcast encryption scheme, and determine a group for each attribute

x for $\forall x \in I_K$ AA_K . The trapdoor information $\{TDM_x\}_{x \in I_K}$ corresponding to its management attribute is encrypted with the private key of the attribute, AT_x . Obtain TDM_x , version 1, which will be sent to the CSP. AA_K calculates each attribute managed by it.

- 3) Key generation module. When a user u_j registers, AA_K will run the $\text{Key_Gen}(\text{Cert})$ function. The details are as follows:

AA_K verifies its certificate. If it is correct, selects $\forall v_{x,j}, z_j, k_j \in \mathbb{Z}_p$ randomly for each attribute x of u_j , calculate

$$\{B_{x,j} = A_x^{v_{x,j} \cdot H(\text{ID})} \cdot AT_{x,K}, D_{x,j} = g^{-v_{x,j} \cdot H(\text{ID})}\}_{x \in I_u}, D_{j1} = g^{\alpha/z_j + \beta k_j}$$

and $D_{j2} = g^{-k_j}$, to get the user's private key $sk_{j,k}$, send $sk_{j,k}$ to the user, where

$$sk_{j,k} = \{S_K, \{B_{x,j}, D_{x,j}\}_{x \in I_u}, t_{\text{end}}, I_u = \{att_i\}, D_{j1}, D_{j2}, z_j\};$$

- 4) Encryption module. Input plaintext message m , system public parameter PP , data owner runs $\text{Encrypt}(PP, m)$. The details are shown as follows:

Choose the symmetric encryption key k , and encrypt the confidential information m symmetrically to obtain $E_K(m)$; construct an access control policy $\Gamma = (M, \rho)$, where M is an $l \times d$ matrix, and encrypt the symmetric encryption key k with attributes. Randomly select $s \in \mathbb{Z}_p$, record the vector $\vec{v} = (s, v_2, v_3, \dots, v_d)$, then $\lambda_i = \vec{v} \cdot M_i$, calculate $C = k \cdot e(g, g)^{\text{as}}$ for all attributes involved in the access control strategy, obtain the

corresponding attribute public key GTDM, and calculate $\{C_i = g^{\lambda_i \cdot TD_i}, C'_i = g^{\beta \lambda_i}\}_{i \in I_A}$ (IA represents all attributes involved in the access control policy),

And finally, get the ciphertext CT, and send it to the cloud server C S P.

$$CT = \{E_k(m), C = k \cdot e(g, g)^{\alpha s}, \{C_i = g^{\lambda_i \cdot TD_i}, C'_i = g^{\beta \lambda_i}\}_{i \in I_A}, (M, \rho)\};$$

The wireless transceiver module is connected with the voice controller for digital signal data transmission and reception;

The data management module is used for storing voice information;

The mobile terminal is connected with the voice controller to receive the digital signal sent by the voice controller through the communication system and share data with the host computer.

2. The bone conduction communication system based on the Internet of Things as described in claim 1 is characterized by a voice controller constituted of a built-in frequency analysis unit, a phase curve calculation unit, an error calculation unit, and a sound signal recognition unit;

The frequency analysis unit analyzes the frequency signal of sound signals;

The phase curve calculation unit calculates a phase curve that approximates the time change of the phase of the frequency signal;

The error calculation unit calculates the error between the phase curve and the phase of the frequency signal; the sound signal recognition unit identifies whether the sound signal is a periodic sound signal based on the error.

3. The bone conduction communication system based on the Internet of Things as described in claim 1 is characterized by the host computer which comprises a first channel terminal, a second channel terminal, and a microphone terminal;

A data sending module that is electrically connected to the microphone terminal, to send data to the mobile terminal;

A data receiving module that is electrically connected to the second sound channel terminal to receive data from the mobile terminal;

A safety authentication module that is electrically connected to the data sending module and the data receiving module;

A power taking module, the input end of which is electrically connected to the first sound channel terminal, and the output end of the power taking module supplies power to the data sending module, the data receiving module, and the safety authentication module.

4. The bone conduction communication system based on the Internet of Things as described in claim 1 is characterized by the data scan lines which include data lines, scan lines and pixels;

The pixel is formed at the intersection of the data line and the scan line, and includes a first sub-pixel, a second sub-pixel, a third sub-pixel, and a fourth sub-pixel;

The first sub-pixel includes a first switch, a first liquid crystal capacitor, and a first storage capacitor. The first terminal of the first switch is connected to the scan line, the second terminal of the first switch is connected to the data line, and the third terminal of the first switch is connected to the first terminal of the first liquid crystal capacitor and the first terminal of the first storage capacitor;

The second sub-pixel includes a second switch, a second liquid crystal capacitor, and a second storage capacitor. The first terminal of the second switch is connected to the scan line, the second terminal of the second switch is connected to the data line, and the third terminal of the second switch is connected to the first terminal of the second liquid crystal capacitor and the first terminal of the second storage capacitor, and the second storage capacitor line is electrically connected to the second terminal of the second storage capacitor;

The third sub-pixel includes a third switch, a third liquid crystal capacitor, and a third storage capacitor. The first terminal of the third switch is connected to the scan line, the second terminal of the third switch is connected to the data line, and the third terminal of the third switch is connected to the first terminal of the third liquid crystal capacitor and the first terminal of the third storage capacitor. The second storage capacitor line is electrically connected to the second terminal of the third storage capacitor;

The fourth sub-pixel includes a fourth switch, a fourth liquid crystal capacitor, and a fourth storage capacitor. The first terminal of the fourth switch is connected to the scan line, the fourth terminal of the fourth switch is connected to the data line, and the third terminal of the fourth switch is connected to the first terminal of the fourth liquid crystal capacitor and the first terminal of the fourth storage capacitor, and the first storage capacitor line is electrically connected to the second terminal of the fourth storage capacitor;

When the scan line is enabled, the first switch element, the second switch element, the third switch element, and the fourth switch element are turned on, so that the signal of the data line is transmitted to the first sub-pixel, the second sub-pixel, the third sub-pixel and the fourth sub-pixel. When the scan line is disabled, the electrical levels of the first storage capacitor line, the second storage capacitor line, the third storage capacitor line, and the fourth storage capacitor line will be changed respectively, so that the pixel voltage of the first sub-pixel will have a first offset voltage from the input voltage, the pixel voltage of the second sub-pixel will have a second offset voltage from the input voltage, and the pixel voltage of the third sub-pixel will have a third offset voltage from the input voltage, and the pixel voltage of the fourth sub-pixel will have a fourth offset voltage from the input voltage. Hence, the pixel voltage of the first sub-pixel, the second sub-pixel, the third sub-pixel, and the fourth sub-pixel will be different from each other. Furthermore, the first offset voltage, the second offset voltage, the third offset voltage, and the fourth offset voltage are different from each other.

5. A communication method of a bone conduction communication system based on the Internet of Things as described in claim 1 constitute the following contents:

The microphone signal is provided through the headset unit. The headset signal provided by the voice controller is converted into a corresponding voice;

The microphone signal transmitted by the headset unit is controlled, detected, and communicated through the voice controller;

The said signal is converted into a digital signal and compressed in real-time to become data in smaller volume and sent to the host computer through the communication system;

The voice signal is received through the signal receiving module;

Encrypt the voice signal through the encryption module;

Receive and send digital signal data through the wireless transceiver module;

Store voice information through the data management module;

Share the data in the form of digital signals with the host computer, which are sent by the reception voice controller to the mobile terminal through the communication system.