

Multimedia Device and Process for Data Transmission in a Multimedia Device

Specification

The invention relates to a multimedia device in accordance with the generic part of Claim 1 as well as to a process for data transmission in a multimedia device in accordance with the generic part of Claim 2.

A device and process of this type are known from DE 198 58 310 B4.

The current apparatuses of entertainment electronics such as, e.g., television apparatuses, audio apparatuses, DVD apparatuses, satellite receivers, video recorders, set-top boxes, etc. are customarily operated by a remote control that usually communicates wirelessly with the corresponding apparatuses. All these multimedia apparatuses, which also include computers nowadays, are designated in the following as "apparatus". All these apparatuses as well as increasingly also other devices present in households such as, e.g., garage-door controls, alarm systems, heating controls, household apparatuses and kitchen apparatuses as well as telecommunication devices such as telephone, fax, internet access are currently networked to an increasing degree and controlled to the extent possible by only one single remote control. Many of the cited apparatuses can be individually

configured for different users and adapted to preferences of the particular user. A few known adaptations will be explained using the example of a television receiver:

- A “child safety” can be provided that allows only selected television channels and/or allows a television reception only at predefined times;
- television habits can be preprogrammed, for example, in that a certain user views certain transmissions on certain channels on certain days of the week at certain times;
- a list of preferred television channels can be set up for each user that are preferably displayed as favorites in a selection menu;
- the individual key assignment of the keys of the remote control can be changed according to user and apparatus;
- safeties can be provided in interactive systems such as interactive television, home shopping, home banking, video on demand or the like, for example, limitations for orders of items or films, types of films (e.g., g-rated), etc.

It is necessary for the above reasons to automatically adapt the remote control to the particular user and to configure and release individual access authorization.

To this end it has already been frequently suggested that the remote control be provided with an identification device that recognizes, automatically if possible, a person with access authorization. Thus, DE 190 58 310 B4 suggests providing a fingerprint reader in the remote control that detects biometric data of the user by sensors and activates an individual operating profile upon recognition of a person with authorized access.

Even other detection apparatuses for biometric data such as a voice recognition circuit, an iris scanning apparatus and a face recognition apparatus have already been suggested (cf. WO 02/17627 A2).

The fingerprint of a person is used especially frequently for identification such as described, e.g., in US 2001/007592 A1, US 2005/0149870 A1, US 5, 758, 257, US 5, 771, 307, US 5, 920, 642, US 6, 020, 882, US 6, 130, 726, US 6, 137, 539, US 6, 914, 517 B2, US 6, 968, 565 B1, or WO 01/56,213 A1.

The following problems are present in all these remote controls:

- A high degree of security should be insured, which means that an apparatus can not be operated by a foreign remote control and that a new user can not be created “in an unauthorized manner”;

- the hardware cost of the remote control should be as low as possible;
- the current consumption of the remote control should be as low as possible;
- the communication between remote control and apparatus should be as “tap-proof” as possible, which is especially important because there are a plurality of programmable remote controls on the market that can record, store and reproduce signals transmitted by an original remote control.

There are various suggestions for increasing security. Thus, US 2001/0007592 A1 suggests scanning a series of several fingerprints of different fingers.

EP 1 286 518 A2 suggests providing at least one key of the remote control with a fingerprint reader so a check of the authorized user is performed each time during the querying of certain functions such as, e.g., change of channel, confirmation key or the like.

In order to increase the access security the older, non-pre-published German Patent Application 10 2006 042 014 of the Applicant suggested providing, in addition to a reading device for biometric data, especially a fingerprint

reader, another hardware device that identifies the remote control as such, which is realized in the concrete exemplary embodiment by a so-called SIM ("Single Identity Module") card. Thus, at least the new creation of a user profile or the changing of an existing user profile is only possible if the SIM card is inserted into the remote control.

The invention has the problem of improving the initially cited multimedia device as well as the process for data transmission in a multimedia device of the initially cited type in such a manner that high transmission security of the data from the remote control to the apparatus is ensured with a low hardware cost.

This problem is solved for the multimedia device but the features indicated in Claim 1 and for the process by the features indicated in Claim 2.

Advantageous embodiments and further developments of the invention can be gathered from the subclaims.

In brief, the partial problem of the reduced hardware costs is solved in that the biometric data detected by the remote control is transferred to the apparatus and is not evaluated until it is there. The evaluation of the biometric data requires a relatively high processor power, that is present in any case in the apparatus, whereas the detection of the biometric data, for

example, with a fingerprint reader requires only comparatively less computer power so that a simpler and therefore less expensive processor can be used in the remote control, which processor then also has a lower current requirement. The increased security of the data transmission is ensured by a special encoding of the data transmitted from the remote control to the apparatus with the inclusion of data stored on the SIM card.

The invention is explained in more detail in this connection in the following using an exemplary embodiment.

- Fig. 1 shows a block schematic of a multimedia device with remote control and multimedia apparatus;
- Fig. 2 shows a flowchart of the processing steps of the process in the initialization of a connection between remote control and apparatus;
- Fig. 3 shows a flowchart of the processing steps of the process in an identification process.

Fig. 1 shows a remote control 1 that controls an apparatus 2 that for its part can control a plurality of other apparatuses, as indicated above. In fig. 1 only the components decisive for the control are shown.

The remote control 1 comprises a microprocessor 3, a memory 4, a SIM card reader 5, a keyboard 6 and a device 7 for detecting biometric data, in

particular an apparatus for detecting a fingerprint. Furthermore, the remote control comprises a transmitting/receiving device 8, preferably for sending and receiving infrared signals. The cited components 4-8 are connected to microprocessor 3.

Memory 4 can be divided into several subgroups and comprise, for example, a read-only memory for programs and a processing memory. A SIM card to be set into the SIM card reader 5 also contains one or more memories in a known manner. Sending/receiving unit 8 communicates via a bidirectional wireless radio connection 9 with apparatus 2. Apparatus 2 also comprises a microprocessor 10, a memory 11, that also comprises a program memory and a processing memory as well as another memory that is designated here as a user databank 12 and, finally, a sending/receiving unit 13 that communicates wirelessly with sending/receiving unit 8 of the remote control.

Microprocessor 10 has an output 14 that communicates via an interface 15 with one or more apparatuses to be controlled.

Any desired number of different apparatuses to be controlled can be connected with known connections, e.g., "SCART" cable, "USB" connection or the like to interface 15.

It should be emphasized that microprocessor 3 of remote control 1 has less computer power than microprocessor 10 of the apparatus. It therefore also has less current consumption and is more economical.

The initialization phase will now be described with reference made to Fig. 2. At first, the SIM card must be inserted in a step 20 into the SIM card reader 5 of Fig. 1. The SIM card contains the following stored data:

1. A personal identification number (so-called PIN),
2. personal data of a user such as, e.g., name, date of birth, sex, credit card number, etc.,
3. a first private code (PrivK 1), with which the data cited under 2. and 3. is only accessible after the inputting of the PIN cited under 1.

Furthermore, the SIM card contains the following freely accessible data:

4. a second private code (PrivK 2),
5. a personal identification code (PIC),
6. a first public code (PubK 1) and
7. a second public code (PubK 2).

As will be explained in even more detail further below, the codes PubK 1 and PrivK 1 form a first and the codes PubK 2 and PrivK 2 form a second

pair of codes that are used for encoding and decoding. A so-called asymmetric cryptography is used here in which a code of one of the cited pairs, usually the so-called public code, is used for encoding data and for decoding the other code of the pair, usually the so-called private code, is used for decoding. Thus, different codes are used for encoding and for decoding. A decoding of data with the code that was used for the encoding is not possible. The algorithms for encoding and decoding are known in principle. Refer, for example, to the asymmetric encoding algorithm RSA, the Rabin cryptosystem or the Elgamal cryptosystem. After the insertion of the SIM card the PIN is queried at first (step 21), that is inputted via the keyboard 6 (fig. 1) and is usually a four-digit number. This clears the SIM card and the personal data, cited above and blocked by the PIN, and the private first code PrivK 1 are accessible.

The remote control then sends the first private code PrivK1 via the sending/receiving unit 8 (step 22) and the second public code PubK2 (step 24) to apparatus 2, where it is received by sending/receiving unit 13 and stored via microprocessor 10 in memory 11 (steps 22-25). Then, the biometric data of the user is read in via the fingerprint reading device 7 (step 27) and transmitted to apparatus 2 (step 28) where it is encoded with the previously received and stored public code PubK2 (step 29). In a similar manner the personal identification code PIC is queried by the SIM card and transmitted to apparatus 2 (step 30), where it is also encoded with the public

code PubK 2 (step 31). Then the personal data of the user is either queried by the SIM card or inputted via the keyboard and transmitted to apparatus 2 (step 32), where it is also encoded with the second public code PubK 2 in step 33.

The second public code PubK 2, that was stored in apparatus 2 in step 25 is canceled after these procedures in step 34. A user profile is then created and stored in user databank 12 that contains the following data at first:

- the non-encoded first private code PrivK 1,
- the biometric data of the user encoded with the code PubK 2,
- the encoded personal identification code (PIC) and the encoded personal data, each encoded with PubK 2.

In addition, the user can add other data to the personal data such as, e.g., a channel list of preferred television channels, individual key assignments of the keys of the remote control, blocks television channels, television times, etc.

The described initialization procedure is to be classified as critical to the extent that the first private code PrivK 1 is transmitted wirelessly and can therefore be “eavesdropped” if a suitable receiving apparatus is in the range of transmission. In the case of an infrared transmission the danger that a

suitable receiving apparatus is in the range of transmission is, however, very small since the range of transmission is sharply limited and an undisturbed sight connection is required.

Subsequently, however, there is great security since the remaining data is encoded with the public code PubK 2, that is cancelled after the initialization in apparatus 2 and this data can not be decoded with the private first code PrivK 1.

For a further increasing of security even code PrivK 1 on the SIM card can be cancelled so that it can be designated as a “private” code that is still available only for the apparatus.

Now the normal identification process will be described in conjunction with fig. 3, with which a connection is established between remote control 1 and the initialized apparatus 2. It is assumed that remote control 1 is ready to send and apparatus 2 is ready to receive.

In step 35 the biometric data of the user is read, for example, in that the user places a finger on the fingerprint reading apparatus 7, that reads in the corresponding image data. This image data can be compressed in a step 36, which takes place in accordance with known data compression processes such as, e.g., the Huffman code.

This compressed image data is added in step 37 to the personal identification code PIC that is read out either from the SIM card or from memory 4 (fig. 1). This entire data packet consists of the compressed biometric data, the PIC and the code PrivK 2. This data packet is encoded with the first public key PubK 1 in step 39. In addition, a block coding and a so-called forward error correction (in short, FEC, from English "forward error correction") can be optionally carried out (step 40).

The data produced in this manner is then transmitted to apparatus 2 via radio link 9 (step 41) and received by apparatus 2 (step 42). There, this data is at first decoded with the private code PrivK 1 stored in the user databank (step 43), from which a data set with PrivK 2, PIC and the biometric data is obtained (block 44), from which the second private code PrivK 2 is extracted in step 45. The biometric data in the PIC is temporarily stored in working memory 11. The data, namely the PIC, stored in user databank 12 and encoded with the public code PubK 2 prior to being stored, the biometric data and the personal data are decoded with the now decoded and extracted second private code PrivK 2 and in the following step 47 the now decoded data from the user databank and the received data are compared with one another. The PIC is advantageously compared at first. In as far as it does not coincide, the received data does not stem from an authorized remote control, so that further processing steps can be broken off. A request for a repeated sending can optionally be generated that is displayed, for example,

on a screen of the television apparatus or is transmitted to remote control 1 as a return signal via radio link 9 and displayed there.

If a comparison of the PIC yields an authorized remote control, then the biometric data is compared (step 47) and upon agreement microprocessor 10 emits a release signal at its output 14 to interface 15 (step 8). Then, a secured, authorized operation of apparatus 2 and of the other apparatuses connected to it can be carried out by remote control 1. Furthermore, the individual key assignment of the keys of remote control 1 can also be set via radio link 9 corresponding to the identified user. Also, an acknowledge signal for a successful login is transmitted via radio link 9 to the remote control which signal cancels sensitive data in memory 4 in the remote control, in particular the detected biometric data. In a similar manner the data to be compared with each other in memory 11 of the apparatus are also cancelled so that memories 11 and 4 of remote control 1 and of apparatus 2 are back in their initial state after the successful login. The normal operation between remote control 1 and apparatus 2 can then be resumed, that can also be bidirectional.

It can also be provided for reasons of safety that the authorized connection is interrupted after a set time and a new login is to be made in accordance with the steps described in conjunction with fig. 3. It can also be provided that a new identification is to be made for certain control procedures relevant

for security, for example, in the transmission of name, address or credit card number via connected communication apparatuses.

In the case of the personal data of the particular user, user rights can also be given during the initialization in accordance with the processing steps described in conjunction with fig. 2, for example, regarding the creating or changing of user profiles so that, for example, only certain persons identified via their biometric data are entitled to create new users in the user databank or to change rights assigned to certain individual users. On the other hand, it can be stipulated for other data that is also stored in the personal data that the individual user can freely change it after his identification, such as, e.g., individual key assignment of the keys of the remote control, favorites list of individual television transmitters, to the extent that they are approved.

In sum, a very high degree of security is achieved with the invention. Even if the apparatus without an SIM card gets in the hands of unauthorized persons it is not possible to access the protected biometric data and the protected personal data. Only if an authorized person has the apparatus and the SIM card is it theoretically possible to decode the protected data stored in the user databank with the first key PubK 1 stored on the SIM card. However, in order to do this the user must then have direct access to the user databank, which requires a great technical expenditure. It can be provided by the manufacturer here that the corresponding memory is protected in such

a manner that either no access from the outside as possible or that its contents are automatically canceled if an attempt is made to configure the memory. In any case it is recommended to cancel the memory containing the user databank before the apparatus is given to third parties.

Claims

1. A multimedia device with a remote control (1), that comprises
 - a first microprocessor (3),
 - a first hardware device (5) for identifying the remote control (1),
 - a second hardware device (7) for detecting biometric data of a person, and
 - a transmitting device (8) for transmitting data,and with a multimedia apparatus (2) that comprises
 - a receiving device (13) for receiving the data,a memory (11, 12) and a second microprocessor (10), characterized in that the first hardware device is a SIM card (5) on which the following data is stored:
 - a first pair of digital codes (PubK 1, PrivK 1),
 - a second pair of digital codes (PubK 2, PrivK 2),
 - a personal identification code (PIC), and
 - personal data of at least one user,that the memory (12) of the multimedia apparatus (2) holds the following data stored after a first initialization:
 - only one code (PrivK 1) of the first pair of digital codes,
 - only one code (PubK 2) of the second pair of digital codes,

- biometric data and personal data of a user, as well as the personal identification code (PIC) encoded with the only one code (PubK 2) of the second pair of digital codes,

that the second hardware device (7) reads in biometric data of the user upon an established connection between the remote control (1) and the multimedia apparatus (2),

adds to them the personal identification code (PIC) and the other code (PrivK 2) of the second pair of digital codes,

encodes a data packet formed in this manner with the other code (PubK 1) of the first pair of digital codes and transmits the data set encoded in this manner to the multimedia device (2),

that the multimedia device (2) decodes the received, encoded data set with the stored one code (PrivK 1) of the first pair of digital codes,

extracts from it the other code (PrivK 2) of the second pair of digital codes, the personal identification code (PIC) and the biometric data,

extracts from the memory (12) the encoded biometric data, the encoded personal data and the encoded personal identification code (PIC) and decodes them with the other code (PrivK 2) of the second pair of digital codes, compares the received, decoded personal identification code and the decoded, stored personal identification code with one another and upon agreement compares the received, decoded biometric data and the stored, decoded biometric data with each other and only clears the multimedia apparatus (2) upon agreement.

2. A process for data transmission in a multimedia device in accordance with Claim 1 with the following process steps:

Storing of a first code (PrivK 1) of a first pair of digital codes in a memory of a multimedia device,

Storing of user data encoded with a first code (PubK 2) of a second pair of digital codes which data contains biometric data, a personal identification code (PIC) and personal data,

Reading in biometric data of a user into a remote control,

Adding a personal identification code (PIC) from a memory as well as adding a second code (PrivK 2) of the second pair of digital codes for forming a data set, encoding this data set with the second code of the first pair of digital codes,

Transmitting the data set encoded in this manner to a multimedia device,

Decoding the received data set with the stored first code (PrivK 1) of the first pair of digital codes,

Extracting components (PrivK 2, PIC, biometric data) from the decoded data set,

Decoding the encoded data stored in the memory of the multimedia device with the extracted, decoded second code of the second pair of digital codes,

Comparing the decoded, received identification code with the decoded, stored personal identification code and, upon agreement,

Comparing the received, decoded biometric data with the stored, decoded biometric data, and

Clearing the multimedia device if the comparison of the biometric data results in an agreement.

3. The process according to claim 2, characterized in that the biometric data read into the remote control is compressed before the forming of the data set.
4. The process according to Claim 3, characterized in that the compression takes place according to the Huffman code.
5. The process according to one of Claims 2 to 4, characterized in that the data set to be transmitted from the remote control to the multimedia device is block-coded.
6. The process according to one or more of Claims 2 to 5, characterized in that the data set to be transmitted from the remote control to the multimedia device is provided with a forward error correction.